УТВЕРЖДЕН
RU.48957919.501410-02 92-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock 8.0

(версия 8.0.761.1)

Руководство по эксплуатации

RU.48957919.501410-02 92

Листов 441

АННОТАЦИЯ

Данное руководство по эксплуатации освещает вопросы по установке, настройке и сопровождению Системы защиты информации от несанкционированного доступа Dallas Lock 8.0 и предназначено для лиц, ответственных за эксплуатацию системы защиты информации.

Руководство по эксплуатации подразумевает наличие у пользователя навыков работы в ОС Windows.

В документе представлены элементы графических интерфейсов, которые соответствуют эксплуатации СЗИ Dallas Lock 8.0 в ОС Windows 7, Windows 8, Windows 10 и Windows 11. Следует обратить внимание, что элементы графического интерфейса могут иметь незначительные отличия от представленных.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данное руководство предназначено для администратора программного продукта «Система защиты информации от несанкционированного доступа Dallas Lock 8.0» (далее — СЗИ или Dallas Lock 8.0).

В руководстве содержатся сведения, необходимые для получения общего представления о системе защиты, ее функциональных возможностях, а также для установки, настройки и управления работой в соответствии с требованиями безопасности.

В данном руководстве описание работы с системой носит процедурный характер, то есть основное внимание сосредоточено на порядке выполнения тех или иных действий.

Руководство состоит из 23 глав и имеет следующую структуру:

1. Глава 1 содержит общее описание назначения и возможностей системы.
2. В Главе 2 приводятся сведения, необходимые для установки (инсталляции), а также для ее удаления и входа на уже защищенный Dallas Lock 8.0 компьютер.
3. Глава 3 дает общее представление о пользовательском интерфейсе программы администрирования системы и принципах работы, необходимых непосредственно администратору системы.
4. Главы 4–18 подробно описывают функциональные возможности основных подсистем, модулей, механизмов и настроек системы защиты Dallas Lock 8.0.
5. В Главе 19 описываются функциональные возможности модулей централизованного управления системы защиты «Сервер безопасности» и «Менеджер серверов безопасности».
6. В Главе 20 приведены общие сведения о модуле централизованного управления «Единый центр управления Dallas Lock».
7. В Главе 21 приведены общие сведения о модуле «Сервер конфигураций».
8. В Главах 22 и 23 описывается восстановление персонального компьютера (далее — ПК) при сбое системы защиты и восстановление данных жесткого диска.

Вы можете посетить сайт компании-разработчика Dallas Lock 8.0 ООО «Конфидент» www.confident.ru или сайт продуктовой линейки www.dallaslock.ru.

На сайте продуктовой линейки можно получить информацию о системе защиты Dallas Lock 8.0, предыдущих версиях, а также заказать комплекс услуг по проектированию, внедрению и сопровождению продукта. Также при необходимости можно обратиться в службу технической поддержки Dallas Lock 8.0 по электронному адресу: helpdesk@confident.ru.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

СЗИ имеет две редакции: **«К»** и **«С».** Наличие тех или иных функциональных возможностей в редакциях обусловлено уровнем сертификата и требованиями к данному уровню.

Dallas Lock 8.0 редакции **«С»** является расширением версии **«К»** и согласно требованиям имеет дополнительные функциональные возможности. В тексте руководства для выделения разделов, содержащих описание функций, которые относятся только к редакции **«С»**, используется условное обозначение:

Данный параметр доступен только для Dallas Lock 8.0 редакции «С»

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ

1.1 Общее описание

СЗИ Dallas Lock 8.0 предназначена для предотвращения получения защищаемой информации заинтересованными лицами с нарушением установленных норм и правил и обладателями информации с нарушением установленных правил разграничения доступа к защищаемой информации и осуществления контроля за потоками информации, поступающими в автоматизированную систему (далее — АС) и выходящими за ее пределы, обеспечения защиты информации в АС посредством ее фильтрации.

Система защиты Dallas Lock 8.0 представляет собой программный комплекс средств защиты информации в операционных системах (далее — ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.

Использование системы защиты Dallas Lock 8.0 в проектах по защите информации позволяет привести АС в соответствие требованиям законодательства Российской Федерации.

Система защиты предназначена для использования на персональных компьютерах (далее — ПК), портативных компьютерах (ноутбуках), серверах (файловых, контроллерах домена и терминального доступа), также поддерживает виртуальные среды и технологию Windows To Go. Может функционировать как на автономных ПК, так и на компьютерах в составе локальной вычислительной сети (далее — ЛВС), в том числе под управлением контроллера домена.

Система защиты Dallas Lock 8.0 обеспечивает защиту информации от несанкционированного доступа (далее — НСД) на ПК в ЛВС через локальный, сетевой и терминальный входы. Также обеспечивает разграничение полномочий пользователей по доступу к файловой системе (далее — ФС), устройствам и другим ресурсам компьютера. Разграничения касаются всех пользователей: локальных, сетевых, доменных, терминальных.

1.2 Структура и составные модули

СЗИ Dallas Lock 8.0 состоит из следующих основных компонентов:

1. **Программное ядро (Драйвер защиты)**. Является ядром системы защиты и выполняет основные функции СЗИ:
   - обеспечивает мандатный (только для Dallas Lock 8.0 редакции «С») и дискреционный режимы контроля доступа к объектам ФС и устройствам;
   - обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ в соответствии с правами пользователей;
   - обеспечивает работу механизма делегирования полномочий;
   - обеспечивает проверку целостности СЗИ, объектов ФС, программно-аппаратной среды и реестра;
   - драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ.

Драйвер защиты автоматически запускается на защищенном автоматизированном рабочем месте (далее — ЗАРМ) при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие.

С драйвером защиты взаимодействуют защитные подсистемы, перечисленные ниже.

2. **Подсистема администрирования**. Включает в себя:
   - Подсистему локального администрирования. Обеспечивает возможности по управлению СЗИ, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс Windows Explorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования.
   - Подсистему удаленного администрирования. Позволяет выполнять настройку системы защиты с удаленного компьютера.
   - Подсистему централизованного управления. Включает в себя основные компоненты:
     - модуль «Сервер безопасности» (далее — СБ), который позволяет объединять защищенные компьютеры в домен безопасности (далее — ДБ) для централизованного и оперативного управления (далее — ОУ) клиентами;
     - модуль «Менеджер серверов безопасности» (далее — МСБ), который позволяет объединить несколько серверов безопасности в единую логическую единицу — «Лес

безопасности» (далее — ЛБ).

3. **Подсистема управления доступом**. Включает в себя:
   - Подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов.
   - Подсистему доступа к ФС, реестру и устройствам, в составе которой:
     - подсистема дискреционного доступа;
     - подсистема мандатного доступа (только для Dallas Lock 8.0 редакции «С»).
   - Модуль «Загрузчик DL» (только для Dallas Lock 8.0 редакции «С»). Является опционным модулем, включается по команде администратора и может быть не активированным. Активный модуль отрабатывает до начала загрузки ОС.
4. **Подсистема регистрации и учета**. Включает в себя:
   - Подсистему аудита. Обеспечивает ведение аудита и хранение информации 12-ти категорий событий в журналах.
   - Подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.
5. **Подсистема идентификации и аутентификации**. Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в ОС.
6. **Подсистема гарантированной зачистки информации**. Обеспечивает зачистку остаточной информации.
7. **Подсистема преобразования информации**. Обеспечивает:
   - преобразование информации в файлах-контейнерах;
   - преобразование сменных накопителей для защиты от доступа в обход СЗИ;
   - работу с данными при одновременном их преобразовании в файл-дисках;
   - прозрачное преобразование жестких дисков (только для Dallas Lock 8.0 редакции «С») для предотвращения доступа к данным, расположенным на жестких дисках, в обход СЗИ.
8. **Подсистема контроля устройств**. Обеспечивает возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.
9. **Подсистема межсетевого экранирования**. Обеспечивает контроль, а также фильтрацию потоков информации, поступающих в АС и выходящих за ее пределы.
10. **Подсистема обнаружения вторжений**. Обеспечивает обнаружение и блокирование основных угроз безопасности, выполняет одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализирует некоторые отдельные сетевые протоколы.
11. **Подсистема контроля целостности.** Обеспечивает контроль целостности ФС, программно-аппаратной среды и реестра, периодическое тестирование СЗИ, наличие средств восстановления СЗИ, восстановление файлов и веток реестра в случае нарушения их целостности.
12. **Подсистема восстановления после сбоев.**
13. **Подсистема развертывания (установочные модули).**
14. **Подсистема централизованного контроля конфигураций.** Обеспечивает централизованный сбор, передачу и контроль (путем вычисления контрольных сумм и заверения информации простой электронной подписью) информации о состоянии программной среды в сетевом или автономном режиме с помощью программного модуля «Сервер конфигураций Dallas Lock» (далее — СК), а также реализует возможность управления администратором безопасности правами на доступ к модулю.
15. **Подсистема резервного копирования.** Модуль резервного копирования позволяет восстанавливать безвозвратно модифицированные или удаленные файлы или каталоги (с поддержкой вложенных файлов).

1.3 Возможности

СЗИ предоставляет следующие возможности:

1. В соответствии со своим назначением СЗИ Dallas Lock 8.0 запрещает посторонним лицам доступ к ресурсам ПК и позволяет разграничить права пользователей при работе на компьютере (постороннее лицо в данном контексте — человек, не имеющий своей учетной записи на данном компьютере). Разграничения касаются прав доступа к сети, к объектам ФС, веткам реестра и к устройствам. Для облегчения администрирования возможно объединение пользователей в группы. Контролируются права доступа для локальных, доменных, сетевых и терминальных пользователей.
2. Для предотвращения утечки информации с использованием сменных накопителей (таких как

CD-диск, USB-Flash накопитель и прочие) СЗИ обеспечивает следующие функции:

- разграничение доступа как к типам накопителей, так и к конкретным экземплярам;
- преобразование сменных накопителей с использованием ключа (в качестве ключа преобразования используется алгоритм преобразования, пароль и (или) аппаратный идентификатор);
- создание теневых копий файлов, отправляемых на сменные или сетевые накопители.

3. СЗИ Dallas Lock 8.0 позволяет в качестве средства опознавания пользователей использовать аппаратные идентификаторы:
   - USB-Flash-накопители;
   - электронные ключи Touch Memory (iButton) DS-1990, DS-1992, DS-1993, DS-1994, DS-1995, DS-1996;
   - HID Proximity-карты;
   - USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ;
   - USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен PINPad, Рутокен ЭЦП 3.0, Рутокен 2151;
   - USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash;
   - USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64;
   - NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X).

   Дополнительно имеется возможность определения принадлежности аппаратного идентификатора.

Примечание. В СЗИ Dallas Lock 8.0 аппаратная идентификация по умолчанию не является обязательной. Однако СЗИ можно настроить таким образом, что для конкретного пользователя или группы пользователей назначение аппаратного идентификатора будет обязательным.

4. В Dallas Lock 8.0 реализовано хранение авторизационной информации, а также биометрической информации в аппаратном идентификаторе. Определенные настройки при назначении идентификатора в профиле учетной записи делают возможным вход пользователя на ЗАРМ только по одному предъявлению идентификатора. Сохранение информации возможно в защищенной памяти идентификатора или в открытой. В случае если информация сохранена в защищенной памяти, запрашивается PIN-код. Для создания пароля, соответствующего всем установленным настройкам, в системе реализован механизм генерации паролей.
5. Есть возможность включения функции блокировки компьютера пользователя при отключении назначенного аппаратного идентификатора.
6. Для решения проблемы «простых» паролей СЗИ имеет гибкие настройки их сложности. Можно задать минимальную длину пароля, необходимость обязательного наличия в пароле цифр, специальных символов, строчных и прописных букв, степень отличия нового пароля от старого и срок действия.
7. Выбор значения «Число разрешенных сеансов» позволяет осуществлять проверку количества интерактивных сессий для данной учетной записи пользователя в настоящий момент на текущем компьютере: если число больше разрешенного — вход пользователя на ПК запрещается.
8. Включение модуля «Загрузчик DL» (только для Dallas Lock 8.0 редакции «С») позволяет авторизовать пользователя при входе на ПК до загрузки ОС. Загрузка ОС с жесткого диска осуществляется только после ввода особого PIN-кода и его проверки в СЗИ.
9. Помимо стандартного BIOS, модуль «Загрузчик DL» поддерживается ПК с материнскими платами, поддерживающими UEFI-интерфейс и GPT-разметку жесткого диска (только для Dallas Lock 8.0 редакции «С»).
10. В Dallas Lock 8.0 используется два принципа разграничения доступа (применяется полностью независимый от ОС механизм):
    - Мандатный (только для Dallas Lock 8.0 редакции «С») — каждому пользователю и каждому защищаемому объекту присваивается уровень доступа и (или) мандатная метка. Пользователь будет иметь доступ к объектам, уровень доступа которых не превышает его собственный и (или) мандатная метка объекта совпадает с его собственной мандатной меткой.

- Дискреционный — обеспечивает доступ к защищаемым объектам в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа). В соответствии с содержимым списка вычисляются права на доступ к объекту для каждого пользователя (чтение, запись, выполнение и прочие).

11. Dallas Lock 8.0 позволяет настраивать «Замкнутую программную среду» (далее — ЗПС) — режим, в котором пользователь может запускать только программы, определенные администратором.

12. Для удобства и облегчения настройки ЗПС и мандатного доступа реализованы:

- «Режим обучения» — в этом режиме, при обращении к ресурсу, доступ к которому запрещен, на этот ресурс автоматически назначаются выбранные администратором права.
- «Неактивный режим» — режим, в котором возможно полное или частичное отключение подсистем СЗИ Dallas Lock 8.0. Режим используется для диагностики нежелательного вмешательства СЗИ в работу ОС и сторонних приложений. Для включения/настройки режима пользователю нужно право на деактивацию СЗИ.

13. Настройка мандатного доступа (только для Dallas Lock 8.0 редакции «С») для корректной работы пользователей с установленным программным обеспечением (далее — ПО) упрощена автоматической настройкой. В автоматическом режиме данная настройка представляет собой применение определенного шаблона мандатного доступа с помощью встроенных средств СЗИ.

14. Для удобства работы, а также в дополнение к ЗПС в СЗИ реализована возможность использования вместо стандартной графической оболочки Windows защищенной оболочки Dallas Lock, программы, которая отвечает за создание рабочего стола, наличие на нем ярлыков программ, панели задач и меню «Пуск».

15. В Dallas Lock 8.0 реализован контроль доступа к подключаемым (не системным) устройствам: возможность разграничения доступа (мандатным и дискреционным принципами) и аудит событий доступа. Список устройств отображается в виде дерева объектов, которое содержит классы устройств и индивидуальные устройства.

16. В Dallas Lock 8.0 реализована функция разграничения доступа к буферу обмена по процессам. Выполняется путем назначения изолированных процессов. Изолированный процесс — процесс, для которого заблокирована возможность копирования информации в буфер обмена.

17. В СЗИ Dallas Lock 8.0 реализована подсистема обеспечения целостности ресурсов компьютера, которая обеспечивает:

- контроль целостности программно-аппаратной среды при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;
- контроль целостности объектов ФС (файлов и папок) при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;
- контроль целостности веток реестра при загрузке компьютера, по расписанию, через заданные интервалы (периодический контроль) и по команде администратора;
- блокировку входа в ОС компьютера при выявлении нарушения целостности;
- проверку целостности объектов ФС (файлов и папок) при доступе;
- восстановление файлов и веток реестра в случае обнаружения нарушения их целостности.

Для расчета целостности используются контрольные суммы, вычисленные по одному из алгоритмов на выбор: CRC32, MD5, ГОСТ Р 34.11-94.

18. СЗИ Dallas Lock 8.0 включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Параметрами определяется: количество циклов очистки: 1, 2, 3 или 4; производится ли очистка для всех или только конфиденциальных данных (только для Dallas Lock 8.0 редакции «С»). Зачистка дискового пространства производится по команде пользователя или в автоматическом режиме. Подсистема позволяет:

- очищать файл подкачки виртуальной памяти;
- очищать освобождаемое дисковое пространство;
- принудительно зачищать объекты ФС, используя соответствующий пункт в контекстном меню проводника (Windows Explorer);
- осуществлять контроль процесса очистки;
- предотвращать смену пользователя без перезагрузки;
- задавать маскирующую последовательность при зачистке остаточной информации.

19. В СЗИ Dallas Lock 8.0 реализована функция «Зачистка диска», которая позволяет полностью зачищать остаточные данные всего жесткого диска или его разделов. Это может быть полезно при снятии носителей с учета и необходимости полного удаления данных без возможности их восстановления по остаточной информации.

20. В СЗИ Dallas Lock 8.0 реализовано ведение 12-ти электронных журналов, в которых фиксируются действия пользователей:

- Журнал входов. В журнал заносятся все входы (или попытки входов с указанием причины отказа) и выходы пользователей ПК, включая локальные, сетевые, на другие ПК, в том числе терминальные входы и входы для удаленного администрирования.
- Журнал управления учетными записями. В журнал заносятся все события, связанные с созданием или удалением учетных записей пользователей, изменением их параметров.
- Журнал ресурсов. В журнал заносятся события доступа к объектам ФС, программно-аппаратной среды, веткам реестра и к устройствам, для которых назначен аудит.
- Журнал печати. В журнал заносятся все события, связанные с распечаткой документов на локальных или сетевых принтерах.
- Журнал управления политиками. В журнал заносятся все события, связанные с изменением конфигурации СЗИ. Также в этот журнал заносятся события запуска/завершения модулей администрирования Dallas Lock 8.0.
- Журнал процессов. Заносятся события запуска и завершения процессов в ОС.
- Журнал резервного копирования. В журнал заводятся события, связанные с резервным копированием объектов ФС.
- Журнал пакетов межсетевого экрана (далее — МЭ). В журнал заносятся все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера.
- Журнал соединений МЭ. В журнал заносятся сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами.
- Журнал событий ОС. В журнал заносятся сведения о событиях безопасности, генерируемых ОС и прикладным ПО.
- Журнал трафика. В журнал заносятся события, связанные с проходящим сетевым трафиком через контролируемые сетевые интерфейсы.
- Журнал контроля приложений. В журнал заносятся сведения об активности приложений, при вызове ими функций, связанных с безопасностью ОС.

Для облегчения работы с журналами есть возможность фильтрации, архивации, группировки по заданному набору полей и экспорта записей журналов в различные форматы. При переполнении, а также по команде администратора содержимое журнала архивируется и помещается в специальную папку, доступ к которой есть, в том числе, и через средства удаленного администрирования. Этим обеспечивается непрерывность ведения журналов.

21. Подсистема перехвата событий печати позволяет на каждом распечатанном с данного компьютера документе добавлять штамп, сохранять теневые копии распечатываемых документов. В рамках разграничения доступа имеется возможность разграничивать доступ пользователей к возможности печати, нанесения штампов и к самим принтерам.

22. Для защиты данных при их хранении и при передаче по различным каналам связи имеется возможность преобразования данных в файл-контейнер. В качестве ключа преобразования используется пароль и (или) аппаратный идентификатор. Распаковать такой контейнер можно на любом ПК, защищенном Dallas Lock 8.0 («С» или «К» при отсутствии мандатного доступа), при условии ввода верного пароля и наличии аппаратного идентификатора, предъявленных при создании контейнера.

23. Преобразование информации средствами СЗИ осуществляется встроенными алгоритмами преобразования.

24. Для защиты данных при их хранении и обработке имеется возможность работы на преобразованных файл-дисках. Данные файл-диски создаются и подключаются на защищенных ПК с использованием ключевой информации: пароля и (или) аппаратного идентификатора. После подключения преобразованный файл-диск отображается в проводнике ОС как логический диск. Работа на таком файл-диске выполняется одновременно с преобразованием данных, алгоритм преобразования указывается при создании файл-диска.

25. Реализована возможность включения функции блокировки преобразованного файл-диска при отключении назначенного аппаратного идентификатора.

26. При использовании нескольких защищенных СЗИ Dallas Lock 8.0 компьютеров в ЛВС возможно удаленное (сетевое) администрирование. Средствами удаленного администрирования осуществляется изменение политик безопасности, создание, редактирование и удаление учетных записей пользователей, назначение прав доступа к объектам, просмотр журналов, управление аудитом и контролем целостности. Модуль удаленного администрирования входит в состав всех поставок, его не требуется приобретать отдельно.

27. Реализован механизм проверки электронной подписи (далее — ЭП) при обновлении СЗИ Dallas

Lock 8.0.

28. При использовании нескольких защищенных СЗИ Dallas Lock 8.0 и СЗИ НСД Dallas Lock Linux компьютеров в ЛВС, а также нескольких аппаратных плат СДЗ Dallas Lock возможно централизованное управление ими. Это осуществляется с использованием СБ. Этот модуль должен быть установлен на отдельный компьютер, защищенный СЗИ Dallas Lock 8.0. Остальные компьютеры, введенные под контроль данного СБ, становятся его клиентами и образуют ДБ.

- С СБ осуществляется централизованное управление политиками безопасности, просмотр состояния, сбор журналов, создание/удаление/редактирование параметров пользователей, просмотр событий сигнализации о НСД на клиентах, управление ключами преобразования и прочее. С помощью МСБ имеется возможность объединения нескольких СБ в ЛБ.
- С помощью СБ возможны централизованная установка и удаление СЗИ Dallas Lock 8.0 и СЗИ НСД Dallas Lock Linux на компьютерах в сети, ввод в ДБ защищенных ПК и обновление версий Dallas Lock 8.0.
- Для ускорения внедрения СЗИ Dallas Lock 8.0 в крупных сетях может использоваться механизм удаленной установки и удаленного обновления версий средствами групповых политик AD с использованием сформированного на СБ msi-файла.
- В модули централизованного управления (СБ и МСБ) встроен механизм визуализации сети, защищаемой Dallas Lock 8.0. На отдельной вкладке есть возможность просмотреть и отредактировать блок-схему объектов ДБ, сохранить схему в файл.
- С помощью СБ возможно централизованно управлять контролем целостности защищенных СЗИ Dallas Lock 8.0 компьютеров в ЛВС.

29. Для решения задач организации централизованного управления решениями продуктовой линейки ООО «Конфидент» (СЗИ Dallas Lock 8.0, модули МЭ и СОВ Dallas Lock, СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock, СДЗ Dallas Lock, шлюз безопасности WAF Dallas Lock) и контроля конфигурации сетевого оборудования используется Единый центр управления Dallas Lock (далее ЕЦУ). ЕЦУ предоставляет следующие функциональные возможности:

- отслеживание статуса модулей;
- удаленное развертывание модулей;
- управление учетными записями, политиками и параметрами безопасности (+синхронизация);
- сбор, хранение и анализ журналов;
- оперативное управление;
- выполнение заданий на модулях;
- сигнализация.

30. СЗИ Dallas Lock 8.0 содержит подсистему самодиагностики основных функций безопасности СЗИ (тестирование).

31. Для повышения отказоустойчивости ДБ предусмотрена возможность ввода СБ в состав существующего домена. В этом случае сервера автоматическим образом выполняют реплицирование всех настроек домена и последующих действий администратора информационной безопасности. Нагрузка между реплицированными СБ распределяется. В связи с этим появилась возможность поддерживать большее число рабочих станций в составе ДБ.

32. Для удобства администрирования СЗИ возможно задание списка расширений файлов, работа с которыми будет блокирована. Это позволяет запретить сотрудникам работу с файлами, не имеющими отношения к их профессиональным обязанностям (mp3, avi и т. п.).

33. Для проверки соответствия настроек СЗИ есть возможность создания нескольких видов отчетов:

- отчета по назначенным правам и конфигурации;
- отчета со списком установленного ПО («Паспорта ПО»);
- отчета с характеристикой аппаратной части ПК («Паспорта аппаратной части»).

34. Предусматривается ведение резервных копий программных средств защиты информации, их периодическое обновление и контроль работоспособности, а также возможность возврата к настройкам по умолчанию.

35. При необходимости переноса настроек Dallas Lock 8.0 и СБ (политики, пользователи, группы, права доступа и т. д.) на другие компьютеры и для сохранения настроек при переустановке существует возможность создания файла конфигурации, который будет содержать выбранные администратором параметры. Файл конфигурации может быть применен: в процессе установки СЗИ, обновления или на уже ЗАРМ локально или средствами СБ.

36. СЗИ обеспечивает контроль съемных машинных носителей информации.

37. СЗИ обеспечивает защиту АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных

правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

- Для снижения трудоемкости настройки МЭ возможно использовать «Режим обучения МЭ», в котором при обращении к веб-ресурсу, доступ к которому разрешен, разрешающие права назначаются автоматически либо интерактивно.
- Посредством фильтрации возможно контролировать сетевой трафик по его содержимому (анализируется присутствие известных протоколов, медиа-контента и мобильный код) во всем фильтруемом трафике.
- Динамическая активация определенных правил МЭ в зависимости от условий функционирования системы, таких как нарушение целостности, отсутствие антивируса KES, отсутствие обновлений ОС, сигнатур системы обнаружения вторжений (далее — СОВ) или сигнатур антивируса, обеспечивается механизмом «профилей МЭ».
- Механизм «сетевых профилей» МЭ позволяет применять правила МЭ и фильтрации не безусловно, а в зависимости от параметров сети, через которую получен сетевой пакет. Есть возможность применять правила МЭ или фильтрации не безусловно, а только для определенных сетей, определяющихся сетевым профилем.

38. СЗИ обеспечивает защиту АС, используя сигнатурные и эвристические методы для анализа сетевого трафика и журналов ОС на предмет нештатных ситуаций и попыток проведения вторжений. Анализ собранных данных о сетевом трафике проходит в режиме, близком к реальному масштабу времени. Обеспечивает защиту от атак на сетевые протоколы на различных уровнях модели OSI. Также осуществляет перехват вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений.

39. Для снижения трудоемкости и эффективной настройки СОВ возможно в упрощенном интерфейсе определить требуемые уровни защищенности системы без проведения индивидуальных и точных настроек.

40. В СЗИ реализован механизм «Безопасной среды» (песочница), который позволяет производить проверки функционирования (попытки выполнения потенциально опасных действий) с целью определения степени доверия к стороннему ПО в изолированной, защищенной среде без внесения изменений в основную ОС.

41. В СЗИ на основе ролевой модели доступа реализован гибкий и понятный механизм разграничения прав на администрирование и аудит СБ и всего ДБ.

42. СК позволяет выполнять по сети сбор информации о ПО ПК с установленным Dallas Lock 8.0, отслеживать изменения в установленном ПО на клиентах, выполнять контроль и фиксацию состояния программной среды, формировать «Проект паспорта ПО», «Паспорт ПО», утверждать «Паспорт ПО» с помощью установки простой ЭП, создавать и редактировать права учетных записей СК.

1.4 Политика лицензирования

Подсистемы СЗИ Dallas Lock 8.0 доступны для использования при наличии и регистрации соответствующего серийного номера лицензии. Лицензируются следующие защитные механизмы:

1. Защита от НСД (СЗИ НСД).
2. Средство контроля подключения носителей информации (СКН).
3. Средство контроля отчуждения информации с носителей информации (СКН).
4. Межсетевой экран (МЭ).
5. Система обнаружения вторжений (СОВ).
6. Резервное копирование (РК).
7. Сервер конфигураций Dallas Lock (СК DL).

2 УСТАНОВКА И УДАЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ

2.1 Подготовка компьютера к установке

2.1.1 Требования к аппаратному и программному обеспечению

СЗИ Dallas Lock 8.0 может быть установлена на ПК, портативные и мобильные ПК (ноутбуки и планшетные ПК), сервера (файловые, контроллеры домена, терминального доступа) и виртуальные машины (например, VMware), работающие как в автономном режиме, так и в составе ЛВС.

СЗИ Dallas Lock 8.0 может работать на любом компьютере, работающем под управлением следующих ОС:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter) (см. Формуляр RU.48957919.501410-02 30 п. 3.3.4);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter) (см. Формуляр RU.48957919.501410-02 30 п. 3.3.4);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

СЗИ Dallas Lock 8.0 поддерживает 32- и 64-битные версии ОС Windows[1].

СЗИ Dallas Lock 8.0 позволяет защищать информационные ресурсы рабочего пространства Windows To Go ОС Windows 8, Windows 10 и Windows 11 на USB-накопителе.

Минимальная и оптимальная конфигурация ПК определяется требованиями к версии ОС Windows, на которую установлена СЗИ Dallas Lock 8.0.

Для размещения файлов системы и ее работы требуется не менее 1 Гбайт пространства на системном разделе жесткого диска.

Для использования Dallas Lock 8.0 на компьютере в составе ЛВС необходимо настроить сетевой протокол TCP/IP.

Для использования аппаратных идентификаторов требуется наличие в аппаратной части ПК соответствующих портов: USB-порта или COM-порта.

2.1.2 Ограничения

СЗИ Dallas Lock 8.0 имеет следующие ограничения:

1. При наличии на компьютере нескольких жестких дисков ОС должна быть установлена на первый жесткий диск.
2. При наличии на жестком диске нескольких разделов ОС должна быть установлена на диск C.
3. Установка Dallas Lock 8.0 всегда производится в каталог C:\DLLOCK80.
4. На время установки и удаления СЗИ необходимо отключить программные антивирусные средства.

Для корректной работы сетевых сигнатур СОВ необходимо указать номера или диапазон используемых портов (см. «Сигнатуры трафика»).

[1] Архитектура IA64 (Itanium) не поддерживается.

Примечание. При запуске установки Dallas Lock 8.0 на ОС Windows, установленную на сменный накопитель по технологии Windows To Go, может возникнуть ошибка подсистемы установки Windows Installer: 2755. В этом случае нужно распаковать установочный msi-файл Dallas Lock 8.0 в выбранный каталог командой «C:\> msiexec /a DallasLock8.0C.msi[2] /qb targetdir=c:\имя_каталога». После чего в каталоге, указанном в параметре targetdir, должны появиться: файл dlinst.exe и каталоги Files_x64, Files_x86. Затем нужно запустить программу установки из командной строки: «C:\имя_каталога\dlinst.exe /msi».

Данная ошибка является особенностью работы Windows To Go с msi-файлами.

Внимание! При необходимости изменить размер системного диска C потребуется удалить Dallas Lock 8.0 и после изменения размера установить заново.

Примечание. После установки Dallas Lock 8.0 компьютеру, работающему под управлением серверной ОС, уже нельзя добавлять роль контроллера домена.

Внимание! При обновлении ОС Windows (до Windows 8, Windows 8.1, Windows 10, Windows 11) изделие необходимо удалить (см. «Удаление системы защиты»), выполнить обновление, после чего установить изделие, используя при необходимости функцию сохранения конфигурации.

Примечание. Для корректной установки СЗИ Dallas Lock 8.0 на 32-х разрядную версию ОС Windows требуется не менее 2 ГБ оперативной памяти.

2.1.3 Предварительная подготовка

Перед установкой СЗИ Dallas Lock 8.0 необходимо выполнить следующие действия:

1. Если на компьютере уже установлена СЗИ, ее необходимо удалить.
2. Необходимо убедиться, что на диске C имеется необходимое свободное пространство для установки системы защиты.
3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows и устранить выявленные дефекты.
4. Рекомендуется произвести дефрагментацию диска.
5. Проверить компьютер на отсутствие вирусов.
6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы.
7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.

Также рекомендуется отключить кэширование записи для всех дисков. Для отключения кэширования записи необходимо:

1. В консоли управления компьютером открыть Диспетчер устройств.
2. Выбрать в узле дерева консоли «Дисковые устройства» диск, в его контекстном меню выбрать пункт «Свойства» и в появившемся диалоге открыть вкладку «Политика».
3. Снять флаг «Разрешить кэширование записи на диск» («Включить кэширование записи»).
4. Нажать кнопку «ОК».
5. Повторить вышеуказанные действия для всех дисков.

[2] DallasLock8.0K.msi

Примечание. Если используется RAID-контроллер, то, возможно, в BIOS контроллера нужно включить режим эмуляции «int13». На многих системных платах, имеющих встроенный RAID-контроллер, можно выбрать режим работы этого контроллера «Native» или «RAID». Рекомендуется использовать режим «Native». Необходимо использовать эти режимы с осторожностью, так как их переключение влияет на работу ОС.

2.1.4 Особенности установки

Внимание! Устанавливать СЗИ на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь.

Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Запуск установки от имени другого пользователя (Run as) не допускается.

Примечание. Если установка производится под учетной записью доменного пользователя:

1. Пользователь должен обладать правами локального администратора.
2. В процессе эксплуатации Dallas Lock 8.0 необходимо зарегистрировать в СЗИ хотя бы одну учетную запись локального пользователя с правами администратора, так как при возможном выводе компьютера из домена вход под доменной учетной записью будет невозможен.

Пользователь, установивший СЗИ, автоматически становится привилегированным пользователем — **суперадминистратором**. Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять учетную запись суперадминистратора средствами Windows запрещено.

Внимание! Имя и пароль пользователя для входа в ОС, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленной СЗИ Dallas Lock 8.0 пользователем в качестве суперадминистратора.

Если же компьютер является клиентом контроллера домена и при установке использовалась конфигурация по умолчанию[3], то зайти на ЗАРМ можно под любым доменным пользователем, так как в СЗИ автоматически создается и регистрируется учетная запись «**»[4].

Примечание. В процессе установки Dallas Lock 8.0 будет произведена автоматическая настройка брандмауэра Windows (Windows Firewall).

Внимание! Если будут использоваться сторонние firewall-программы, то необходимо добавить разрешения для TCP портов 17490, 17491, 17492, 17493 в их настройках вручную.

Примечание. Если СЗИ Dallas Lock 8.0 устанавливается на компьютер с устаревшей версией пакета обновлений (Service Pack) для текущей ОС, то при установке появится предупреждение.

2.2 Установка системы защиты

1. Для установки СЗИ Dallas Lock 8.0 необходимо запустить установочный файл «DallasLock8.0C.msi» («DallasLock8.0K.msi»), который находится в корневой директории дистрибутива (или выбрать данное действие в меню окна autorun).

   Если Dallas Lock 8.0 устанавливается на ПК, не оснащенный приводом компакт дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с установочного диска на данный ПК необходимый MSI-файл любым удобным способом: через ЛВС, USB-Flash накопитель

[3] Подробнее см. «Сохранение конфигурации».

[4] Подробнее см. «Регистрация доменных учетных записей по маске».

и др.

После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность отмены установки с возвратом сделанных изменений. Для этого служит кнопка «Отмена». Выполнение следующего шага установки выполняется с помощью кнопки «Далее».

2. При установке системы защиты на компьютере с установленной ОС 7 и выше после запуска приложения на экране будет выведено окно для подтверждения операции (рис. 1).

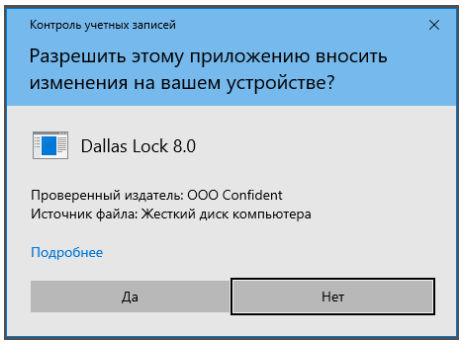


Рис. 1. Разрешение на установку программы в ОС

После подтверждения запустится программа установки СЗИ Dallas Lock 8.0 (рис. 2).

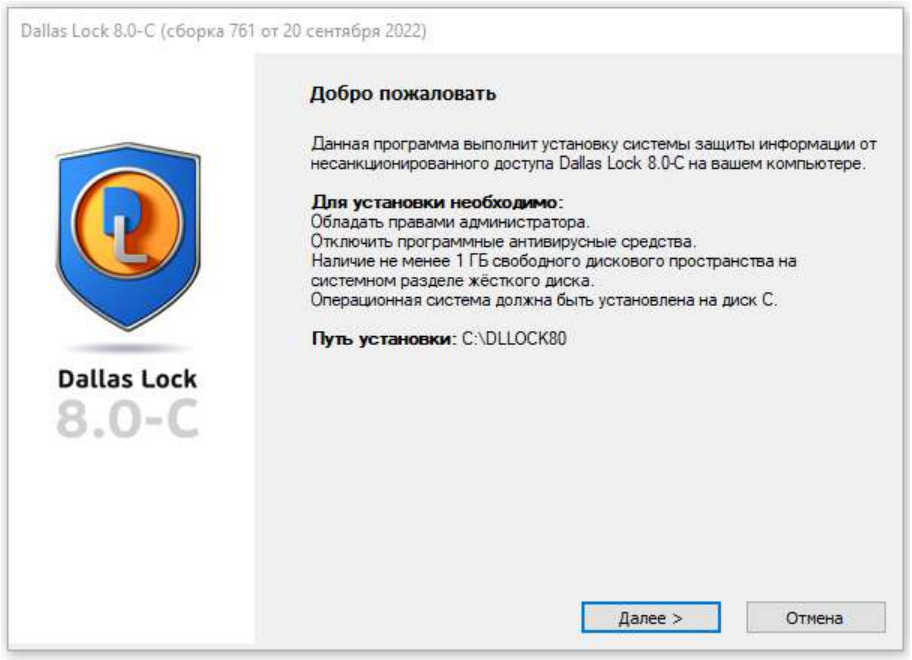


Рис. 2. Окно начала установки системы защиты

Для продолжения установки нажать кнопку «Далее».

3. Для защиты от нелегального использования продукта необходимо ввести номер лицензии Dallas Lock 8.0 и код технической поддержки, которые указаны на обложке футляра (рис. 3). Номер лицензии может активировать один или несколько модулей Dallas Lock 8.0 (МЭ, СОВ, СКН, РК), либо оставить их неактивными (в зависимости от приобретенного изделия).

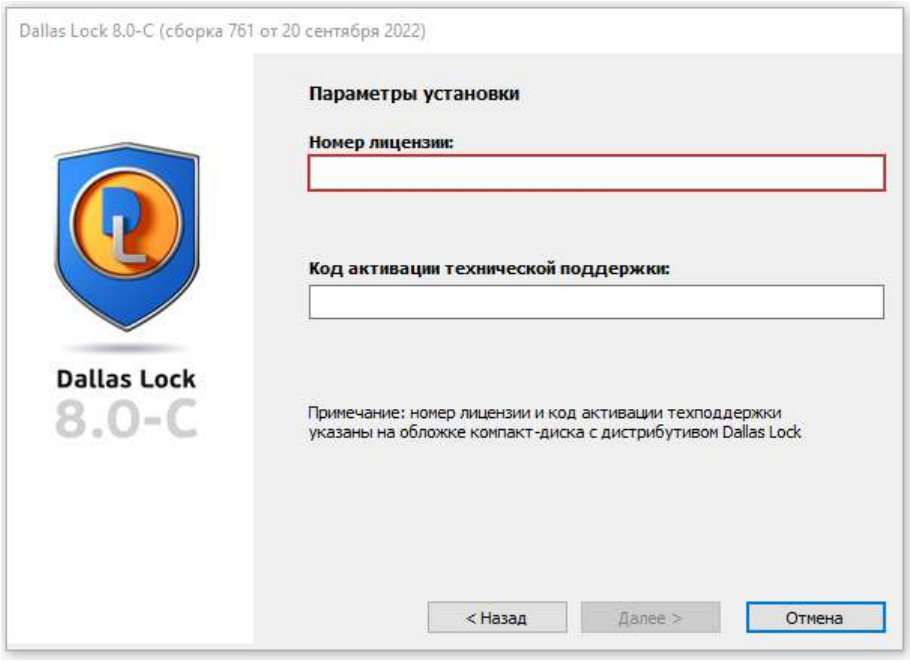


Рис. 3. Ввод параметров установки

Примечание. Поле «Код активации технической поддержки» не является обязательным при установке СЗИ, но является обязательным при обновлении. При установке без использования кода технической поддержки его необходимо ввести в процессе эксплуатации СЗИ (см. «О программе»).

Для продолжения установки нажать кнопку «Далее».

4. В том случае, когда необходимо ввести компьютер в ДБ в процессе установки системы, необходимо поставить флаг «Ввести компьютер в домен безопасности» и заполнить поля подключения (см. «Ввод клиента в ДБ в процессе установки Dallas Lock 8.0»). Если этого не сделать на этапе установки, то компьютер не будет введен в ДБ, но это можно будет сделать и после установки СЗИ.

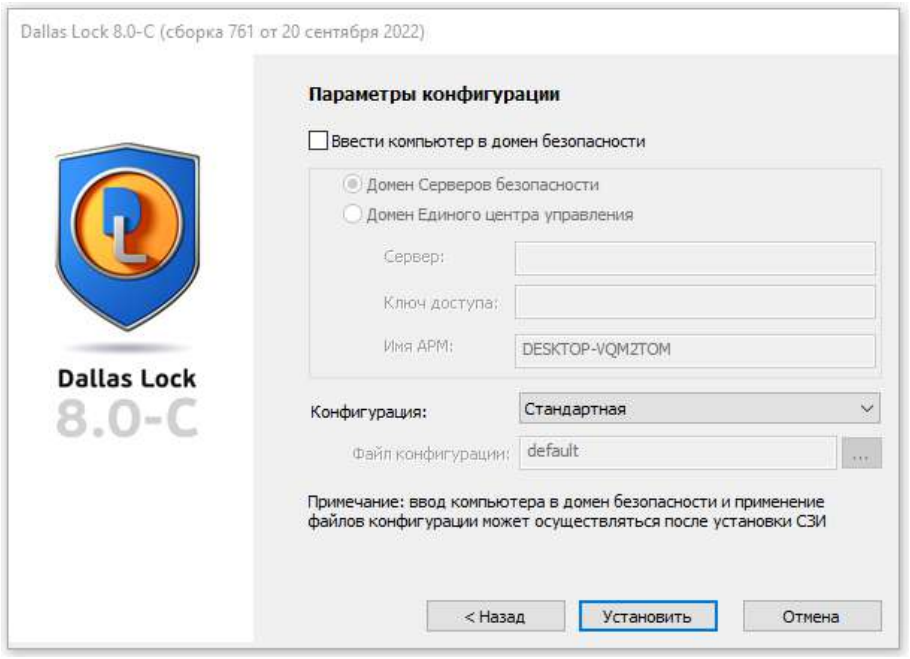


Рис. 4. Введение в ДБ на этапе установки

5. Опционально указать файл конфигурации (рис. 5, рис. 6). В выпадающем списке содержатся пункты:
   - «Стандартная»;
   - «Базовая для 1Г» — устанавливаются параметры для АС, соответствующие требованиям

к АС класса защищенности 1Г[5];

– «Базовая для 1Б» (только для Dallas Lock 8.0 редакции «С») — устанавливаются параметры для АС, соответствующие требованиям к АС класса защищенности 1Б[5];
– «Указать файл…».

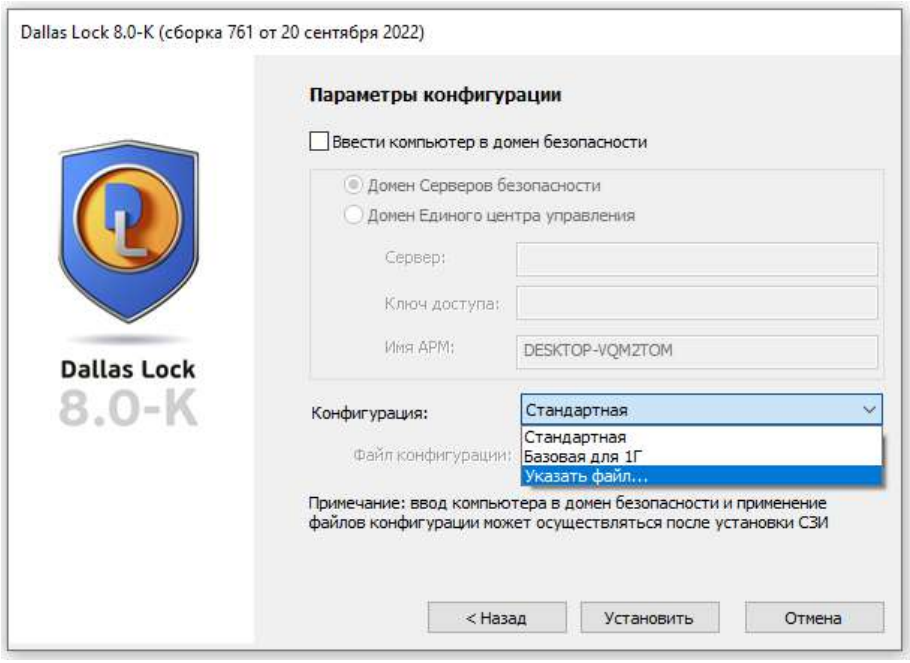


Рис. 5. Указание файла конфигурации для Dallas Lock 8.0-K

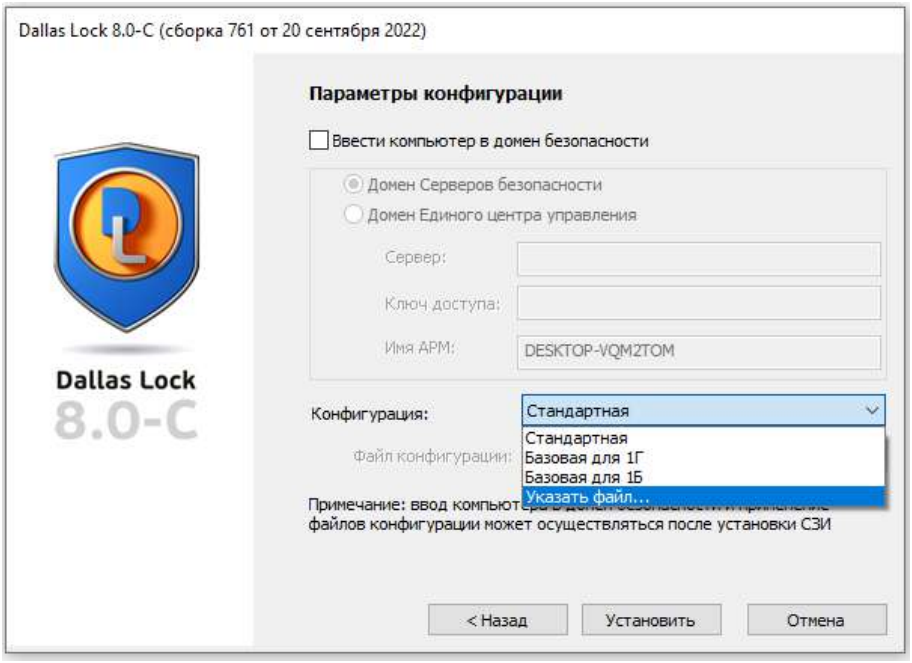


Рис. 6. Указание файла конфигурации для Dallas Lock 8.0-C

Для этого необходимо в выпадающем меню «Конфигурация» выбрать «Указать файл…», нажать кнопку поиска рядом с полем ввода и в появившемся окне проводник выбрать заранее сохраненный файл (см. «Сохранение конфигурации»). Для продолжения установки нажать кнопку «Начать установку».

6. Далее возможно наблюдать за процессом установки. Если процесс прошел без ошибок, то для завершения установки требуется перезагрузка ПК. Через 1 минуту после нажатия кнопки «Перезагрузка» произойдет автоматическая перезагрузка ПК (рис. 7).

[5] В соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992).

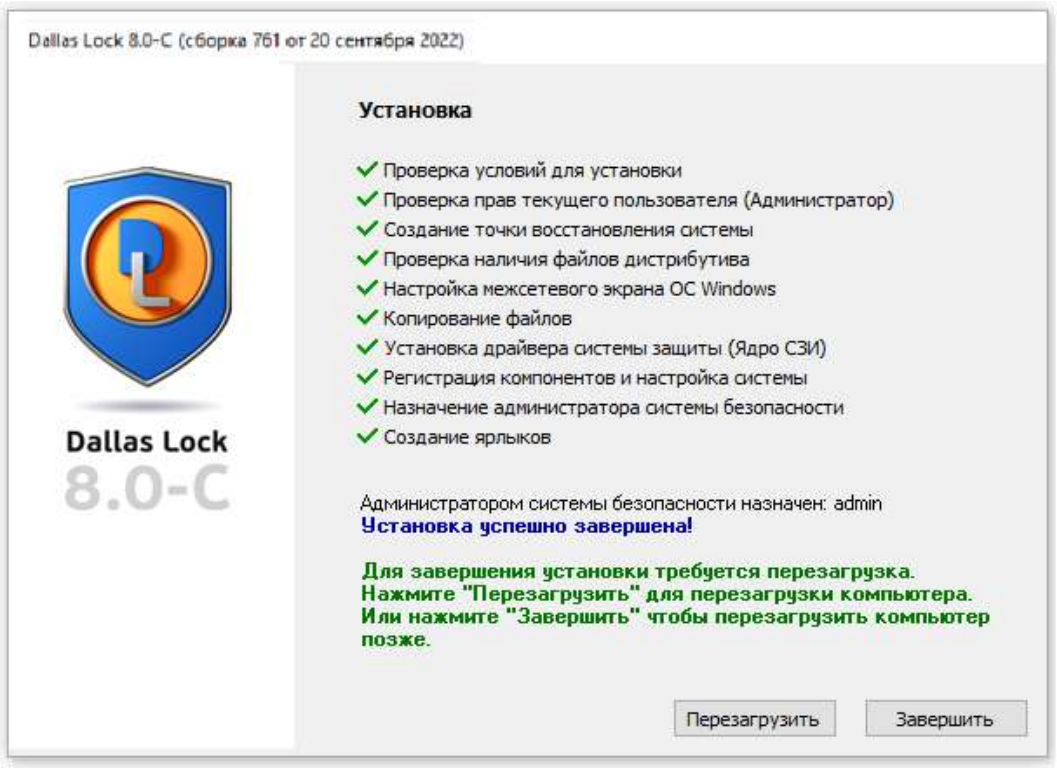


Рис. 7. Завершение установки программы

Примечание. В процессе установки СЗИ Dallas Lock 8.0 автоматически создается точка восстановлении системы.

При возникновении ошибок в создании точки востановления системы (Рис. 8), необходимо включить «Создание точки восстановления системы».

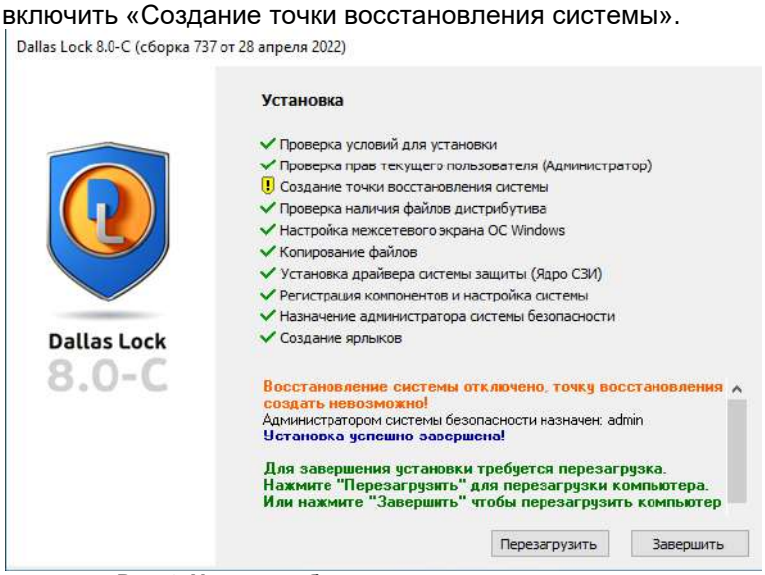


Рис. 8. Установка без точки восстановления системы

Чтобы включить «Создание точки восстановления системы» в Windows 10 откройте «Свойство системы». В разделе «Защита системы», если для системного диска устройства установлено значение «Отключено», нажмите кнопку «Настроить». Выберите опцию «Включить защиту системы». Нажмите «Применить» и «ОК».

При этом установка СЗИ Dallas Lock 8.0 будет завершена успешно, даже без создания точки восстановления системы.

После перезагрузки первый вход на ЗАРМ сможет осуществить пользователь, под учетной записью которого выполнялась установка системы защиты Dallas Lock 8.0. Это может быть локальный пользователь ОС, доменный пользователь, если компьютер является клиентом контроллера домена, или учетная запись Windows Live ID (Windows 8 и выше).

Во время первого входа на ЗАРМ после загрузки ОС появится всплывающее сообщение о том, что данный компьютер защищен СЗИ Dallas Lock 8.0.

После установки системы защиты и перезагрузки компьютера в меню «Пуск» и на рабочем столе

появится ярлык оболочки администратора СЗИ Dallas Lock 8.0.

Рис. 9. Ярлык оболочки администратора Dallas Lock 8.0

2.3 Удаление системы защиты

Право удаления СЗИ может быть установлено для отдельных пользователей или групп пользователей администратором системы защиты. Необходимый параметр «Деактивация системы защиты» находится в категории «Параметры безопасности» → «Права пользователей» (см. «Полномочия пользователей на администрирование системы защиты»), при этом необходимо являться администратором ОС.

Перед удалением системы защиты с ПК рекомендуется сохранить файл конфигурации СЗИ Dallas Lock 8.0 (см. «Сохранение конфигурации»).

Перед удалением системы защиты необходимо завершить работу всех приложений и сохранить результаты, так как удаление Dallas Lock 8.0 потребует принудительной перезагрузки компьютера.

Удаление производится с помощью Мастера установок. В разных операционных системах удаление программ может осуществляться по-разному.

В ОС Windows 10 необходимо вызвать пункт «Параметры», выбрать пункт «Приложения». В появившемся окне выделить «Dallas Lock 8.0С»(«Dallas Lock 8.0К»), выбрать действие «Удалить» и подтвердить удаление (рис. 10).

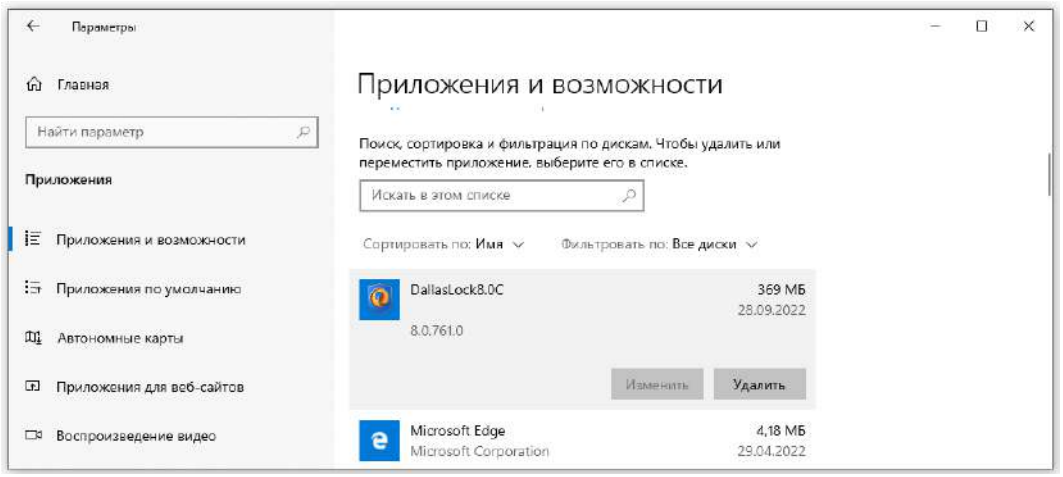


Рис. 10. Удаление Dallas Lock 8.0

После успешного удаления СЗИ Dallas Lock 8.0 появится информационное окно о необходимости перезагрузки ПК. По истечении 1 минуты после нажатия кнопки «Перезагрузка» будет выполнена принудительная перезагрузка ОС компьютера.

Примечание. Удаление\обновление СЗИ Dallas Lock 8.0 при наличии преобразованной зоны невозможно, в таком случае выводятся следующие сообщения:

1. При локальном удалении\обновлении СЗИ Dallas Lock 8.0 выводится сообщение об ошибке с информацией о том, что необходимо удалить преобразованные зоны (Рис. 11).

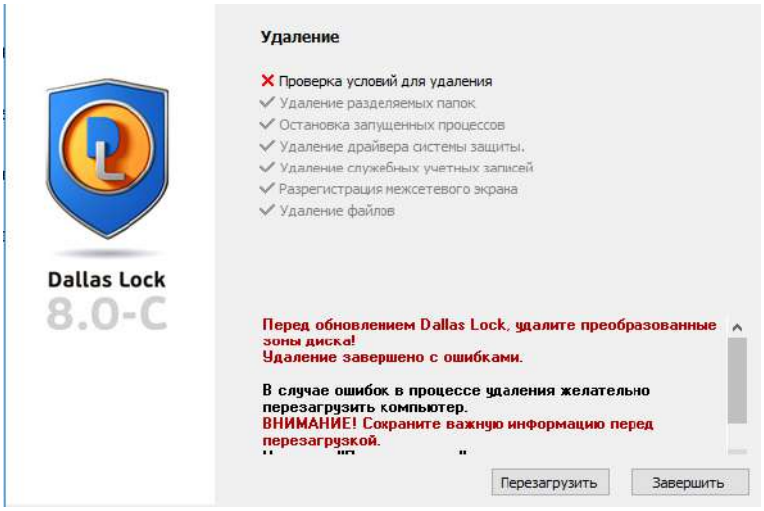


Рис. 11. Удаление Dallas Lock 8.0 с преобразованной зоной

2. При удаленном удалении\обновлении СЗИ Dallas Lock 8.0 для клиента СБ выводится сообщение об ошибке с формулировкой «В процессе установки произошла неисправимая ошибка».

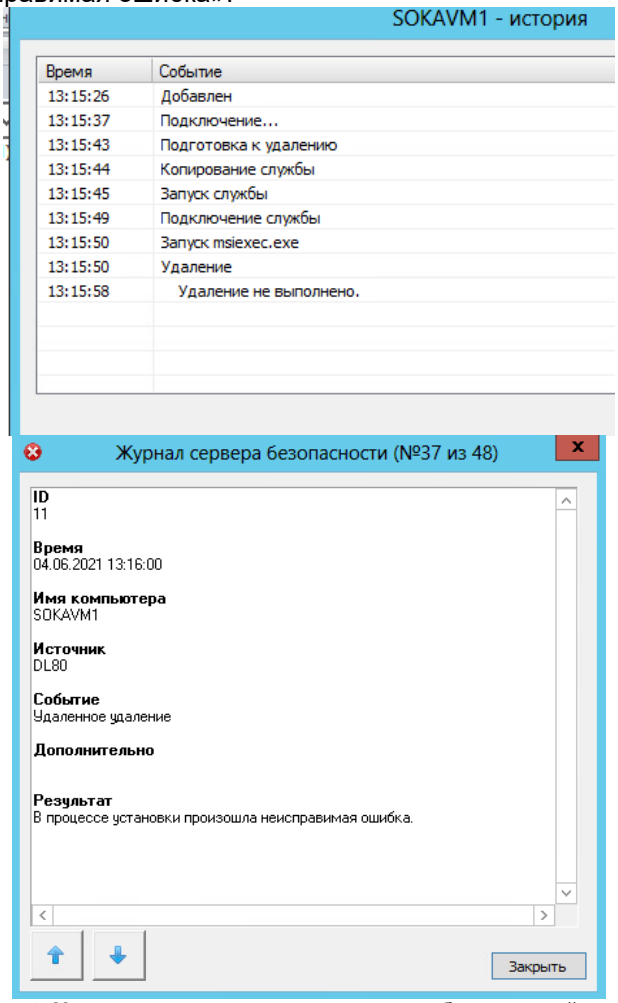


Рис. 12. Удаленное удаление клиента с преобразованной зоной

2.4 Обновление системы защиты

Для защищенных СЗИ Dallas Lock 8.0, а также защищенных более ранними версиями Dallas Lock «7.7» и «7.5» возможно обновление до последней сборки Dallas Lock 8.0, прошедшей испытания с привлечением испытательной лаборатории.

Для локально установленной системы защиты обновление выполняется путем запуска обновленного дистрибутива и заполнения параметров как при установке. Заполнение поля «Код технической поддержки» при обновлении является обязательным.

СЗИ при обновлении автоматически проверяет ЭП исполняемых модулей и запрещает установку исполняемых модулей, не прошедших проверку ЭП.

В процессе обновления автоматически сохраняется и применяется конфигурация уже установленной версии, поэтому путь к файлу конфигурации можно оставить без изменений. Однако дополнительно рекомендуется воспользоваться сохранением конфигурации предыдущей версии СЗИ.

Для клиентов ДБ обновление СЗИ может быть выполнено средствами централизованного управления с СБ (см. «Обновление версий Dallas Lock средствами СБ»).

Примечание. Обновление Dallas Lock на ЗАРМ можно произвести под учетной записью, для которой выполняются следующие условия:

1. Учетная запись, из-под которой производится обновление, должна быть в группе Администраторы ОС ЗАРМ.
2. Учетная запись, из-под которой производится обновление, должна иметь права на удаление Dallas Lock на ЗАРМ. Это настраивается в правах пользователей Dallas Lock, параметр «Деактивация системы защиты». В значение данного параметра прописывается учетная запись, имеющая право на удаление системы защиты (по умолчанию это суперадминистратор ЗАРМ Dallas Lock).

Информация о появлении обновленной версии СЗИ отображается на сайте www.dallaslock.ru.

Также реализован механизм проверки наличия более новых версий Dallas Lock 8.0 с использованием открытого канала связи (протокол http).

Для проверки наличия обновления необходимо выполнить следующие действия:

1. Открыть дополнительные функции кнопки меню оболочки администратора  и нажать кнопку «О программе» (доступно через дополнительное меню всех управляющих приложений: оболочка администратора/Консоль сервера безопасности/Менеджер серверов безопасности).
2. Нажать кнопку «Проверить обновление».
3. Будет произведена проверка наличия обновления. В открывшемся окне будет отображено сообщение о результатах проверки.

Для получения и применения обновления необходимо выполнить действия, изложенные в п. 3.5 Формуляра RU.48957919.501410-02 30.

2.5 О программе

Со следующими сведениями о СЗИ можно ознакомиться в информационном окне «О программе», вызвав его из списка дополнительных функций кнопки главного меню  :

- полное наименование и редакция СЗИ;
- номер и дата сборки;
- номер лицензии;
- код технической поддержки (если он вводится при установке либо в процессе эксплуатации СЗИ);
- дата завершения технической поддержки;
- код информационно-технического сопровождения (см. «Журнал СБ»);
- количество терминальных сессий (см. «Ограничение количества терминальных сессий»);
- активные компоненты (модули, на которые приобретена лицензия);
- адрес сайта компании разработчика;
- адрес сайта СЗИ;
- адрес технической поддержки;
- номер телефона.

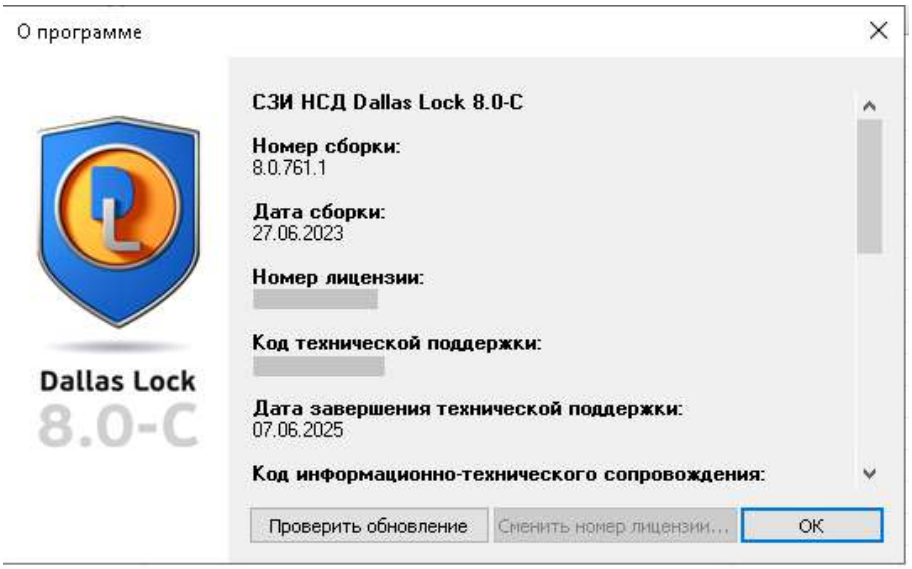


Рис. 13. Окно «О программе»

Процесс обновления СЗИ с помощью кнопки «Проверить обновление» описан в разделе «Обновление системы защиты».

При установке без использования кода технической поддержки его необходимо ввести в процессе эксплуатации СЗИ: нажать кнопку «Сменить номер лицензии» и ввести код технической поддержки, также в появившемся окне можно изменить номер лицензии.

Кнопка смены лицензии будет неактивна в том случае, если клиент централизованно управляется с СБ. В таком случае для смены лицензии необходимо менять номер централизованно средствами Консоли сервера безопасности (далее — КСБ) либо выводить клиента из состава ДБ.

Смену лицензии на клиенте может осуществлять суперадминистратор либо пользователь, которому назначено право «Деактивация системы защиты» (см. «Полномочия пользователей на администрирование системы защиты»). Смена лицензии на КСБ производится пользователем, которому назначена роль «Администратор СБ», либо роль, для которой установлена привилегия «Управление СБ». Для смены лицензии с КСБ на клиентском компьютере пользователю должна быть назначена роль с привилегией «управление режимами работы» (см. «Ролевая модель учетных записей СБ»).

Следует обратить внимание, что при активном модуле «Межсетевой экран» в случае ввода номера лицензии для изделия без модуля «Межсетевой экран» на экран будет выведено предупреждение и соответствующий модуль будет деактивирован.

Действующий код технической поддержки является условием предоставления помощи в установке и настройке СЗИ специалистами компании-разработчика, а также условием доступа к сертифицированным обновлениям.

При завершении срока технической поддержки при запуске модулей администрирования будет появляться предупреждающее сообщение.

2.6 Вход на защищенный компьютер

При загрузке компьютера, защищенного СЗИ Dallas Lock 8.0, в зависимости от ОС, появляется экран приветствия (приглашение на вход в систему) (рис. 14, рис. 15).

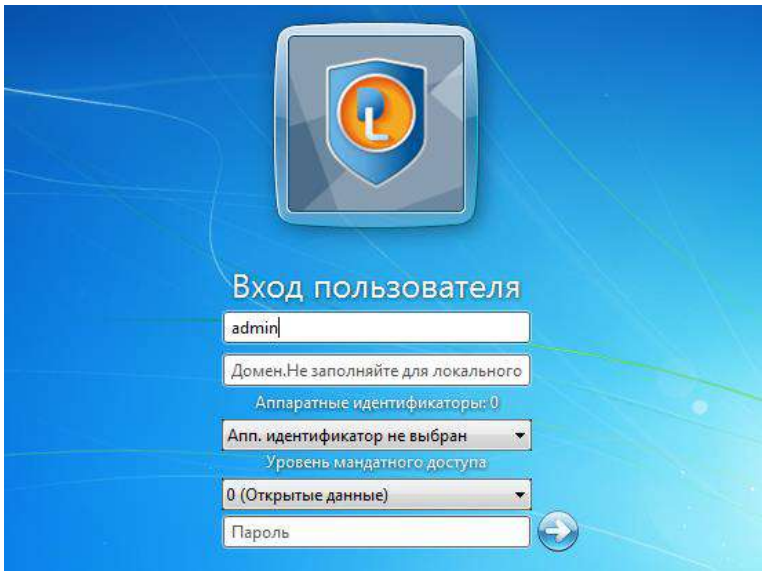


Рис. 14. Экран приветствия в ОС Windows 7

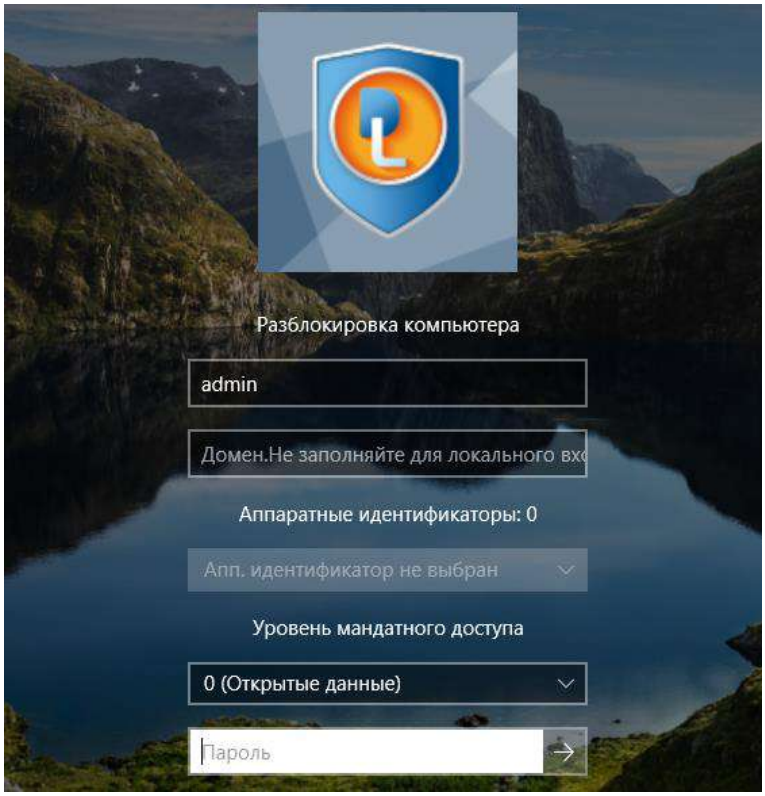


Рис. 15. Экран приветствия в ОС Windows 10

Для входа на защищенный СЗИ Dallas Lock 8.0 компьютер каждому пользователю предлагается выполнить следующую последовательность шагов:

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе. В зависимости от настроек системы защиты в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.
3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить (см. ниже).
4. Выбрать уровень доступа и (или) мандатную метку (если включен параметр «Вход: выбор мандатной метки при входе в ОС»), назначенный пользователю администратором безопасности (только для Dallas Lock 8.0 редакции «С»).
5. Ввести пароль. При вводе пароля поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка).

6. При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
7. Нажать кнопку «Enter».

После нажатия кнопки «Enter» в системе защиты сначала проверяется возможность входа пользователя с данным именем и доменом, после чего проверяется соответствие с именем пользователя номера аппаратного идентификатора, зарегистрированного в системе защиты, и правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход в систему, иначе вход в систему пользователю запрещается.

Примечание. При вводе имени и пароля переключение раскладки клавиатуры (русская/латинская) производится нажатием комбинации клавиш, установленной при настройке свойств клавиатуры. Текущий язык отображается индикатором клавиатуры.

Во время первого входа на ПК после установки или обновления Dallas Lock 8.0 в области уведомлений Windows будет появляться сообщение о том, что ПК защищен Dallas Lock 8.0.

2.6.1 Вход с использованием смарт-карт с сертификатом УЦ Windows

Для возможности входа на защищенный системой защиты Dallas Lock 8.0 компьютер при помощи смарт-карт, через удостоверяющий центр MS Windows, необходимо соблюдение следующих условий:

- компьютер, на который осуществляется вход, должен быть введен в доменную сеть Windows и находиться под управлением AD;
- включена политика Dallas Lock 8.0 «Вход: разрешить использование смарт-карт».

Если все условия соблюдены, экран приветствия будет содержать отдельную опцию, позволяющую войти в ОС с использованием смарт-карт.

Для перехода к выбору входа по смарт-карте в ОС Windows 7 необходимо на экране приветствия нажать кнопку «Сменить пользователя», после чего появится возможность выбрать тип входа (рис. 16).

Рис. 16. Выбор типа входа в ОС Windows 7

В ОС Windows 10 выбор типа входа отобразится внизу экрана слева (рис. 17).

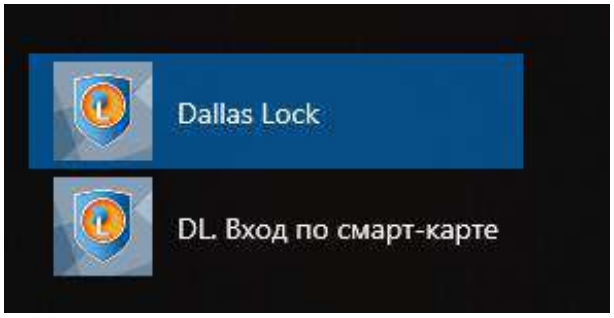


Рис. 17. Выбор типа входа в ОС Windows 10

При выборе входа по смарт-карте необходимо вставить смарт-карту в считывающее устройство, ввести PIN-код и нажать кнопку «Enter» (рис. 18).

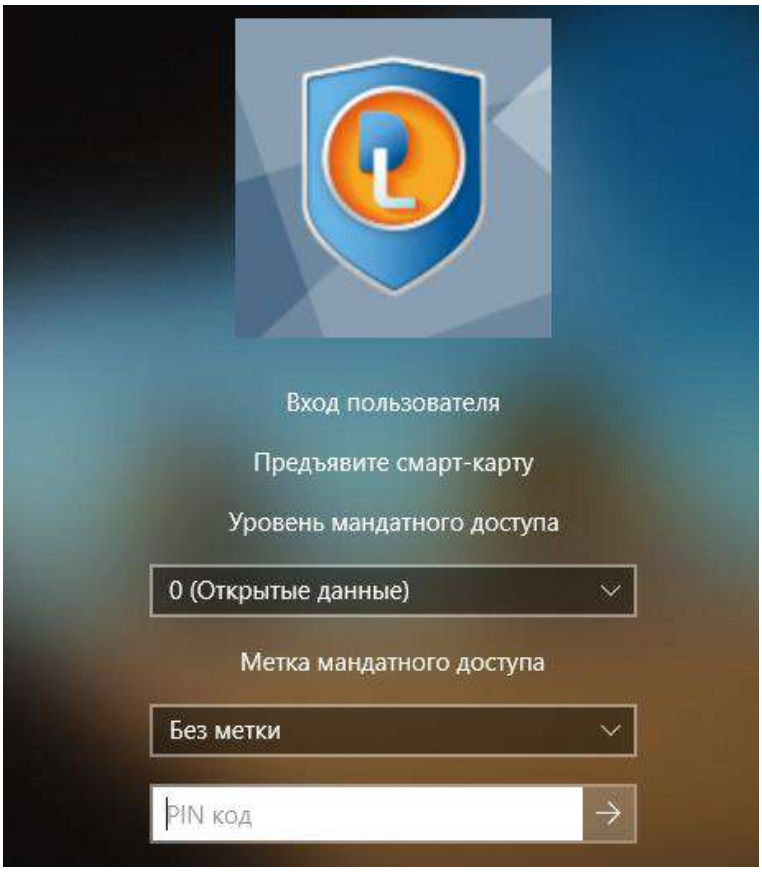


Рис. 18. Экран входа по смарт-карте в ОС Windows 10

2.6.2 Вход с аппаратным идентификатором

Если пользователю в процессе работы назначен аппаратный идентификатор, то, для того, чтобы его предъявить, необходимо выполнить следующие шаги:

1. В зависимости от типа устройства предъявить идентификатор можно, вставив его в USB-порт или прикоснувшись к считывателю.
2. Необходимо выбрать наименование идентификатора из списка, который появится в выпадающем меню в поле «Аппаратные идентификаторы» (рис. 19).

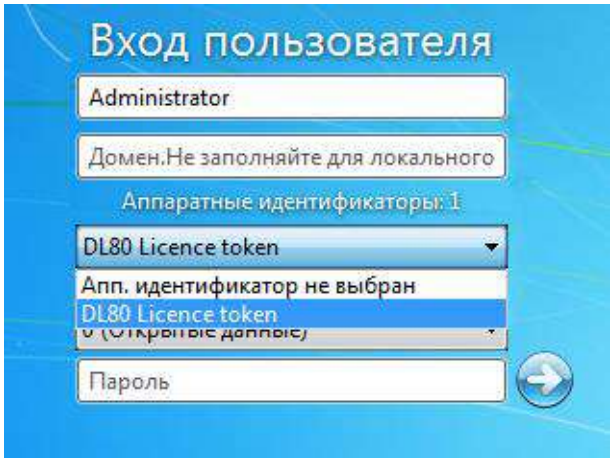


Рис. 19. Выбор аппаратного идентификатора при входе в ОС Windows

При подключении единственного идентификатора он будет выбран автоматически.

3. Далее в зависимости от настроек, произведенных администратором безопасности применительно к учетной записи пользователя, возможны следующие способы авторизации:
   - выбор аппаратного идентификатора и заполнение всех авторизационных полей формы[6]

[6] Для Dallas Lock 8.0 редакции «С» выбор мандатного уровня останется обязательным при любом способе авторизации. Для Dallas Lock 8.0 редакции «К» данные поля отображаться не будут.

(рис. 20);

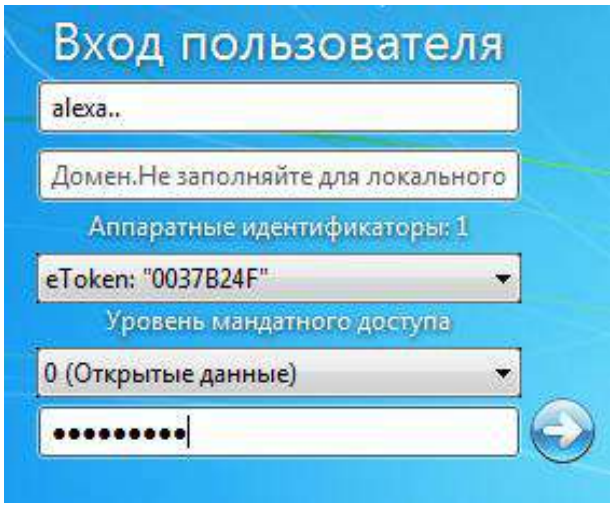


Рис. 20. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (рис. 21);

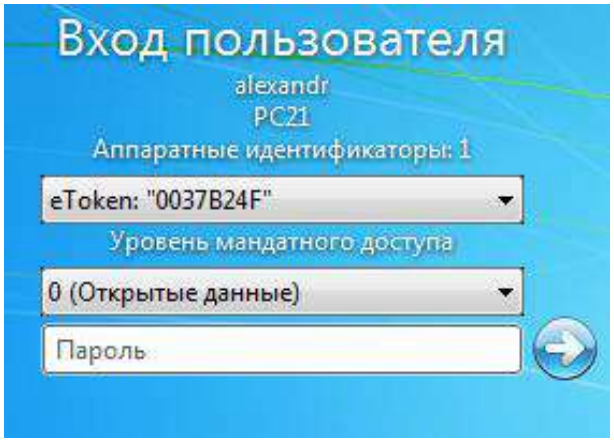


Рис. 21. Поля авторизации после предъявления идентификатора

- выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 22);

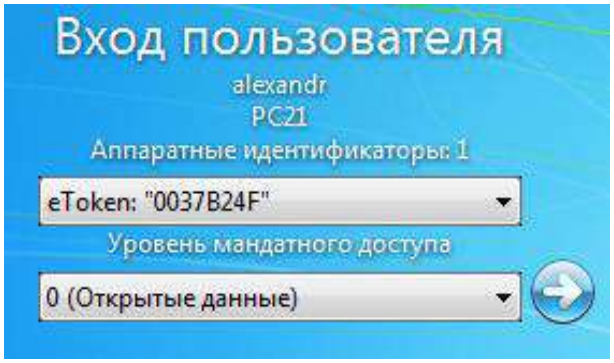


Рис. 22. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 23).

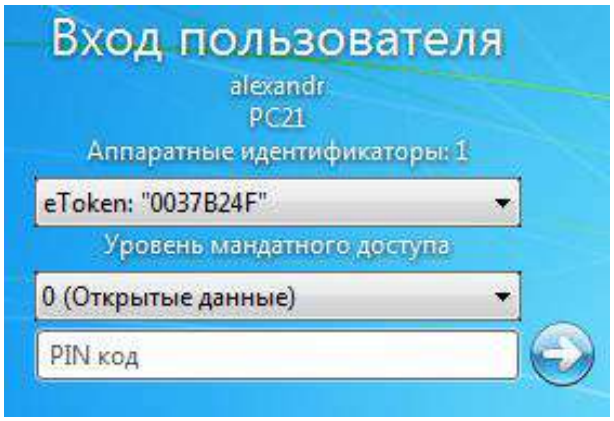


Рис. 23. Поля авторизации после предъявления идентификатора

При использовании идентификаторов типа USB-ключи и смарт-карты JaCarta PKI/BIO, в память которых записана биометрическая информация (см. «Запись биометрических данных в идентификатор»), возможны следующие способы авторизации в зависимости от произведенных администратором безопасности настроек:

- ввод PIN-кода и биометрических данных (рис. 24);

Рис. 24. Ввод авторизационных данных (PIN-код и биометрия)

- ввод PIN-кода или биометрических данных (рис. 25);

Рис. 25. Ввод авторизационных данных (PIN-код или биометрия)

- ввод только биометрических данных (рис. 26).

Рис. 26. Ввод авторизационных данных (биометрия)

2.6.3 Ограничение количества терминальных сессий

СЗИ Dallas Lock 8.0 позволяет осуществлять полноценную защиту терминального сервера, предоставляющего вычислительные ресурсы терминальным клиентам.

По умолчанию после установки Dallas Lock 8.0 ограничивает число разрешенных терминальных подключений до двух.

Администратор безопасности может увеличить количество разрешенных терминальных подключений. Для этого необходимо иметь специальный аппаратный ключ (eToken или Рутокен (Rutoken)), содержащий значение максимального количества терминальных подключений, который необходимо предъявить на терминальном сервере. Чтобы предъявить аппаратный ключ, необходимо установить на ПК его драйвер и вставить устройство в USB-разъем.

При попытке подключения клиента к терминальному серверу осуществляется проверка числа доступных терминальных подключений. Если подключение приведет к превышению максимально возможного количества терминальных сессий, то оно будет заблокировано, а пользователю

выведется сообщение об ошибке.

Допустимое количество терминальных сессий можно посмотреть в информационном окне «О программе», вызвав его из списка дополнительных функций кнопки главного меню  , а также в любом сформированном отчете.

При использовании Сервера лицензий (далее — СЛ) количество терминальных сессий становится условно неограниченным (подробнее об использовании СЛ см. в документе «Инструкция по использованию сервера лицензий» RU.48957919.501410-02 И2).

Общее количество терминальных подключений ограничивается соответствующим ограничением сконфигурированного СЛ. Общее количество терминальных подключений ограничивается записью в аппаратном ключе, подключенном к СЛ (должен быть подключен к СЛ постоянно).

Стандартным сценарием работы в связке «терминальный сервер — СЛ» является следующая последовательность действий:

- при попытке начать новое терминальное подключение терминальный сервер отправляет на СЛ запрос;
- СЛ получает запрос и проверяет, не превышает ли общее число терминальных подключений допустимого значения, после чего возвращает на терминальный сервер ответ;
- при создании терминального подключения, если у СЛ есть свободные лицензии на терминальные подключения, СЛ разрешает терминальное подключение путем выдачи терминальному серверу одной лицензии данного типа;
- при завершении подключения лицензия на терминальное подключение возвращается СЛ;
- при выключении терминальный сервер отправляет на СЛ запрос, чтобы СЛ мог освободить занятые терминальным сервером подключения.

Так как ограничение становится динамическим и накладывается СЛ, в окне «О программе» (максимальное) количество терминальных сессий при использовании СЛ посмотреть будет невозможно.

Работа на защищенном СЗИ терминальном сервере с терминальных клиентов, в том числе аппаратная идентификация с терминальных клиентов, производится в соответствии с выполненными настройками в СЗИ.

3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ

СЗИ Dallas Lock 8.0 состоит из следующих программных модулей:

Название	Ярлык программы
Dallas Lock 8.0	
Сервер безопасности Dallas Lock 8.0	**Является службой ОС Windows и взаимодействует с Консолью Сервера безопасности**
Консоль сервера безопасности Dallas Lock 8.0	
Менеджер серверов безопасности Dallas Lock 8.0	

Для локальной настройки политик безопасности используется оболочка администратора СЗИ Dallas Lock 8.0 или контекстное меню объекта Windows Explorer. Для удаленной настройки используется оболочка сетевого администратора (см. «Сетевое администрирование») или КСБ в режиме ОУ.

Глобальные настройки для компьютеров в составе ДБ осуществляются с СБ средствами КСБ или МСБ.

3.1 Администрирование Dallas Lock

Администрирование локально установленной СЗИ Dallas Lock 8.0 осуществляется из окна программы администрирования (оболочки администратора или Admshell). Вызов программы производится двойным щелчком мыши по ярлыку, появившемуся на рабочем столе или в меню «Пуск» после установки Dallas Lock 8.0 (рис. 27).

Рис. 27. Значок ярлыка программы на рабочем столе

Оболочка администратора позволяет настроить систему защиты в соответствии с необходимыми требованиями, управлять работой пользователей, управлять параметрами аудита событий, происходящих в системе, просматривать журналы событий.

Главное окно программы содержит следующие рабочие области (рис. 28).

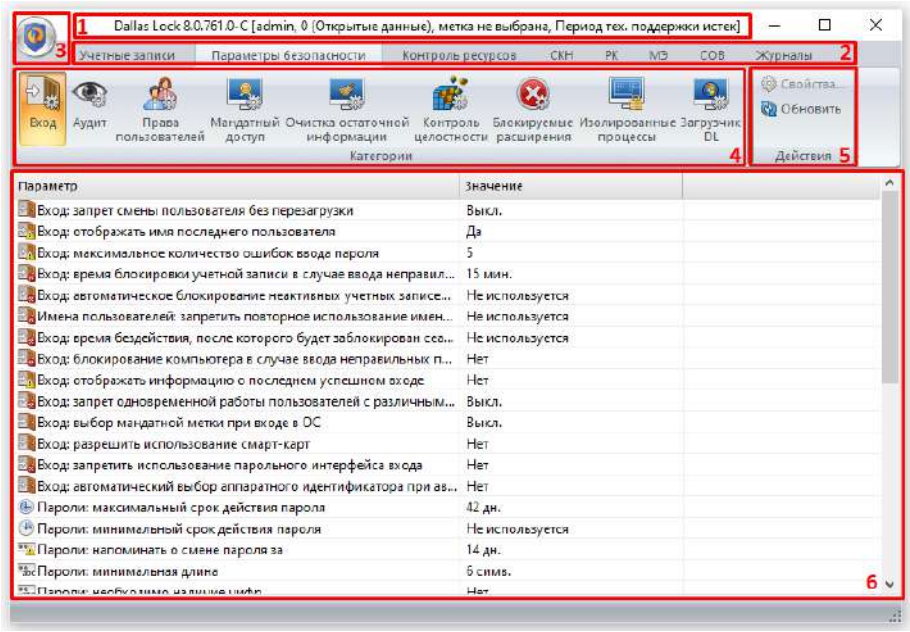


Рис. 28. Окно оболочки администратора системы защиты

1. Заголовок окна (верхняя строка), содержащий имя системы защиты, имя учетной записи, от которой открыта оболочка администратора, уровень текущего доступа пользователя и сведения о сроке технической поддержки.
2. Основное меню с набором вкладок.
3. Управляющая кнопка основного меню для вызова дополнительных функций  .
4. Меню с категориями текущей вкладки и панелью инструментов (действий).
5. Панель действий, позволяющая производить настройку параметров.
6. Рабочая область, содержащая списки параметров или объектов текущей категории.

Доступны следующие вкладки.

Учетные записи
Вкладка позволяет управлять учетными записями пользователей, создавать локальные группы и включать в них пользователей, просматривать список сессий (сеансов) учетных записей на данном ПК, контролировать список сессий-исключений, а также управлять списком заблокированных пользователей и определять принадлежность аппаратных идентификаторов.
Параметры безопасности
Вкладка позволяет осуществить настройку системы защиты в соответствии с требованиями. Вкладка содержит следующие категории: • **«Вход»** — (политики входа) позволяет регулировать все настройки по входу на ЗАРМ и загрузке ОС. Эти настройки распространяются на всех зарегистрированных в системе защиты пользователей. • **«Аудит»** — (политики аудита) позволяет включать/отключать контроль за определенными действиями пользователей. Этот параметр регулирует ведение журналов. • **«Права пользователей»** — (политики прав пользователей) позволяет присваивать права конкретному пользователю или группе пользователей. • **«Мандатный доступ»** — позволяет переименовывать имеющиеся уровни доступа, а также создавать и переименовывать мандатные метки (только для Dallas Lock 8.0 редакции «С»). • **«Очистка остаточной информации»** — настройка параметров очистки. • **«Контроль целостности»** — позволяет управлять проверкой установленной целостности объектов ФС, программно-аппаратной среды и веток реестра. • **«Блокируемые расширения»** — позволяет управлять списком расширений, работа с которыми будет блокирована. • **«Изолированные процессы»** — позволяет управлять списком процессов, работа с

которыми должна быть изолирована, исключить возможность копирования информации через буфер обмена.
- **«Загрузчик DL»** — позволяет настраивать модуль загрузчика DL и управлять прозрачным преобразованием жестких дисков (только для Dallas Lock 8.0 редакции «С»).

Контроль ресурсов

Вкладка позволяет контролировать объекты ФС и устройства, для которых установлены механизмы разграничения доступа, аудита и целостности. Данная вкладка позволяет управлять следующими типами ресурсов:
- **«Все»** — позволяет получить список всех объектов ФС, на которые назначены какие-либо права Dallas Lock 8.0 по доступу (дискреционному и мандатному), аудиту и контролю целостности.
- **«Глобальные»** — содержит фиксированный список мета-объектов ФС, для которых устанавливаются права дискреционного доступа и аудит.
- **«ФС»** — содержит управляемый список объектов ФС, для которых устанавливаются права доступа (дискреционного и мандатного), аудит и контроль целостности.
- **«Реестр»** — содержит управляемый список объектов реестра, для которых устанавливаются права дискреционного доступа, аудита и контроля целостности.
- **«Аппаратные идентификаторы»** — содержит управляемый список аппаратных идентификаторов, для которых устанавливаются права дискреционного доступа.
- **«Устройства»** — позволяет просматривать проводник устройств и классов устройств в виде дерева объектов и управлять разграничением доступа (дискреционного и мандатного), а также назначать аудит.

Также на данной вкладке для каждого типа ресурсов возможно выбрать определенный фильтр по типу контроля объектов:
- **«Дискреционный доступ»** — позволяет просмотреть список объектов ФС, на которые назначены права дискреционного доступа. В свойствах каждого объекта можно просмотреть, для каких пользователей или групп какие права назначены. Фильтр доступен для всех типов ресурсов.
- **«Мандатный доступ»** — позволяет просмотреть список объектов ФС, на которые назначен мандатный доступ (только для Dallas Lock 8.0 редакции «С»). Фильтр доступен для типов ресурсов «ФС» и «Устройства».
- **«Аудит»** — позволяет просмотреть список объектов ФС, на которые назначен аудит. В свойствах объектов из списка можно просмотреть, на какие конкретно события назначен аудит. Фильтр доступен для всех типов ресурсов, кроме аппаратных идентификаторов.
- **«Контроль целостности»** — позволяет просмотреть список объектов ФС, на которые установлен контроль целостности. Отображается также алгоритм расчета. При нажатии кнопки «Проверить» отображается эталонная контрольная сумма, хранимая в базе данных СЗИ. При нажатии «Пересчитать» — расчетная. Фильтр доступен для типов ресурсов «ФС» и «Реестр».

СКН

Вкладка (только в Dallas Lock 8.0 с модулем СКН) позволяет управлять и преобразовывать сменные накопители. Эта вкладка содержит следующие категории:
- **Сменные накопители** — позволяет управлять дескрипторами на сменных накопителях (права доступа, аудит и контроль целостности для сменных накопителей выделены в отдельную категорию).
- **Описание для сменных накопителей** — описание задается для удобства администрирования.
- **Преобразование сменных накопителей** — позволяет управлять ключами преобразования и преобразовывать сменные накопители.

РК

Вкладка позволяет управлять созданием резервных копий и восстановлением файлов из них.
В категории «Задания» отображаются все созданные задания на резервное копирование и их статус.

МЭ

Вкладка (только в Dallas Lock 8.0 с модулем МЭ) позволяет настраивать правила фильтрации сетевого трафика, отображает сетевую статистику и текущие сетевые соединения. Эта вкладка содержит следующие категории:

- **«Адреса»** — содержит список текущих сетевых адресов ПК.
- **«Сетевые профили»** — позволяет управлять применением правил МЭ и фильтрации в зависимости от параметров сети, через которую получен сетевой пакет.
- **«Соединения»** — содержит дерево текущих процессов в ОС, участвующих в сетевой передаче информации. Для каждого процесса в выпадающем списке отображаются сетевые подключения и их детали — номера портов, состояние подключения, протоколы передачи данных, локальный адрес и др.
- **«Параметры»** — позволяет управлять основными параметрами МЭ.
- **«Правила МЭ»** — позволяет управлять правилами фильтрации сетевого трафика. По умолчанию содержит готовые шаблоны наиболее типовых сетевых правил, присутствует возможность включать только определенные правила или добавлять собственные.
- **«Профили МЭ»** — позволяет настраивать динамическое управление правилами МЭ в совокупности в зависимости от текущего состояния системы.
- **«Фильтрация» —** позволяет управлять настройками фильтрации МЭ.
- **«Статистика МЭ»** — позволяет просмотреть сетевую статистику по различным параметрам: весь сетевой трафик за различные периоды, статистика по процессам и по пользователям.
- **«Отключить (Запустить) МЭ»** — позволяет отключить (включить) модуль межсетевого экрана.

СОВ

Вкладка (только в Dallas Lock 8.0 с модулем СОВ) позволяет настраивать собственные сигнатуры, блокировать атакующего, отображает информацию и настройку СОВ. Эта вкладка содержит следующие категории.

- **«Основное»** — позволяет просмотреть версию обновления базы решающих правил. Также отображает статистику сетевых атак, сигнатур журналов, сигнатур трафика и портов.
- **«Сигнатуры»** — позволяет управлять сигнатурами. По умолчанию содержит готовые шаблоны наиболее типовых сигнатур, присутствует возможность включать определенные сигнатуры или добавлять собственные.
- **«Блокировки»** — позволяет блокировать IP-адреса и отображает заблокированные IP-адреса. Также позволяет добавлять «Доверенные» IP-адреса.
- **«Параметры СОВ»** — позволяет назначать электронную подпись доверенным приложениям, контролировать ключи реестра, производить настройку эвристики, а также отключать модуль СОВ.
- **«Безопасная среда СОВ»** — позволяет управлять настройками безопасной среды СОВ (песочницы).

Журналы

Вкладка служит для работы с журналами: просмотра, сортировки, фильтрации, группировки, архивации, экспорта записей. Вкладка «Журналы» содержит следующие категории:

- **«Журнал входов»** — просмотр событий, связанных с загрузкой ПК и входом в ОС.
- **«Журнал управления учетными записями»** — просмотр событий учета действий по изменению учетных записей пользователей.
- **«Журнал ресурсов»** — просмотр событий доступа к объектам и событий очистки остаточной информации.
- **«Журнал печати»** — просмотр событий, связанных с распечаткой документов.
- **«Журнал управления политиками»** — просмотр всех событий по настройке параметров системы защиты, событий по запуску/завершению работы системы «защиты и событий запуска модулей администрирования.
- **«Журнал процессов»** — просмотр событий запуска и завершения процессов.
- **«Журнал резервного копирования»** — просмотр событий, связанных с резервным копированием.
- **«Журнал пакетов МЭ»** — в журнал заносятся все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера.
- **«Журнал соединений МЭ»** — в журнал заносятся сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами.
- **«Журнал трафика»** — в журнал заносятся все события, связанные с проходящим сетевым трафиком через контролируемые узлы сети.
- **«Журнал событий ОС»** — в журнал заносятся сведения о важных событиях безопасности, генерируемые ОС.
- **«Журнал контроля приложений»** — в журнал заносятся сведения о важных событиях безопасности, генерируемые запущенными приложениями.
- **«Журнал из файла»** — открытие и просмотр архивированных журналов.

Для удобства настройки параметры безопасности в оболочке администратора имеют всплывающие подсказки с кратким описанием функциональных возможностей.

3.2 Панель действий

Панель инструментов (действий) в СЗИ Dallas Lock 8.0 для всех категорий содержит набор типовых действий по добавлению, удалению, редактированию, обновлению параметров и другие (рис. 29).

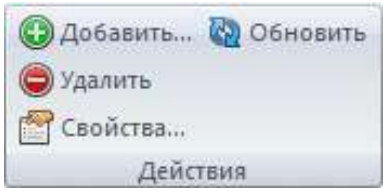


Рис. 29. Панель инструментов

Примечание. Изменение настроек параметров различных категорий возможно несколькими способами: двойным кликом выделенного параметра, с помощью кнопки «Свойства» на панели действий или с помощью контекстного меню параметра, вызываемого правой кнопкой мыши.

3.3 Контекстное меню объектов

СЗИ Dallas Lock 8.0 предоставляет возможность управлять безопасностью любого объекта ФС. После установки системы защиты у каждого объекта ФС в контекстном меню появляются дополнительные пункты: «DL8.0: Права доступа», «DL8.0: Преобразования», «DL8.0: Удалить и зачистить» (рис. 30), подробный механизм каждого из которых описан в соответствующих разделах данного руководства.

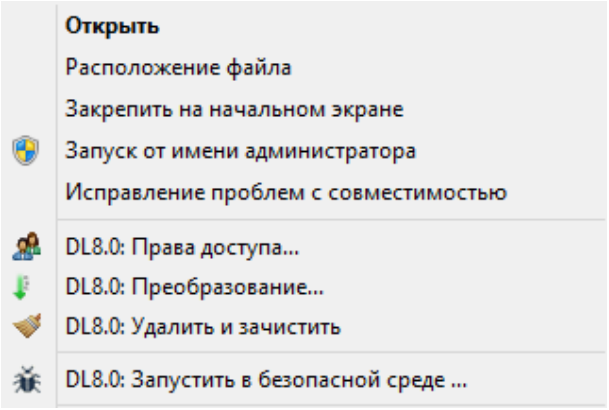


Рис. 30. Контекстное меню объекта ФС

Примечание. Для таких объектов как преобразованные файл-диски, в контекстном меню дополнительно будет присутствовать пункт «DL8.0: Подключить преобразованный файл-диск» (см. «Преобразованные файл-диски»).

3.4 Сортировка списка параметров

Каждая рабочая область любой категории параметров содержит списки параметров или объектов текущей категории. Для удобства работы эти списки можно отсортировать, для чего необходимо кликнуть поле, содержащее название столбца и значок сортировки (треугольник) (рис. 31).

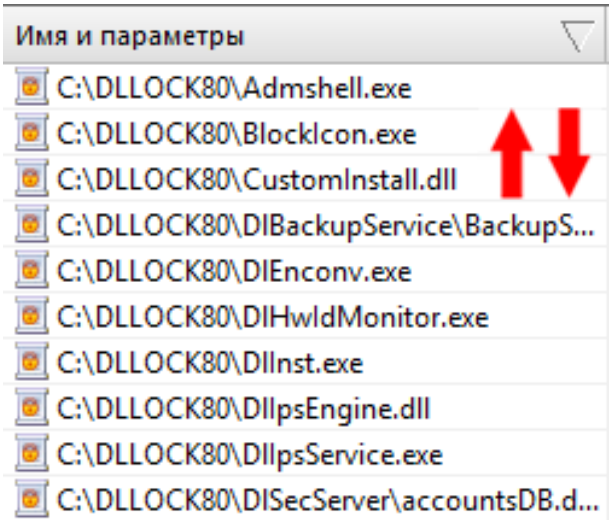


Рис. 31. Сортировка списка параметров

Порядок сортировки параметров в зависимости от типа объектов может быть следующим:

1. Лексикографический порядок (сортировка названий параметров по алфавиту).
2. Алгебраический (в порядке возрастания/убывания численных значений). Например, сортировка записей в журнале процессов по ID процесса.
3. Хронологический (сортировка по дате и времени). Сортировка относится к записям в журналах.

Сортировка может быть выполнена как по возрастанию (прямая сортировка), так и по убыванию (обратная сортировка).

Для некоторых параметров на рабочей области реализована функция поиска по столбцам (рис. 32).

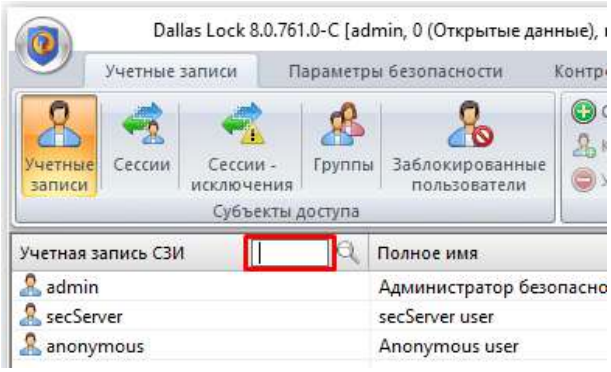


Рис. 32. Поиск значения в столбце

3.5 Значок блокировки на панели задач

После установки СЗИ Dallas Lock 8.0 на панели задач ОС у всех пользователей ЗАРМ присутствует значок блокировки компьютера «BlockIcon» (рис. 33).

Двойное нажатие по этому значку позволит пользователю временно заблокировать компьютер. Разблокировка может быть произведена только пользователем, заблокировавшим компьютер.

Также у этого значка есть контекстное меню, из которого можно запустить оболочку администратора, просмотреть свойства текущего пользователя и выполнить действия с преобразованными файл-дисками (рис. 33).

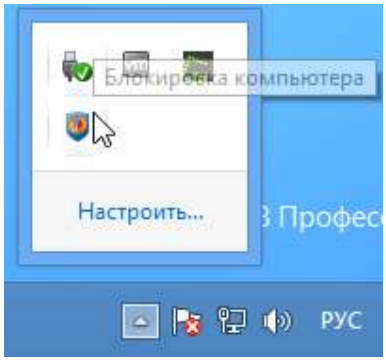


Рис. 33. Контекстное меню значка блокировки

Выбор свойств пользователя из контекстного меню откроет окно с информацией о текущем пользователе компьютера (рис. 34).

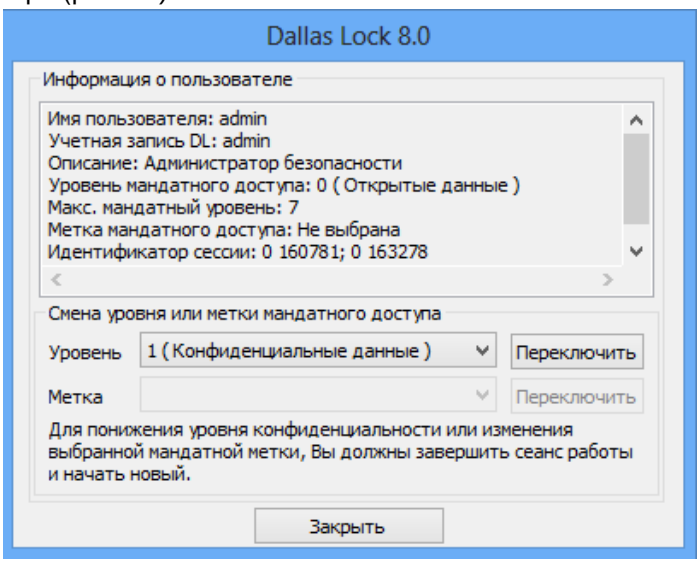


Рис. 34. Окно свойств пользователя, вызванное с помощью значка блокировки

В Dallas Lock 8.0 редакции «С» с помощью данного окна текущему пользователю можно повысить уровень мандатного доступа (см. «Текущий уровень и метка доступа пользователя»).

3.6 Полномочия пользователей на администрирование системы защиты

В СЗИ Dallas Lock 8.0 полномочия на эксплуатацию и администрирование системы защиты определяются статусом пользователя.

В зависимости от предоставленных полномочий, каждый пользователь может быть отнесен к одной из трех категорий:

- **Администратор безопасности (администратор)** — пользователь, наделенный всеми полномочиями на администрирование системы защиты. Администраторов безопасности может быть несколько.
- **Привилегированный пользователь** — наделенный некоторыми полномочиями на администрирование системы защиты.
- **Рядовой пользователь** — не имеющий полномочий на администрирование системы защиты, но в соответствии с политиками безопасности имеющий возможность выполнения некоторых операций (осуществление входа/выхода, преобразования объектов ФС и прочие).

Отдельно выделяется учетная запись пользователя, выполнившего установку системы Dallas Lock 8.0. Этот пользователь условно называется **суперадминистратором**, имеет неограниченные административные права и возможности в настройке системы.

Суперадминистратор регистрирует в системе защиты других пользователей. При этом он может делегировать зарегистрированному пользователю все или часть своих полномочий на администрирование.

Полномочия администратора по управлению работой системы защиты могут быть следующими:

- управление регистрацией субъектов доступа:
  - создание, регистрация и удаление учетных записей;
  - создание и управление составом групп пользователей;
  - управление списком сессий-исключений;
- изменение свойств пользователей:
  - первичные учетные данные (логин, имя, описание);
  - параметры загрузки;
  - назначение аппаратного идентификатора;
  - порядок изменения пароля;
- управление аудитом (доступом к журналам, к теневым копиям распечатываемых документов, к теневым копиям файлов);
- управление параметрами безопасности;
- управление работой пользователей (изменение его прав);
- управление ресурсами дискреционного, мандатного доступов и контролем целостности;
- удаление системы защиты.

3.6.1 Порядок предоставления полномочий

Для того, чтобы некоторый пользователь N имел возможность предоставлять другим пользователям полномочия на администрирование системы защиты, необходимо соблюдение двух условий:

1. Пользователь N должен быть наделен полномочием на изменение параметров безопасности.
2. Пользователь N должен сам обладать тем полномочием, которое хочет предоставить другим пользователям.

В системе защиты реализован механизм контроля за распространением полномочий. Осуществление этого контроля позволяет пользователю предоставлять другим пользователям только те полномочия, которыми он наделен сам. Например, если пользователь не наделен полномочием на управление аудитом, то и никакому другому пользователю он не сумеет предоставить это полномочие.

При попытке предоставить другому пользователю полномочие, которым данный пользователь сам не обладает, система защиты выведет предупреждение. Пользователь не сможет назначить сам себе дополнительное полномочие, повысить уровень доступа, включить себя в группу, обладающую расширенными по сравнению с данным пользователем правами.

Внимание! Назначать параметры и права следует очень внимательно. Если при предоставлении любого полномочия выбрать группу «Все», то данным полномочием будут обладать все пользователи, в том числе и тот пользователь, который установил данный параметр. Так, например, если администратор при запрете локального (интерактивного) входа в ОС выберет группу «Все», то сам он также не сможет больше осуществить вход в ОС. Исключение будет составлять только учетная запись суперадминистратора.

Также следует учесть, что пользователь, обладающий полномочием на редактирование параметров безопасности, может лишить любых пользователей любых полномочий, даже тех, которыми он сам не обладает. Если пользователь сам себя лишил какого-либо полномочия, то восстановить это полномочие он не сможет.

Для предоставления пользователю какого-либо полномочия на администрирование необходимо в оболочке администратора на вкладке основного меню «Параметры безопасности» открыть категорию «Права пользователей». Главное окно программы будет иметь следующий вид (рис. 35):

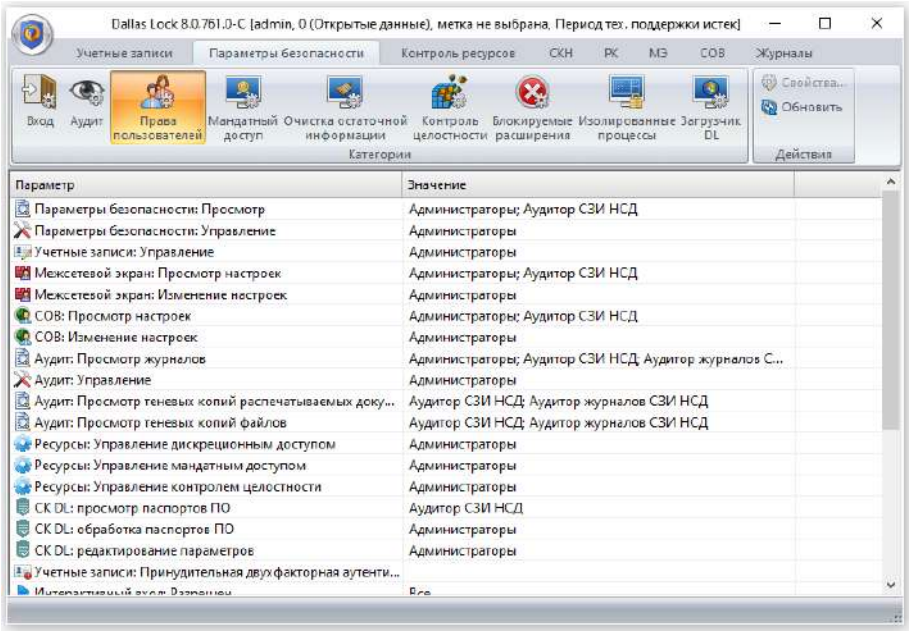


Рис. 35. Окно редактирования прав пользователей на администрирование

В основном окне данной категории перечислены все полномочия, которые могут быть предоставлены пользователям. Чтобы предоставить пользователю необходимое право, нужно дважды щелкнуть на строке с полномочием, либо выделить строку и нажать кнопку «Свойства» на панели «Действия». Откроется окно добавления учетных записей пользователей и групп (рис. 36).

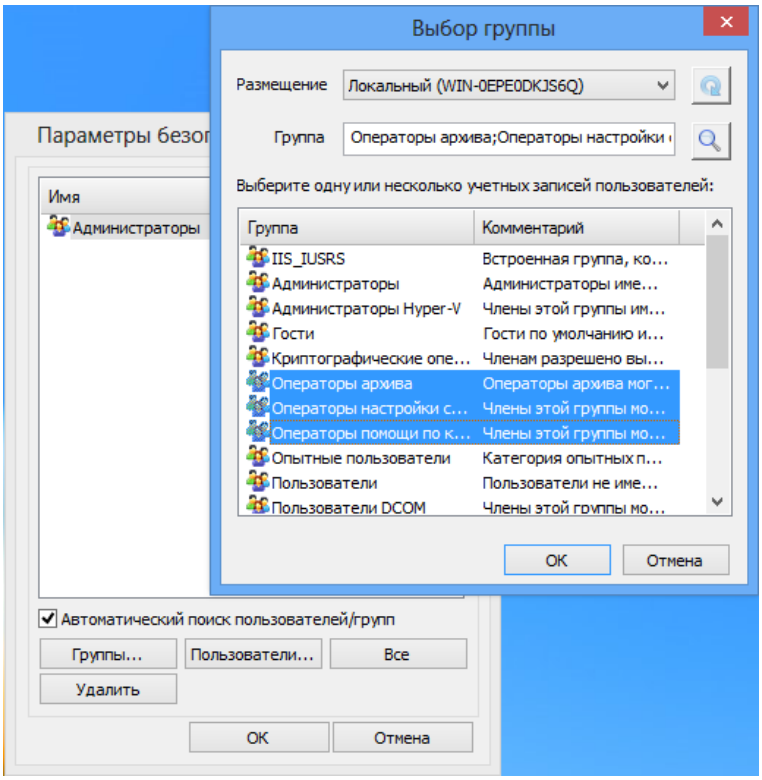


Рис. 36. Назначение пользователей

В списке учетных записей выбрать группы/пользователей, которым следует предоставить данное полномочие по администрированию. На панели главного окна программы в строке редактируемого параметра появятся имена выбранных пользователей и групп.

Примечание. Пользователь, установивший систему защиты (суперадминистратор), имеет полные полномочия на все действия. Ограничить их нельзя. Поэтому, даже если строчка в параметрах безопасности, соответствующая определенному полномочию, пуста, суперадминистратор имеет данное полномочие.

3.6.2 Полномочия на просмотр параметров безопасности

Установленные параметры безопасности СЗИ полностью определяют ее работу. Пользователю могут быть предоставлены полномочия на просмотр уже настроенных параметров безопасности и на управление (настройку) параметрами безопасности.

Если пользователю предоставлено право на управление, то право на просмотр предоставляется автоматически.

Для назначения полномочия на просмотр необходимо в категории «Права пользователей» выбрать параметр «Параметры безопасности: Просмотр» и выбрать учетные записи.

Если пользователю дано право на просмотр, то он может видеть:

- все значения параметров безопасности, установленные в СЗИ;
- распределение полномочий между пользователями (какому пользователю предоставлены те или иные полномочия);
- установленные значения дискреционного и мандатного доступов, а также контроля целостности для объектов ФС, устройств и реестра (причем и в оболочке администратора, и из окна параметров объекта, вызванного через контекстное меню, если это предполагается свойствами объекта).

Для того, чтобы иметь право на изменение и настройку параметров безопасности, дискреционного, мандатного доступов и контроля целостности, необходимо выполнить настройки и определить пользователей для каждого вида параметров (см. ниже).

3.6.3 Полномочия на управление параметрами безопасности

Данные полномочия позволяют изменять параметры безопасности СЗИ.

Если пользователю (группе пользователей) разрешено изменение параметров безопасности, то он может делегировать все свои полномочия другим пользователям с учетом действия контроля за

распространением полномочий (см. выше).

Для того, чтобы назначить управление параметрами безопасности, необходимо выбрать параметр «Параметры безопасности: Управление» в списке, нажать кнопку «Свойства» и добавить учетные записи.

Если пользователю предоставлено право на управление параметрами безопасности, то право на просмотр установленных настроек предоставляется автоматически.

3.6.4 Полномочия на управление дискреционным доступом

Дискреционный доступ подробно рассмотрен в главе «Разграничение доступа к объектам ФС» данного руководства. Дискреционный доступ основывается на предоставлении пользователю прав на определенные операции с объектами ФС.

После предоставления полномочий на управление дискреционным доступом пользователю или группе они получают возможность каждому ресурсу ФС сопоставить список пользователей и/или групп пользователей и каждому пользователю из списка разрешить или запретить определенную операцию с данным ресурсом, а также назначить описание для сменного накопителя.

Для того, чтобы назначить управление дискреционным доступом, необходимо выбрать параметр «Ресурсы: Управление дискреционным доступом» в списке, нажать кнопку «Свойства» и добавить учетные записи.

Если пользователю предоставлено право на управление дискреционным доступом, то право на просмотр установленных настроек предоставляется автоматически.

3.6.5 Полномочия на управление мандатным доступом

Данный параметр доступен только для Dallas Lock 8.0 редакции «С»

Мандатный доступ подробно рассмотрен в главе «Разграничение доступа к объектам ФС» данного руководства. Данной политикой пользователю предоставляются полномочия на управление мандатным доступом.

Для того, чтобы назначить управление мандатным доступом, необходимо выбрать параметр «Ресурсы: Управление мандатным доступом» в списке, нажать кнопку «Свойства» и добавить учетные записи.

Если пользователю предоставлено право на управление мандатным доступом, то право на просмотр установленных настроек предоставляется автоматически.

3.6.6 Полномочия на управление контролем целостности

Механизм контроля целостности подробно рассмотрен в главе «Подсистема обеспечения целостности» данного руководства. Предоставление пользователю полномочий на управление контролем целостности позволяет назначить или отменить контроль целостности любому объекту ФС.

Для того, чтобы назначить управление контролем целостности, необходимо выбрать параметр «Ресурсы: Управление контролем целостности» в списке, нажать кнопку «Свойства» и добавить учетные записи.

Если пользователю предоставлено право на управление контролем целостности, то право на просмотр установленных настроек предоставляется автоматически.

3.6.7 Полномочия на деактивацию системы защиты

Пользователь, обладающий полномочием на деактивацию СЗИ, имеет право удалить СЗИ, включать/выключать «мягкий» режим, «режим обучения» и «неактивный режим», осуществлять смену лицензии.

Процесс удаления описан в разделе «Удаление системы защиты». По умолчанию этим правом обладает только пользователь, установивший систему (администратор безопасности или суперадминистратор). Для назначения данного права другим пользователям необходимо выбрать параметр «Деактивация системы защиты».

Если пользователь, не наделенный данным полномочием, попытается начать процесс удаления, на экран будет выведено предупреждение и процесс прекратится.

Внимание! Для того, чтобы пользователь имел возможность удалить с компьютера систему защиты, он не только должен иметь это полномочие, но и должен иметь полномочия на администрирование ОС (определяется по факту вхождения пользователя в группу администраторов ОС). Рекомендуется удалять СЗИ тем же пользователем, который проводил установку.

Добавить учетные записи в список разрешенных для данного параметра можно, выбрав параметр и нажав кнопку «Свойства».

4 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ

4.1 Управление учетными записями

В СЗИ Dallas Lock 8.0 возможна регистрация пользователей следующих видов:

1. Пользователей, созданных средствами ОС Windows на данном локальном компьютере.
2. Пользователей, созданных средствами СЗИ.
3. Пользователей, созданных средствами службы AD (если компьютер находится в ЛВС под управлением контроллера домена).

Пользователи, зарегистрированные в ОС Windows, автоматически не становятся зарегистрированными пользователями в системе защиты Dallas Lock 8.0 и не могут работать на ЗАРМ. В то же время при создании нового пользователя в системе защиты он автоматически становится пользователем ОС. Процесс регистрации будет описан ниже.

Для просмотра и редактирования учетных записей пользователей в оболочке администратора системы защиты необходимо выбрать вкладку «Учетные записи» (рис. 37):

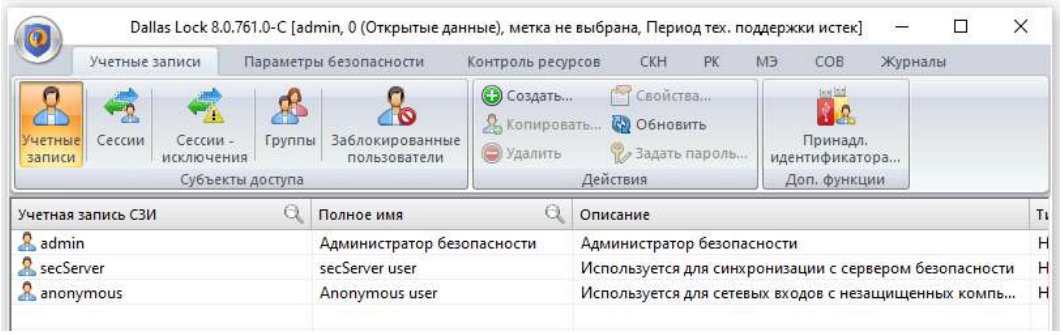


Рис. 37. Вкладка Учетные записи

Число зарегистрированных пользователей на каждом ЗАРМ ограничивается только размером свободного дискового пространства. Один пользователь может быть зарегистрирован на нескольких ПК.

По умолчанию в системе защиты Dallas Lock 8.0 всегда присутствуют следующие учетные записи:

- **суперадминистратор** — учетная запись пользователя, установившего СЗИ (запись невозможно удалить из системы).
- **anonymous** — учетная запись для проверки входов с незащищенной системой машин (запись невозможно удалить из системы, но можно отключить, при этом следует помнить, что учетная запись anonymous на контроллере домена всегда должна быть включена).
- **secServer** — через эту учетную запись СБ подключается к данному ПК и проводит ОУ (запись невозможно удалить из системы, но можно отключить).
- ****** — специальная учетная запись, разрешающая всем доменным пользователям вход на защищенный системой компьютер (см. «Регистрация доменных пользователей»). Создается только на ПК, которые в момент установки СЗИ входят в домен AD. Запись можно удалить или отключить.

Зарегистрированные, но отключенные учетные записи выделяются иконкой  .

Пользователь, установивший систему защиты, обладает всеми полномочиями администрирования (управления) системы защиты и всеми правами по доступу к ресурсам, причем эти права и полномочия в дальнейшем невозможно ограничить. Суперадминистратор регистрирует в системе защиты других пользователей. При этом он может делегировать зарегистрированному пользователю все или часть своих полномочий на администрирование.

4.1.1 Полномочия на управление учетными записями

Регистрировать и удалять пользователей, а также просматривать и редактировать учетные записи может только пользователь, наделенный соответствующими полномочиями по администрированию.

Полномочиями для создания, удаления и изменения учетных записей пользователей в системе защиты обладают: суперадминистратор и пользователи (группы пользователей), указанные в списке разрешенных параметра «Учетные записи: Управление» на вкладке «Права пользователей» (рис. 38). По умолчанию это администраторы.

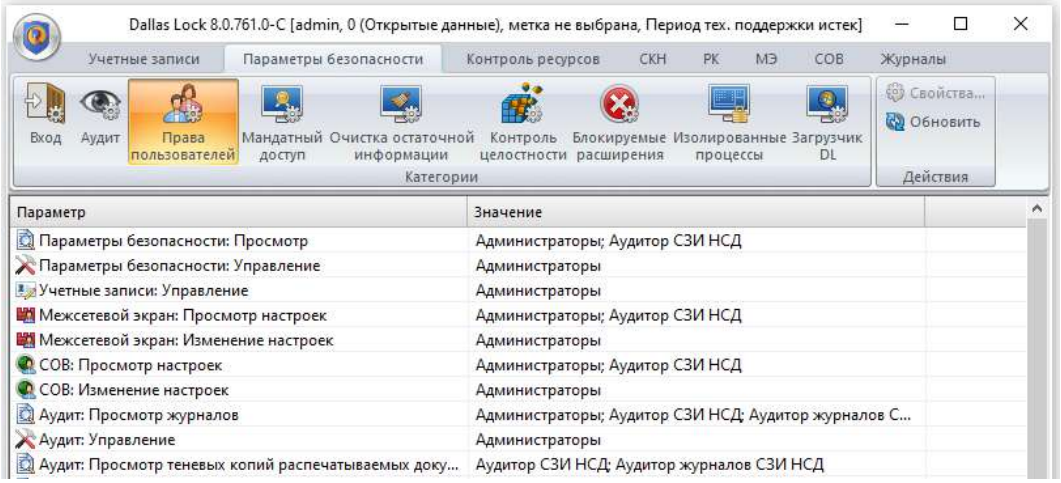


Рис. 38. Параметр, определяющий полномочия на управление учетными записями

4.1.2 Создание и удаление локальных пользователей

В рабочем окне вкладки «Учетные записи» выводится список учетных записей пользователей, зарегистрированных в системе защиты Dallas Lock 8.0. Информация о локальных пользователях, зарегистрированных только в ОС данного компьютера, здесь не просматривается.

Создание пользователей

Перед созданием новой учетной записи необходимо убедиться в том, что нужная учетная запись еще не создана в ОС. В таком случае достаточно будет ее просто зарегистрировать, выбрав из списка, вызываемого кнопкой поиска.

Для создания нового пользователя в системе защиты необходимо:

1. Выделить категорию «Учетные записи» в оболочке администратора.
2. Нажать кнопку «Создать» в категориях «Действия» или выбрать соответствующую из контекстного меню, нажав правую кнопку мыши.
3. На экране появится окно создания новой учетной записи (рис. 39).

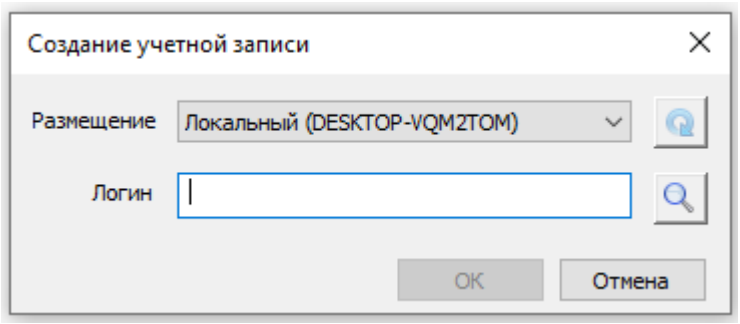


Рис. 39. Окно создания учетной записи

4. В поле «Размещение» необходимо выбрать значение «Локальный».
5. В поле «Логин» необходимо ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:
   - максимальная длина имени — 20 символов;
   - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ *);
   - разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть прописные и строчные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

Кнопка поиска, расположенная рядом с полем логина, разворачивает список учетных записей пользователей, зарегистрированных в ОС данного ПК, и позволяет выбрать пользователя из уже существующих (рис. 40).

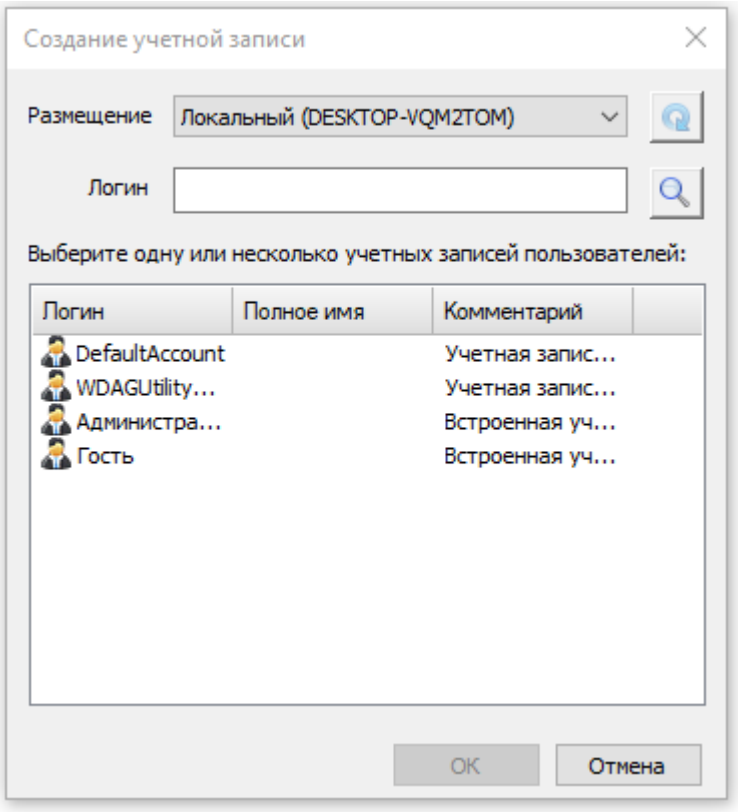


Рис. 40. Учетные записи, зарегистрированные в ОС компьютера

Также можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

6. После нажатия «OK» появится окно редактирования параметров учетной записи (рис. 41).

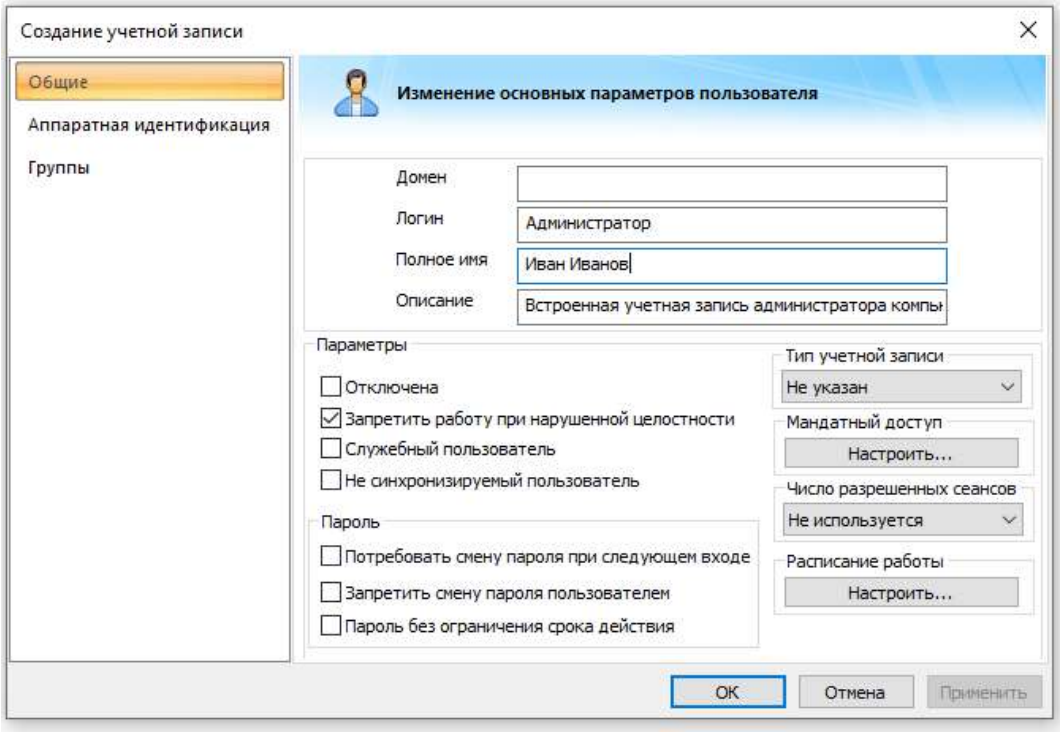


Рис. 41. Окно редактирования параметров новой учетной записи

На вкладке «Общие» предлагается заполнить следующие учетные данные и параметры:

- Заполнить **«Полное имя»** пользователя.
- В поле «**Описание**» ввести любой комментарий. Длина комментария не более 256 символов. Вводить комментарий и полное имя не обязательно.
- Политики «**Отключена**» и «**Запретить работу при нарушении целостности**» задаются при необходимости:

a. Администратор имеет возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на АРМ до тех пор, пока администратор не деактивирует эту опцию.
b. Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «Запретить работу при нарушении целостности» активизирована, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется до тех пор, пока администратор не разблокирует учетную запись. Если же эта опция не включена, то при обнаружении нарушения целостности будет отображено только предупреждение.

- Флаг в поле «**Служебный пользователь**» предоставляет данной учетной записи особый статус (см. «Служебный пользователь»).
- Флаг в поле **«Не синхронизируемый пользователь»** устанавливает статус, при котором данная учетная запись не синхронизируется с СБ (см. «Синхронизация»).
- Необходимо выбрать **«Тип учетной записи».** Для типа «Временный» обязательным условием является настройка расписания работы пользователя (см. ниже). По умолчанию тип учетной записи будет иметь значение «Не указан».
- Необходимо выбрать уровень доступа для пользователя в поле «**Мандатный доступ»** (только для Dallas Lock 8.0 редакции «С»)**,** под которым пользователь сможет работать (см. «Мандатный доступ»).
- Необходимо выбрать значение в поле **«Число разрешенных сеансов»** (см. «Число разрешенных сеансов»).
- Необходимо задать «**Расписание работы»** пользователя, выбрать период и время. Вне указанного периода пользователь не сможет зайти на АРМ. По окончании времени работы ПК пользователя будет заблокирован при условии включения параметра безопасности «Принудительное завершение работы по расписанию» («Параметры безопасности» → «Права пользователей»).

Примечание. «Расписание работы» пользователя может быть определено с дискретностью 30 минут.

- Отмеченный параметр «**Потребовать смену пароля при следующем входе**» единовременно запросит смену пароля при входе.
- Поле «**Запретить смену пароля пользователем**».
- Флаг в поле «**Пароль без ограничения срока действия**» отменяет действие политики входа «Максимальный срок действия паролей», распространяемой на всех пользователей.

Примечание. Поле **«Логин»** и поле **«Домен»** остаются без возможности изменения (название домена для локального пользователя остается пустым).

Далее, в процессе создания или регистрации нового локального пользователя администратор имеет возможность включить его в определенную группу. В окне закладки «Группы» отображены названия групп, в которые включен пользователь (рис. 42). По умолчанию каждый новый пользователь входит в группу «Пользователи».

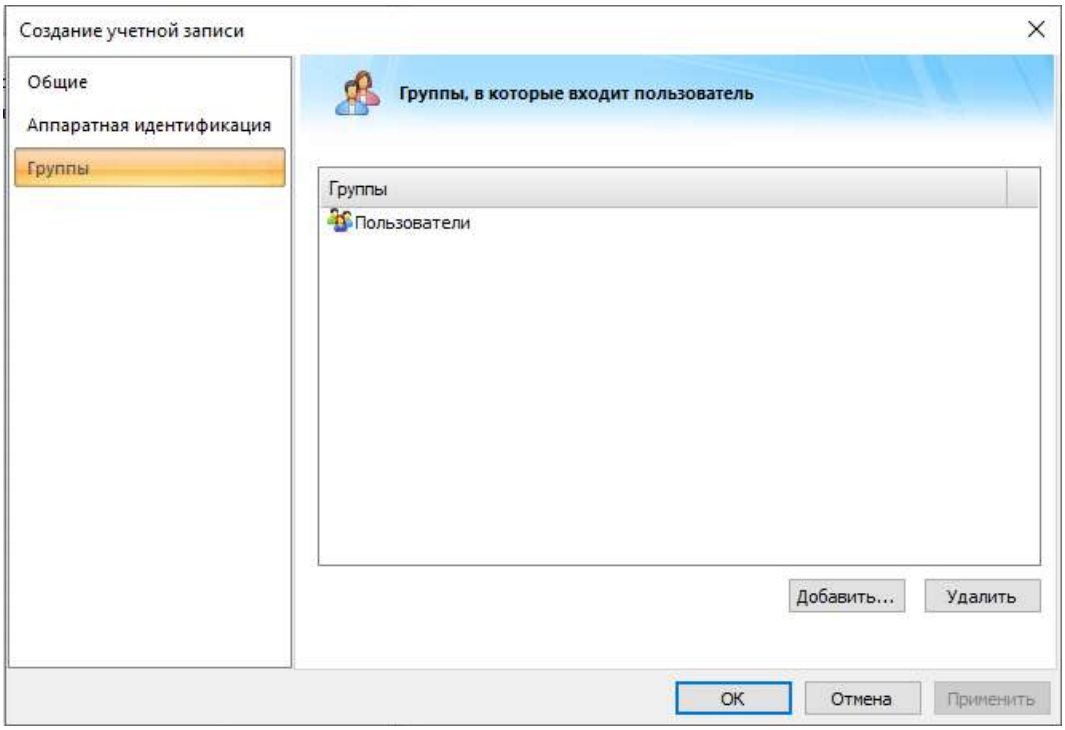


Рис. 42. Окно редактирование списка групп пользователя

Примечание. Если для регистрации в СЗИ при выборе пользователей, имеющихся в ОС, одновременно выделить несколько учетных записей, то для них настраиваются одинаковые свойства в одном окне.

7. Чтобы включить пользователя в определенную группу, необходимо нажать «Добавить». Появится список всех групп пользователей, имеющихся в системе (кроме тех, в которые пользователь уже включен) (рис. 43).

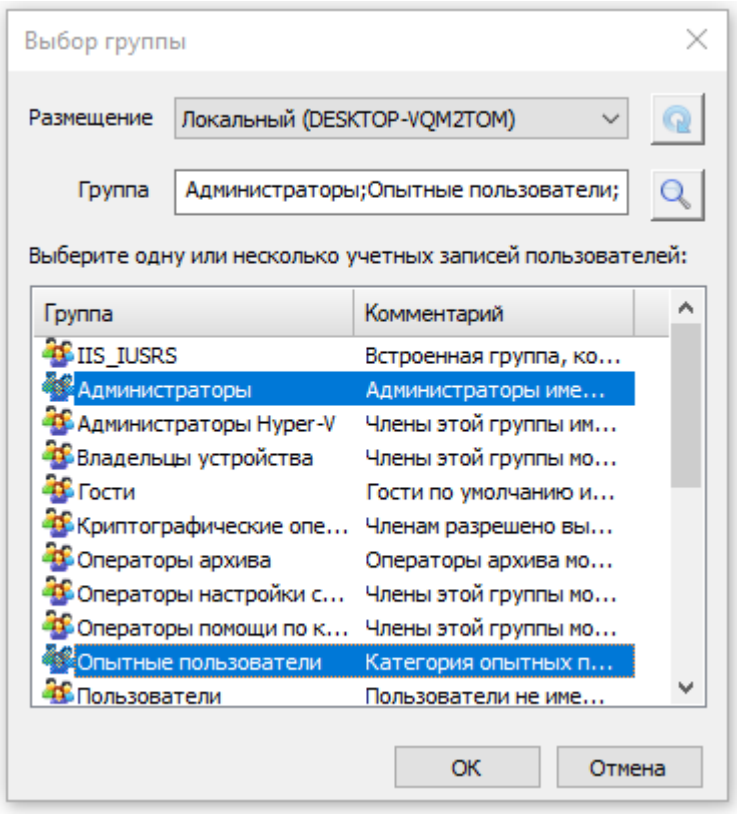


Рис. 43. Окно выбора групп для учетной записи

8. В поле «Размещение» необходимо оставить значение «Локальный». В списке групп нужно

выбрать необходимую. Одновременно можно выделить несколько групп в списке.

Кнопка поиска в данном окне помогает найти необходимые группы по названию или его части. Возможна сортировка по алфавиту списка групп нажатием на поле с названием и со значком сортировки (треугольник).

9. Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки «ОК» (рис. 44).

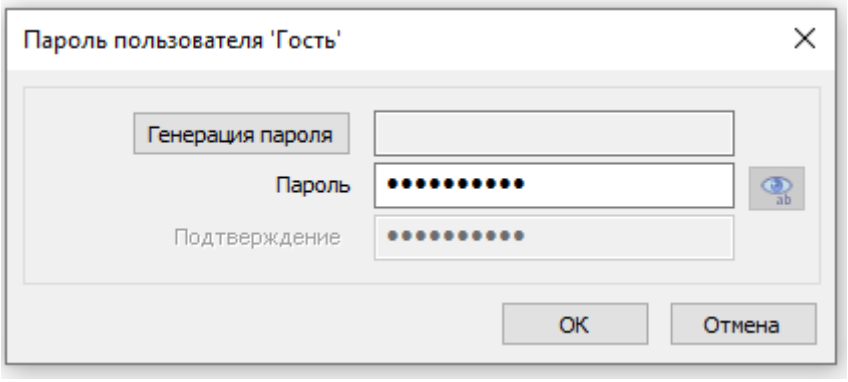


Рис. 44. Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля составляет 31 символ;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности «Пароли: необходимо наличие специальных символов» в разделе «Настройка параметров входа»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. «Настройка параметров входа»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку с надписью: «Генерация пароля». Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля «Пароль» и «Подтверждение».

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Примечание. Если в СЗИ регистрируется пользователь, учетная запись которого уже имеется на локальном компьютере, то его пароль для входа в ОС автоматически становится паролем для входа в систему защиты, поэтому операция по назначению пароля не предлагается. При необходимости пароль можно изменить средствами СЗИ.

Примечание. После того, как пользователь зарегистрирован, менять его имя средствами ОС не рекомендуется. В противном случае, зайти этим пользователем на ЗАРМ возможности не будет.

Также следует учесть, если учетная запись (в том числе в составе группы) отмечена в значении для параметра «Учетные записи: Принудительная двухфакторная аутентификация», то присвоение аппаратного идентификатора станет обязательным условием, иначе при завершении ее регистрации или редактировании в СЗИ появится предупреждение об ошибке (см. «Принудительная двухфакторная аутентификация»). Это правило распространяется для вновь создаваемых учетных записей пользователей.

Удаление пользователей

Для удаления пользователя из системы защиты вне зависимости от того, какими средствами он создан или зарегистрирован в самой системе защиты, необходимо выделить его имя в списке главного окна программы, нажать кнопку «Удалить» или выбрать соответствующее действие из контекстного меню. Подтвердить операцию. Учетная запись будет удалена и из системы защиты, и из ОС.

Следует отметить, что при удалении самой системы защиты Dallas Lock 8.0 с компьютера учетные записи пользователей, созданные средствами системы защиты через оболочку администратора, остаются в ОС, как и учетные записи, созданные в ОС и зарегистрированные в системе защиты.

Создание учетной записи путем копирования

При создании учетной записи пользователя, которая имеет одинаковые свойства с другой учетной записью, можно воспользоваться функцией копирования. Для этого необходимо выбрать учетную запись в списке и нажать «Копировать» на панели действий (рис. 45).

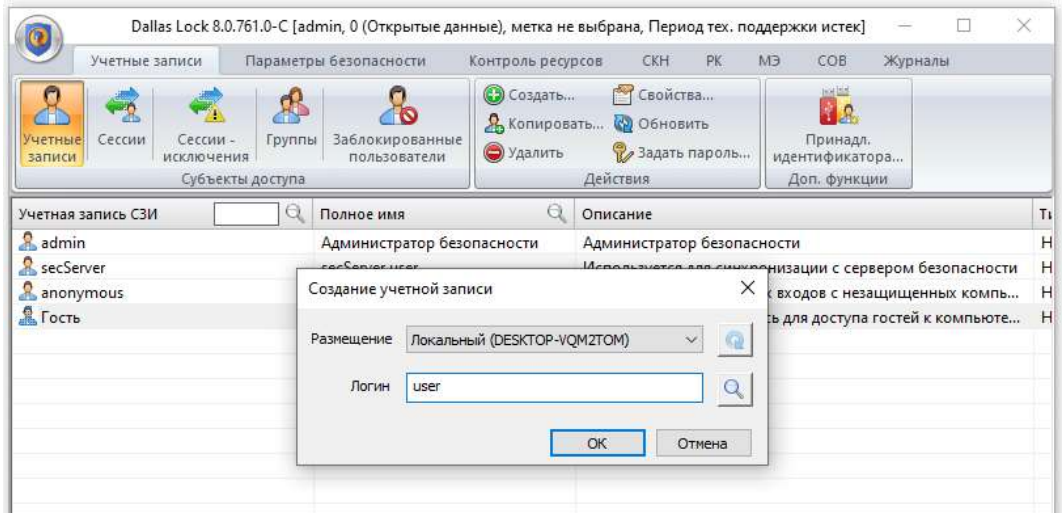


Рис. 45. Создание новой учетной записи с копированием свойств уже созданной

В появившемся окне ввести имя учетной записи. Далее, в окне свойств, которые будут в точности повторять свойства выделенной учетной записи, их можно отредактировать. Далее необходимо создать пароль.

Для создаваемой учетной записи будут скопированы свойства и список групп; установка параметров доступа на ресурсы не копируется и осуществляется индивидуально для данной учетной записи (или для группы, в которую она входит).

Создание учетной записи путем копирования свойств другой имеет смысл только для локальных учетных записей.

4.1.3 Регистрация доменных пользователей

Чтобы зарегистрировать в СЗИ учетную запись доменного пользователя, необходимо выполнить следующее.

1. Получить список доменных пользователей. Для этого, при создании учетной записи, в выпадающем меню размещения необходимо выбрать имя домена и нажать кнопку поиска (рис. 46).

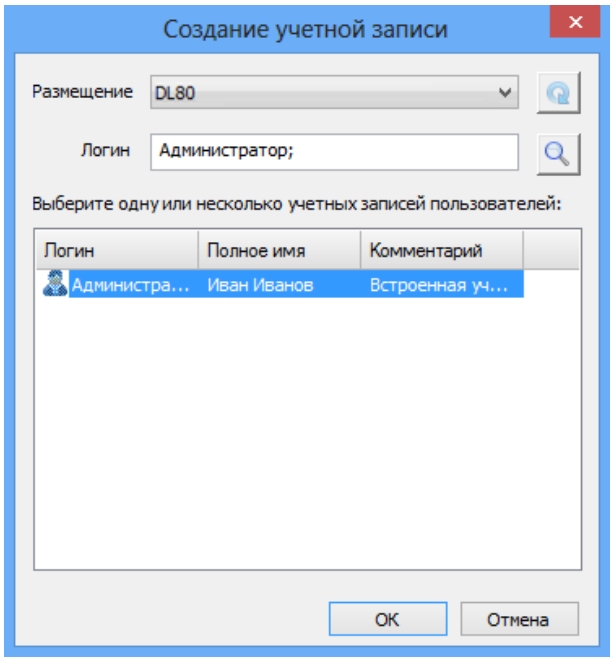


Рис. 46. Заполнение имени учетной записи

Для получения списка учетных записей домена необходимо дополнительно ввести авторизационные данные администратора домена. После авторизации появится список пользователей, зарегистрированных на контроллере домена. Для поиска необходимой записи можно воспользоваться сортировкой или ввести первые буквы и нажать кнопку поиска  .

2. Выбрать учетную запись пользователя и нажать «OK». Можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

В системе защиты автоматически сформируется учетная запись пользователя с теми параметрами, которые соответствуют ей на контроллере домена (имя домена, логин, пароль, полное имя, название групп на контроллере домена). Автоматически учетная запись пользователя в списке учетных записей будет иметь вид: «имя домена/имя пользователя».

Имеющихся доменных пользователей можно зарегистрировать в СЗИ, но их нельзя создать средствами СЗИ. Если нужен новый доменный пользователь, его придется создать средствами администрирования на контроллере домена, и только после этого зарегистрировать в СЗИ.

Список доменных пользователей и групп кэшируется СЗИ в своей памяти. Поэтому, если новый пользователь создан на контроллере домена, он может появиться в списке системы защиты не сразу. Необходимо обновить список с помощью кнопки «Обновить».

Примечание. Процесс получения списка доменных пользователей может быть достаточно длительным. Во время этого процесса возможно появление окошка с просьбой ввести идентификационную информацию администратора.

С зарегистрированными в СЗИ доменными пользователями можно проводить любые операции по реализации политик безопасности, однако нельзя менять пароль средствами системы. При попытке изменить пароль будет выведено предупреждение (рис. 47).

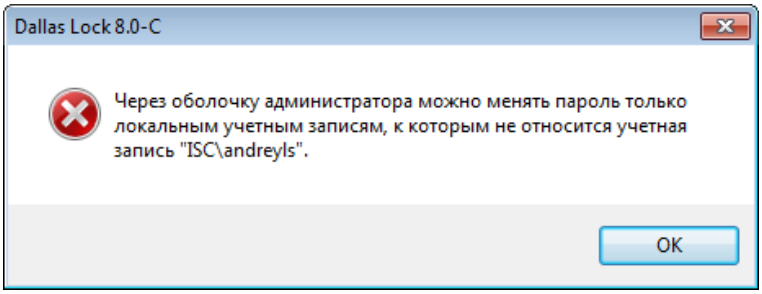


Рис. 47. Сообщение системы при попытке смены пароля

Примечание. Аппаратный идентификатор может быть назначен только для отдельно взятой доменной учетной записи, зарегистрированной в системе защиты, без маски.

Также средствами Dallas Lock 8.0 невозможно изменить список групп, в которые входит доменный пользователь.

4.1.4 Регистрация доменных учетных записей по маске

Очень часто компьютеры с установленной системой защиты объединены в локальную сеть, физическую и логическую структуру которой объединяет служба каталогов Microsoft Active Directory. Это позволяет централизованно администрировать все ресурсы, включая пользователей, файлы, периферийные устройства, доступ к службам, сетевым ресурсам, веб-узлам, базам данных и прочие. Группа компьютеров, совместно использующих общую базу данных каталога, образуют домен.

Таким образом, с учетными записями пользователей, созданными в домене, можно проводить операции на рабочих станциях, зарегистрированных в этом домене, и в том числе регистрировать в системе защиты Dallas Lock 8.0.

В системе защиты Dallas Lock 8.0 реализован механизм регистрации доменных учетных записей пользователей системы с использованием масок, по символу «*». В этом контексте символ «*» имеет значение «все». Учетная запись «Имя_домена*» означает всех пользователей данного домена.

По такой маске возможна регистрация только доменных учетных записей, для локальных это невозможно, и каждая запись должна быть создана отдельно. В то же время, если известен пароль локального пользователя, СБ сможет такого пользователя создать на клиенте.

При установке СЗИ с конфигурацией по умолчанию, если ПК является членом домена Windows, в системе защиты автоматически регистрируется учетная запись «**». Это означает, что вход на ЗАРМ могут осуществлять все доменные пользователи (в том числе пользователи доверенных доменов).

Механизм регистрации доменных учетных записей системы с использованием масок позволяет привести систему входа к строгому виду.

Каждая учетная запись может быть в состоянии «вход разрешен» и «вход запрещен». Чтобы запретить вход под соответствующей учетной записью, необходимо, чтобы был поставлен флаг в поле «Отключена» в окне параметров учетных записей (рис. 48).

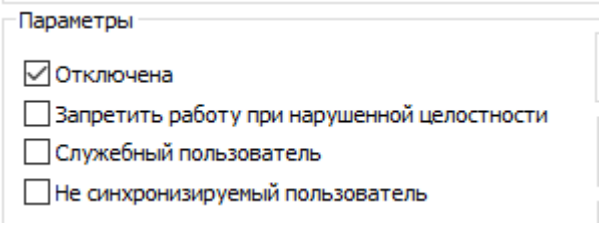


Рис. 48. Окно редактирования учетной записи

Если для существующей учетной записи вида «**» запретить вход в систему и одновременно разрешить вход для учетных записей типа «ZCB*», то в систему защиты пользователи доменов входить не смогут, но смогут входить только пользователи домена ZCB. Другой пример: если запретить вход в систему для записи «ZCB*» и разрешить для «ZCB\admin1», «ZCB\admin2», то это будет означать, что из домена ZCB на защищенный системой компьютер смогут входить только пользователи admin1 и admin2.

Таким образом, систему проверки пользователей можно легко привести к «строгой» системе, достаточно отключить учетную запись «**», и, далее, в явном виде регистрировать учетные записи необходимых доменных пользователей.

Примечание. Если в СЗИ зарегистрирована доменная учетная запись «**» или «Имя_домена*», то назначать права на доступ к объекту можно как для учетной записи «**» (или «Имя_домена*»), так и для каждой индивидуальной учетной записи домена, выбрав ее из списка через дескриптор объекта (см. ниже).

4.1.5 Создание и удаление групп пользователей

Группы предназначены для объединения пользователей, у которых права безопасности могут быть схожими. Такое объединение может упростить работу администратора при выполнении настроек СЗИ.

Группы безопасности упрощают управление доступом к ресурсам. Можно добавлять пользователей к группам безопасности, а затем предоставлять этим группам права доступа, и удалять их оттуда в соответствии с потребностями этих пользователей.

Для просмотра и редактирования списка групп системы безопасности в оболочке администратора системы необходимо выбрать категорию «Группы» на вкладке «Учетные записи». В окне системы Dallas Lock 8.0 автоматически появляется ряд предварительно сконфигурированных групп в локальной ОС Windows, в которые можно включать пользователей.

Вновь созданные с помощью Dallas Lock группы автоматически создадутся и на локальном ПК. Удаленные локальные группы удалятся и из ОС на локальном ПК.

Примечание. В данные локальные группы, сформированные в системе защиты Dallas Lock 8.0, можно добавить только локальных пользователей. Доменные пользователи добавляются в группы на контроллере домена. Также при настройке параметров безопасности при добавлении групп появляется возможность выбора или локальных групп, или групп пользователей, расположенных на контроллере домена.

При установке Dallas Lock 8.0 по умолчанию реализовано автоматическое создание двух групп пользователей с предустановленными правами: группа «Аудитор СЗИ» и группа «Аудитор журналов СЗИ» (см. «Полномочия на просмотр и управление параметрами аудита»).

В главном окне оболочки администратора вкладка «Группы» имеет следующий вид (рис. 49):

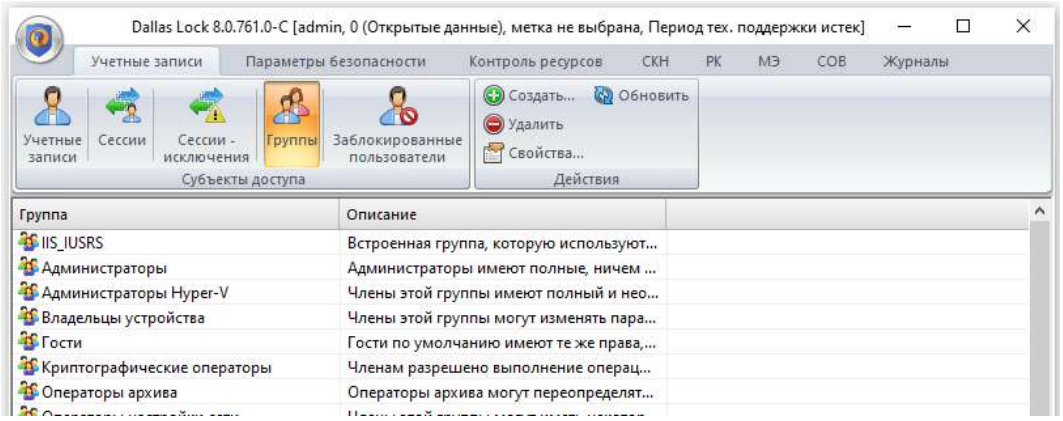


Рис. 49. Общий вид закладки «Группы»

Для создания новой группы необходимо:

1. В разделе «Группы» на вкладке «Учетные записи» нажать «Создать» (или выбрать данное действие из контекстного меню). Откроется окно, содержащее два поля: «Группа», «Описание» (рис. 50).

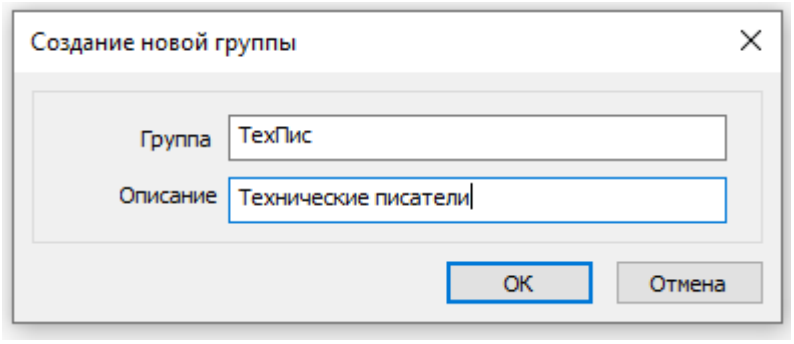


Рис. 50. Окно создания новой группы

2. В поле «Группа» следует ввести название группы, в поле «Описание» — назначение группы или комментарий (необязательное поле). Нажать «ОК».

Изменить описание группы можно, используя кнопку «Свойства» на панели «Действия» или выбрав данное действие из контекстного меню.

Назначить все необходимые политики безопасности для созданной группы можно, редактируя параметры безопасности различных категорий параметров.

Для удаления группы необходимо выделить группу, которую следует удалить, нажать кнопку «Удалить» на панели «Действия» или выбрать данное действие в контекстном меню. На экране отобразится подтверждение на удаление.

4.1.6 Число разрешенных сеансов

При настройке свойств учетной записи имеется возможность определить число разрешенных сеансов для данной учетной записи (рис. 51).

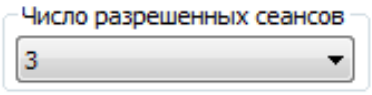


Рис. 51. Свойства учетной записи. Параметры сеансов доступа

При установленном значении для каждой учетной записи (локальной или доменной) будет проверяться количество одновременных интерактивных и сетевых сессий (входов).

Если число больше установленного, то вход пользователя на ПК запрещается. Если стоит ограничение для учетной записи по маске, ограничение будет действовать на каждого доменного пользователя индивидуально.

Таким образом, установив параметр «Число разрешенных сеансов» равным 1, можно настроить запрет вторичного (параллельного) входа пользователя в ОС.

Примечание. Следует помнить, что при смене пользователя (возможность Windows 7 и более новых ОС) интерактивная сессия пользователя, инициирующего смену, не завершается. Если после этого выполнить авторизацию под тем же самым пользователем, ОС Windows выполнит попытку создания новой интерактивной сессии до уничтожения старой. Соответственно, это приведет к временному (несколько секунд до завершения старой сессии) увеличению числа сессий на единицу. Поэтому, например, если ограничить число сеансов пользователя единицей, данный пользователь не сможет выполнить «смену пользователя» и войти опять под своими учетными данными (временно создать две сессии не разрешит данная настройка Dallas Lock).

4.1.7 Смена пароля пользователя

Смена пароля средствами ОС

Пользователь может самостоятельно сменить пароль для авторизации, для этого необходимо выполнить следующие шаги:

1. После входа в ОС пользователю необходимо нажать комбинацию клавиш «Ctrl+-Alt+Del» и в списке операций выбрать «Сменить пароль».

   На экране появится диалоговое окно с полями для заполнения (рис. 52).

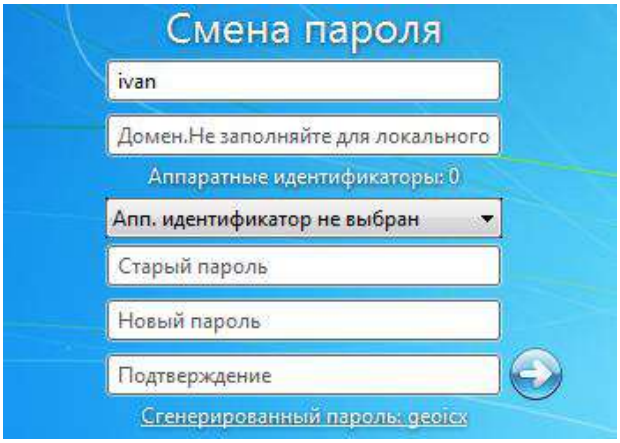


Рис. 52. Поля заполнения при смене пароля

2. В открывшемся окне необходимо ввести имя пользователя, имя домена (для доменного пользователя, для локального — оставить это поле пустым), старый пароль, новый пароль и подтверждение нового пароля.
3. Выбрать назначенный аппаратный идентификатор.

Примечание. Если текущему пользователю назначен аппаратный идентификатор, на который записаны авторизационные данные, то при смене пароля, помимо заполнения других полей, необходимо предъявить идентификатор и ввести PIN-код пользователя идентификатора.

4. Для создания пароля, отвечающего всем требованиям параметров безопасности, установленных системой защиты Dallas Lock 8.0, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать поле с надписью: «Генерация пароля». Система автоматически создаст случайный пароль, советующий установленным параметрам безопасности, значение которого необходимо ввести в поля «Новый пароль» и «Повтор».
5. Далее нажать кнопку «ОК» для сохранения нового пароля или кнопку «Отмена».

В соответствии с политиками безопасности в системе могут быть включены настройки сложности паролей. Сложные пароли при их регулярной смене снижают вероятность успешной атаки на пароль. Поэтому при смене пароля пользователю необходимо иметь информацию о требованиях для установки паролей. В соответствии с тем, какие из параметров включены, при смене пароля пользователем, на экране могут возникать сообщения об ошибках. При возникновении подобных сообщений необходимо изменить пароль в соответствии с требованиями политик безопасности, установленными администратором.

Смена пароля с помощью оболочки администратора

В некоторых ситуациях, например, когда пользователь забыл свой пароль, администратору бывает необходимо задать пользователю новый пароль, не зная старого.

Для этого в оболочке администратора нужно выбрать соответствующего пользователя в списке и нажать на действие «Задать пароль».

В появившемся окне нужно ввести новый пароль, его подтверждение и нажать кнопку «ОК».

Можно воспользоваться генератором паролей и ввести сформированный СЗИ пароль в соответствующие поля.

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто. В случае корректного ввода нового пароля появится сообщение об успешной смене пароля.

Примечание. Сменить пароль для пользователя через оболочку администратора системы Dallas Lock 8.0 можно только для локальных пользователей. Пароли доменных пользователей меняются на Контроллере домена.

4.1.8 Сессии-исключения

Для корректной работы в режиме совместимости со сторонним ПО в СЗИ Dallas Lock реализован механизм регистрации сессий, которым в качестве исключения разрешается работа с ФС, несмотря на отсутствие явного санкционированного входа.

Зарегистрированные в Dallas Lock 8.0 сессии называются сессии-исключения. СЗИ Dallas Lock уже содержит список настроенных сессий первой необходимости. По умолчанию все сессии-исключения отключены, кроме одной «Для работы всех служебных записей».

Чтобы просмотреть список сессий-исключений и добавить новые, необходимо в оболочке администратора на вкладке «Учетные записи» раскрыть категорию «Сессии-исключения» (рис. 53).

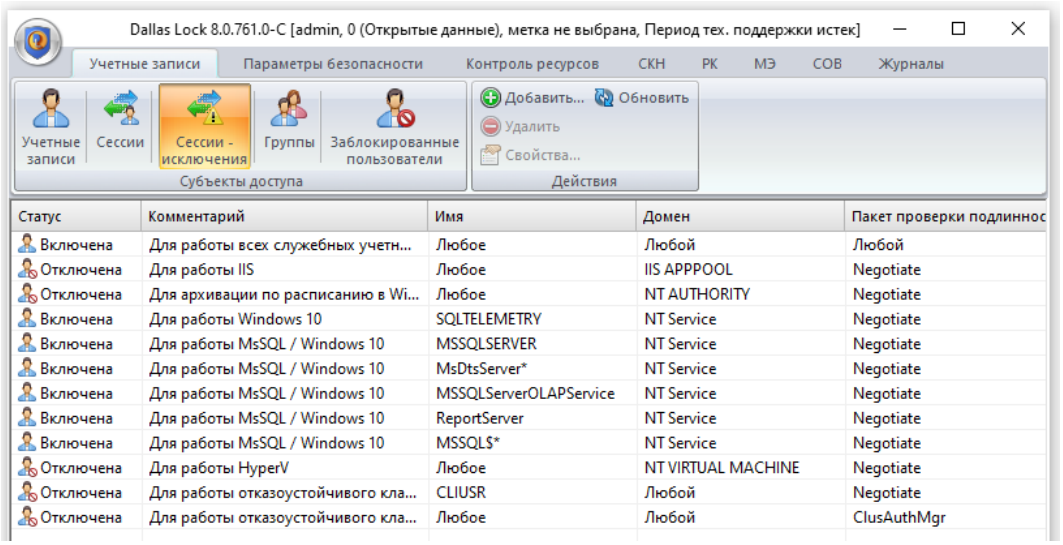


Рис. 53. Окно со списком сессий для работы ПО

Чтобы зарегистрировать в СЗИ сессию, необходимо нажать «Добавить». В появившемся окне ввести параметры сессии.

Добавленную в список сессию можно временно отключить, не удаляя из списка, и заново включить. Для этого в окне параметров сессии необходимо отметить флагом поле «Исключение активно» (рис. 54).

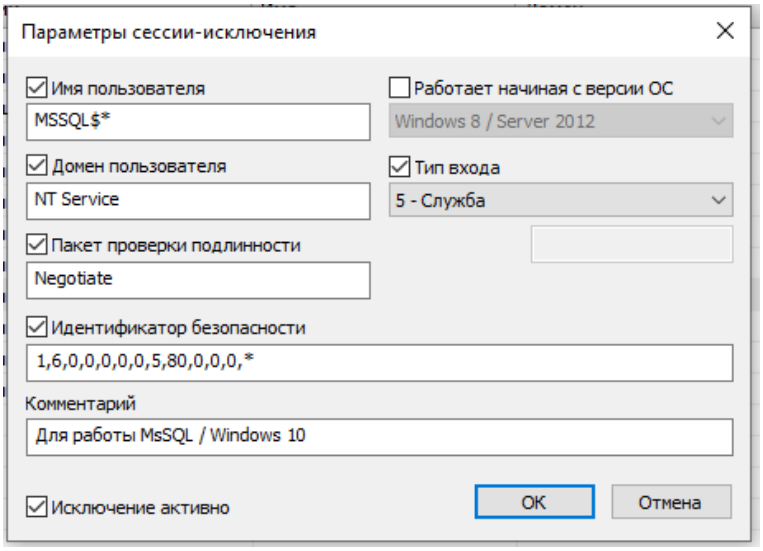


Рис. 54. Редактирование параметров сессии-исключения

Удалять из списка зарегистрированные по умолчанию в Dallas Lock 8.0 сессии-исключения не рекомендуется.

4.2 Заблокированные пользователи

Учетная запись пользователя по разным причинам может быть заблокирована, например, вследствие неправильного ввода пароля несколько раз.

Чтобы открыть список заблокированных пользователей, необходимо на вкладке основного меню «Учетные записи» выбрать категорию «Заблокированные пользователи» (рис. 55).

В данном списке можно разблокировать отдельно выделенную учетную запись или несколько одновременно выделенных (действие «Разблокировать») и разблокировать все записи одновременно (действие «Разблокировать всех»).

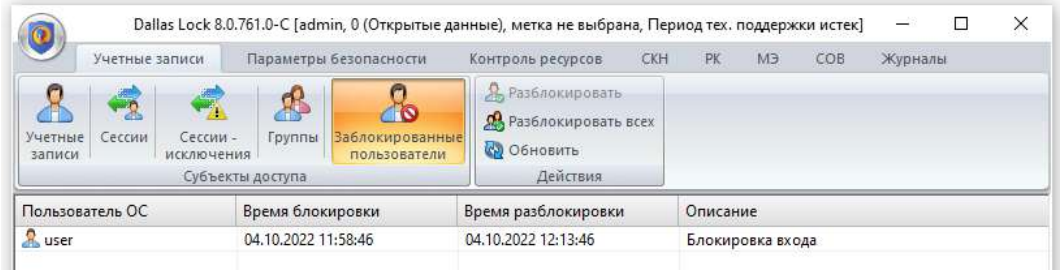


Рис. 55. Действия со списком заблокированных пользователей

Внимание! Важно не путать данное свойство с параметром «отключена» учетной записи, несмотря на одинаковый запрет доступа к работе на ПК. Примером различного состояния заблокированных и отключенных учетных записей может быть следующий.

Под одной доменной учетной записью, зарегистрированной в Dallas Lock 8.0 по маске, могут работать несколько доменных пользователей, и некоторые из них могут быть заблокированы, но в то же время доменная учетная запись по маске не отключена. Учетные записи данных заблокированных пользователей будут отображаться в списке, несмотря на то, что индивидуально в СЗИ они не зарегистрированы (зарегистрирована уч. запись по маске). В этом случае для разблокировки индивидуальных пользователей, для которых зарегистрирована одна на всех учетная доменная запись по маске, используется данная функция разблокировки в окне «Заблокированные пользователи».

4.3 Аппаратная идентификация пользователя

Практически все решения защиты информационных ресурсов основаны на доступе с использованием персональных паролей.

Дополнительное использование аппаратной идентификации позволяет решить проблему человеческого фактора, связанного с хранением сложных паролей, и усилить защиту информации.

4.3.1 Назначение аппаратной идентификации

Перед назначением аппаратного идентификатора следует:

1. Установить драйвер соответствующего идентификатора (установка драйверов возможна как перед установкой СЗИ на ТС, так и после).
2. Настроить в системе защиты его считыватель.

Подробное описание настройки считывателей приведено в «Настройка средств аппаратной идентификации» данного руководства.

Для назначения идентификатора пользователю необходимо в окне создания или редактирования учетной записи пользователя открыть закладку «Аппаратная идентификация» (рис. 56).

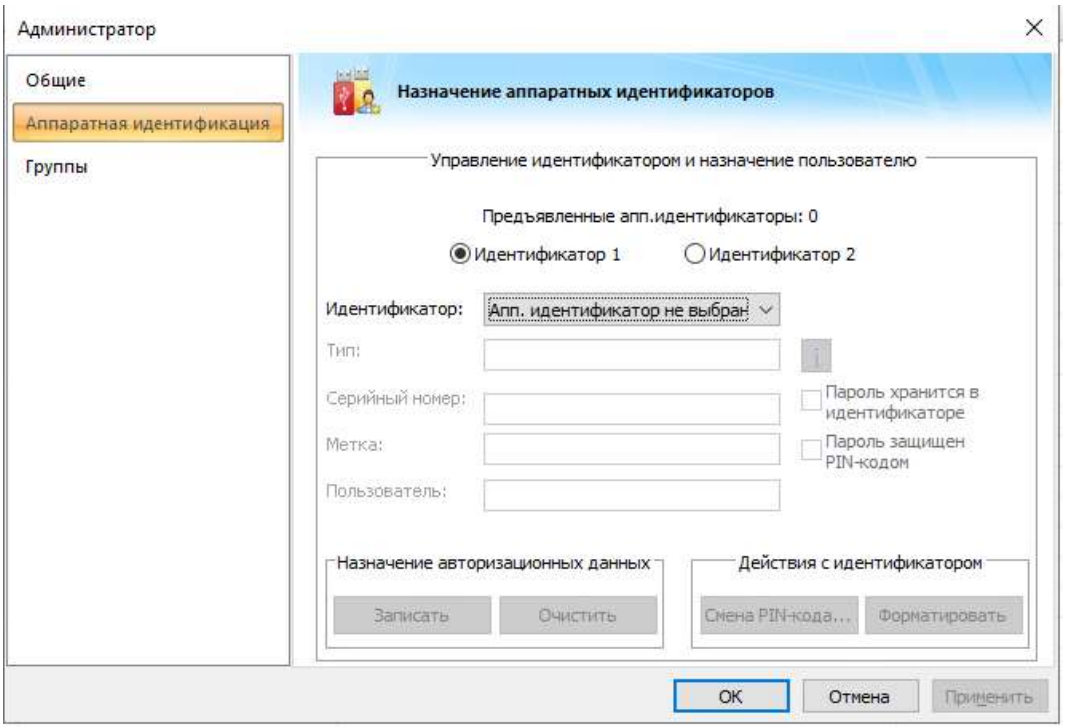


Рис. 56. Вкладка назначения аппаратных идентификаторов пользователю

Необходимо предъявить аппаратный идентификатор, вставив его в соответствующий USB-порт или прикоснувшись к считывателю (в зависимости от типа идентификатора). В строке состояния «Предъявленные аппаратные идентификаторы» появится цифра с количеством идентификаторов, предъявленных в данный момент, а в списке выпадающего меню — наименования. Для пользователя можно назначить два индентификатора. Для установки первого индентификатора, сделать активным поле «Индентификатор 1», после выбрать необходимый идентификатор из списка (рис. 57).

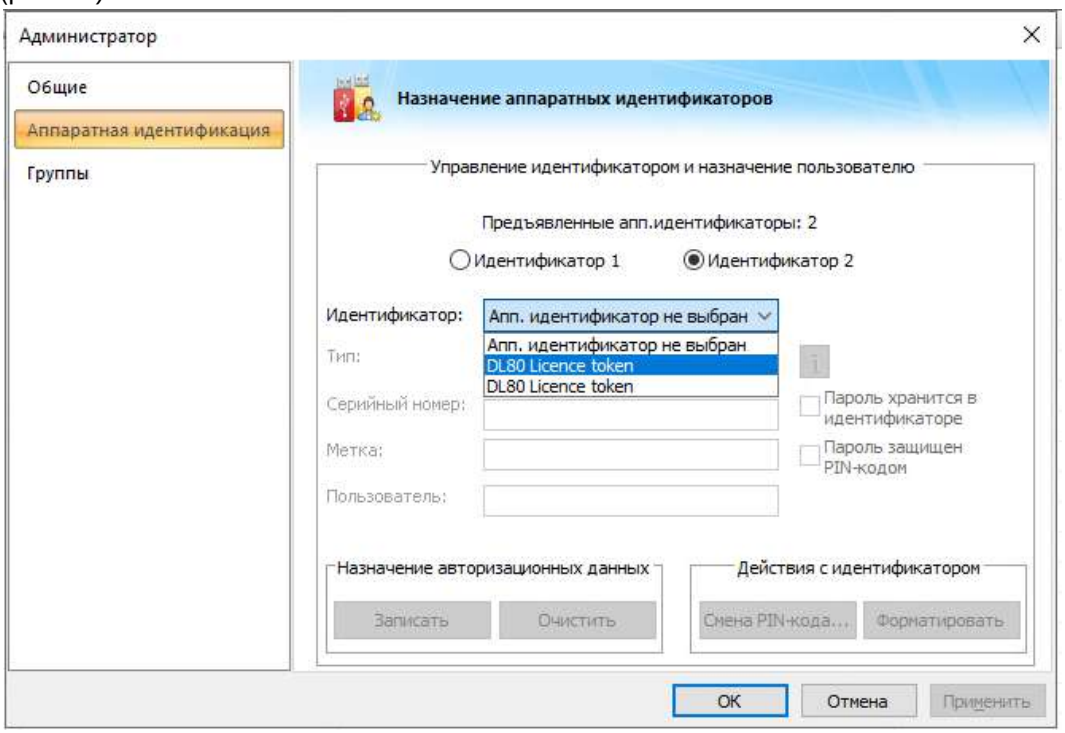


Рис. 57. Выбор зарегистрированного идентификатора

После выбора идентификатора в полях с параметрами появятся: наименование его типа, номер, изображение, и для некоторых видов идентификаторов[7] станут доступны дополнительные функции

[7] USB-ключи Aladdin eToken Pro/Java, смарт-карты Aladdin eToken PRO/SC, USB-ключи Рутокен (Rutoken), USB-ключи и смарт-карты JaCarta, USB-ключи и смарт-карты ESMART Token ГОСТ.

(рис. 58).

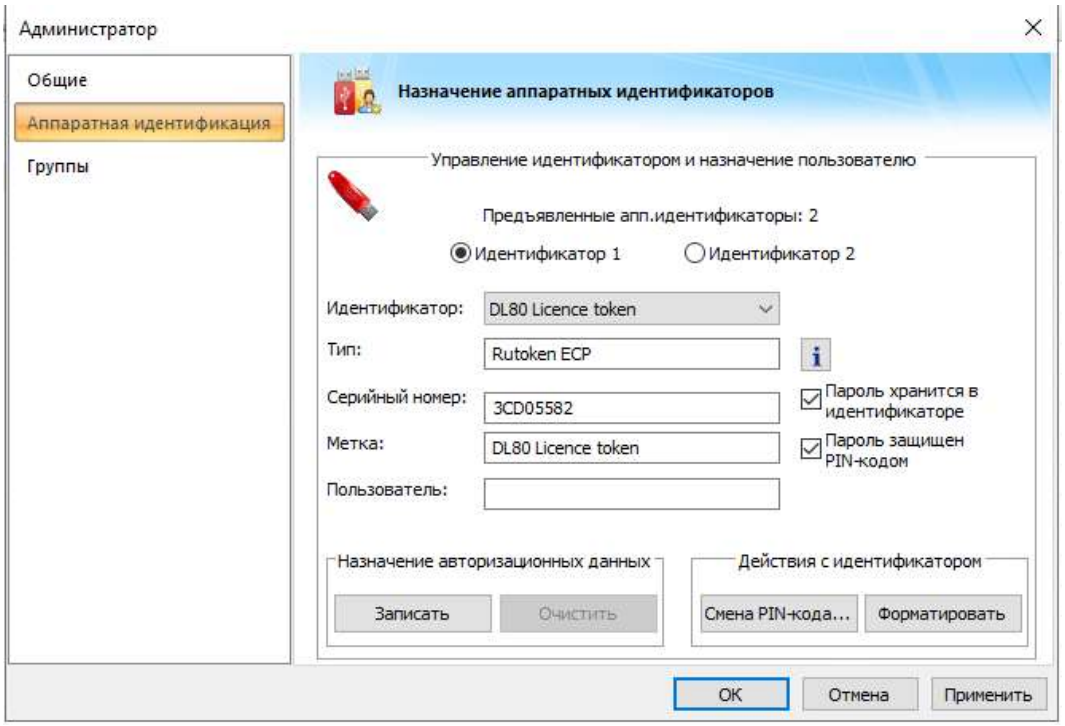


Рис. 58. Параметры назначенного идентификатора

После выбора идентификатора для пользователя необходимо нажать «Применить» и «OK». Для установки второго идентификатора следует проделать действия выше с активным полем «Индентификатора 2». Таким образом, после назначения идентификатора для учетной записи для входа в ОС помимо ввода авторизационной информации, станет необходимо предъявить и назначенный аппаратный идентификатор.

После выбора предъявленного идентификатора дополнительная кнопка  позволяет открыть окно с информацией о параметрах данного идентификатора.

Примечание. Для аппаратных идентификаторов Рутокен в СЗИ Dallas Lock 8.0 существует возможность записи авторизационных данных пользователя без заполнения поля PIN-кода идентификатора, если на идентификаторе установлен PIN-код по умолчанию.

4.3.2 Принудительная двухфакторная аутентификация

В системе защиты Dallas Lock 8.0 для учетной записи пользователя или группы пользователей может быть установлена обязательная двухфакторная аутентификация для входа в ОС: аутентификация с вводом пароля и предъявлением назначенного аппаратного идентификатора.

Функционально для обязательной двухфакторной аутентификации необходимо выполнение двух условий:

1. Для параметра сложности паролей «Пароли: минимальная длина» не должно быть установление значение «Не используется».
2. Для параметра безопасности «Учетные записи: Принудительная двухфакторная аутентификация» в значении должны быть выбраны необходимые учетные записи пользователей или группы.

За последнее отвечает параметр «Учетные записи: Принудительная двухфакторная аутентификация» («Параметры безопасности» → «Права пользователей»). Если в значении данного параметра стоит определенная учетная запись или группа, то при регистрации новой учетной записи (в составе данной группы или индивидуально) присвоение идентификатора будет обязательным, иначе будет выведено предупреждение об ошибке.

4.3.3 Снятие аппаратной идентификации

Для того, чтобы снять назначение аппаратного идентификатора для учетной записи отдельного пользователя, необходимо на закладке «Аппаратная идентификация» окна параметров учетной

записи в меню отображения имени идентификатора выбрать значение «Аппаратный идентификатор не назначен», нажать «Применить» и «ОК».

Сам идентификатор для последующего применения рекомендуется очистить от авторизационных данных, если они были назначены (см. ниже), или отформатировать.

4.3.4 Действия с идентификатором

Для идентификаторов типа **USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ; USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен PINPad, Рутокен ЭЦП 3.0, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X)** доступны дополнительные расширенные возможности аппаратной идентификации.

Для работы с данными аппаратными идентификаторами необходимы **их авторизационные PIN-коды:** PIN-код администратора и PIN-код пользователя, которые уже установлены в памяти самих идентификаторов по умолчанию (так называемые «заводские настройки»). Информацию о них можно получить из документации, поставляемой вместе с аппаратными идентификаторами и драйверами.

Для обеспечения требуемого уровня безопасности данные PIN-коды следует изменить. Это можно также сделать, воспользовавшись специальной утилитой для идентификатора, либо используя окно параметров назначенного пользователю идентификатора в оболочке администратора системы защиты. Для этого в поле «Действия с идентификатором» необходимо выбрать кнопку «Смена PIN-кода» или кнопку «Форматировать».

По нажатию кнопки «Смена PIN-кода» откроется окно, в котором необходимо ввести значения PIN-кода пользователя: старое (текущее) значение, новое значение и повтор. Дополнительные кнопки рядом с полями ввода позволят изменить скрытые под звездочками символы на явные, повтор ввода PIN-кода в этом случае не потребуется (рис. 59).

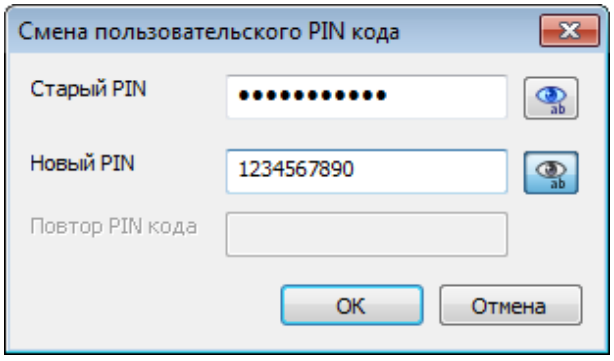


Рис. 59. Окно смены PIN-кода

По нажатию кнопки «Форматировать» откроется окно форматирования аппаратного идентификатора (рис. 60), в котором необходимо заполнить следующие поля:

- **Текущий PIN-код администратора** данного аппаратного идентификатора, необходимый для легального форматирования идентификатора;

Ввести новые данные:

- **Метка** — любое наименование;
- **Новый PIN-код** администратора и повтор;
- **Новый PIN-код** пользователя и повтор.

Если два данных PIN-кода должны совпасть, то флаг в поле «PIN-код администратора и пользователя совпадают» позволит ввести PIN-код только в одно поле.

Внимание! Параметры символов PIN-кода для идентификатора (наличие цифр, букв и другие) определяются настройкой параметров в утилите соответствующего идентификатора. И прежде чем изменять PIN-коды идентификатора, следует настроить данные параметры именно в утилите, которые по умолчанию **выключены.**

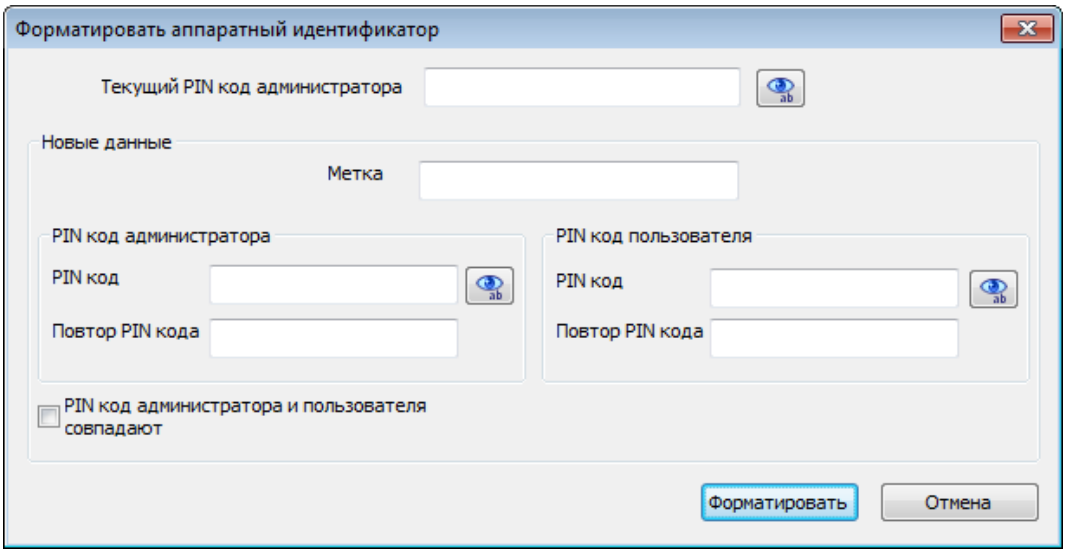


Рис. 60. Окно форматирования идентификатора

Примечание. Для аппаратных идентификаторов Рутокен. Форматировать идентификатор в СЗИ Dallas Lock 8.0 возможно только после форматирования идентификатора в «Панели управления Рутокен» с выбором опции: «Смену PIN-кода пользователя может производить: Администратор» или «Смену PIN-кода пользователя может производить: Пользователь и Администратор». Предварительно отформатированные производителем или в «Панели управления Рутокен» идентификаторы с параметром: «Смену PIN-кода пользователя может производить: Пользователь» — невозможно форматировать через СЗИ из-за ограничений, заданных производителем идентификаторов Рутокен.

Примечание. Форматирование устройства JaCarta-2 ГОСТ должно выполняться только с использованием ПО «АРМ администратора безопасности JaCarta-2 ГОСТ».

4.3.5 Поддержка биометрии

Для идентификаторов типа **USB-ключи и смарт-карты JaCarta PKI/BIO** доступны дополнительные расширенные возможности по поддержке биометрии.

Внимание! Для работы с биометрическими данными при установке Единого клиента JaCarta необходимо на шаге выбора компонентов для установки убедиться, что компонент «Поддержка биометрии» отмечен, как устанавливаемый.

Для обеспечения требуемого уровня безопасности данные PIN-коды следует изменить (см. «Действия с идентификатором»).

По нажатию кнопки «Форматировать» откроется окно установки типа авторизации, в котором необходимо выбрать:

- **Тип авторизации пользователя.** В выпадающем меню доступны следующие типы авторизации:
  - PIN-код — аутентификация по PIN-коду;
  - Биометрия — аутентификация по отпечаткам пальцев;
  - PIN-код или биометрия — аутентификация по одному из вышеперечисленных способов;
  - PIN-код и биометрия — аутентификация с использованием обоих способов.
- **Количество отпечатков пальцев пользователя.** В выпадающем меню доступны значения от 1 до 10.

Далее откроется окно форматирования аппаратного идентификатора (рис. 60), поля в котором надо заполнить способом, приведенным в «Действия с идентификатором».

После завершения форматирования появится окно регистрации отпечатков (рис. 61).

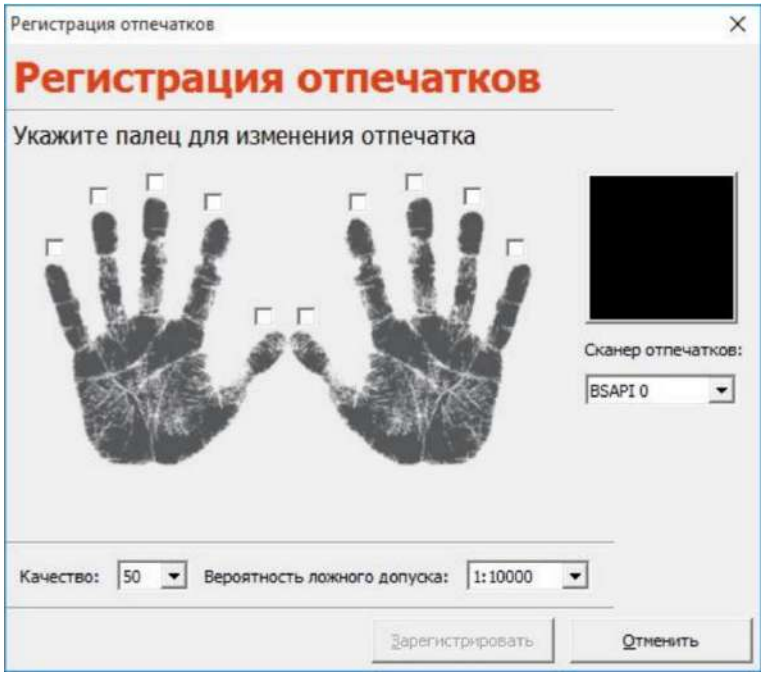


Рис. 61. Окно регистрации отпечатков

Порядок регистрации отпечатков:

- указать палец путем установки флага,
- приложить палец к сканеру при появлении соответствующей надписи,
- убрать палец со сканера при появлении надписи об успешном создании шаблона,
- повторно приложить палец к сканеру для проверки созданного шаблона.

Также доступны для изменения параметры качества сканирования[8] и вероятности ложного допуска[9]. Данные параметры можно выбрать в выпадающем меню.

При необходимости регистрации нескольких отпечатков пальцев нужно повторить процедуру регистрации, после чего нажать кнопку «Зарегистрировать». Появится окно с сообщением о том, что отпечаток зарегистрирован.

Запись биометрических данных в идентификатор

Для записи в память идентификатора биометрических данных пользователя и защиты хранимых данных необходимо выполнить следующее:

1. После выбора в выпадающем списке необходимого идентификатора отметить флагом поле «Пароль хранится в идентификаторе». Поле «Пароль защищен PIN-кодом» выделится автоматически. Далее — нажать кнопку «Записать» (Рис. 62).

[8] Данный параметр определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться (подробнее см. Единый клиент JaCarta «Руководство администратора»).

[9] Данный параметр обозначает вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя (подробнее см. Единый клиент JaCarta «Руководство администратора»).

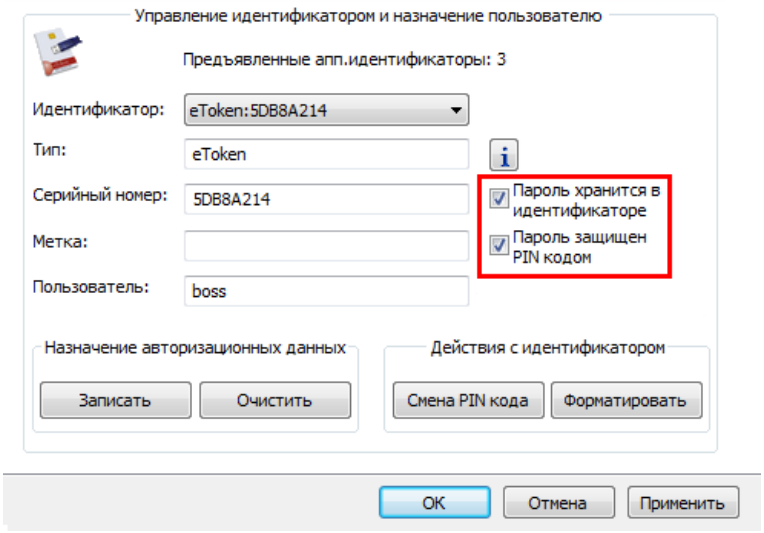


Рис. 62. Запись биометрических данных

2. В появившемся окне ввести дополнительную информацию: пароль пользователя (рис. 63), нажать «OK».

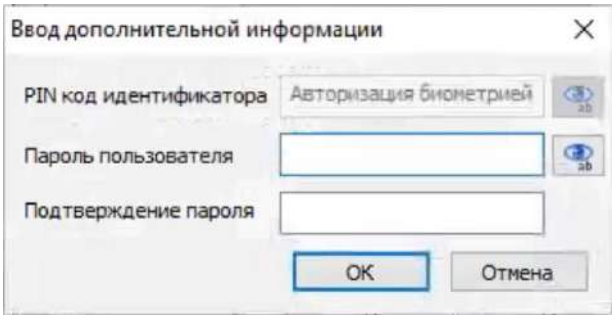


Рис. 63. Ввод дополнительной информации

3. В появившемся окне авторизации для подтверждения действий с помощью PIN-кода и/или биометрии, согласно произведенным настройкам типа, необходимо указать запрашиваемые данные и нажать «Подтвердить».
4. В окне параметров учетной записи системы защиты нажать «Применить» и «OK».
5. После этого в память данного идентификатора будет прописан логин учетной записи пользователя и его биометрические данные, причем данные будут защищены паролем самого пользователя.

Теперь для входа в ОС после предъявления идентификатора пользователю необходимо заполнить только поле ввода PIN-кода и выполнить проверку биометрических данных в зависимости от типа установленной авторизации (см. «Вход с аппаратным идентификатором»).

4.3.6 Запись авторизационных данных в идентификатор

Запись авторизационных данных в память идентификатора доступна для следующих типов: **USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ; USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен PINPad, Рутокен ЭЦП 3.0, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X).**

Записать в память аппаратного идентификатора авторизационные данные (логин и пароль) учетной записи пользователя, которому он назначается, можно тремя способами:

1. Записать в память идентификатора логин и пароль пользователя и хранение данных защитить PIN-кодом. Для этого необходимо выполнить следующее. После выбора в выпадающем списке необходимого идентификатора отметить флагом поле «Пароль хранится в идентификаторе».

Поле «Пароль защищен PIN-кодом» выделится автоматически. Далее — нажать кнопку «Записать» (рис. 64).

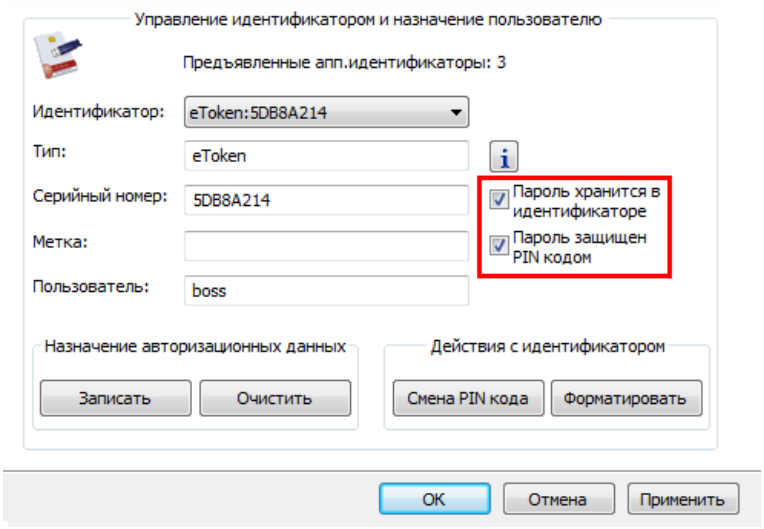


Рис. 64. Запись авторизационной информации в идентификатор

В появившемся окне ввести дополнительную информацию: PIN-код пользователя идентификатора и пароль пользователя (рис. 65), нажать «OK».

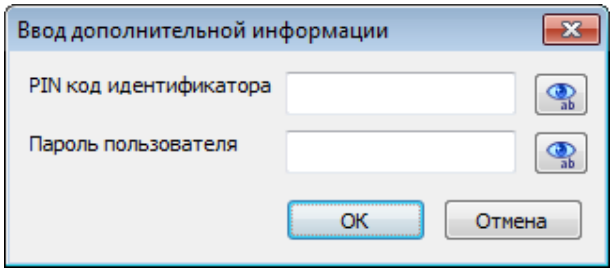


Рис. 65. Ввод дополнительной информации

В окне параметров учетной записи системы защиты нажать «Применить» и «OK».

После этого в память данного идентификатора будет прописан логин и пароль учетной записи пользователя, причем пароль будет защищен PIN-кодом самого идентификатора.

Теперь для входа в ОС после предъявления идентификатора пользователю необходимо заполнить только поле ввода PIN-кода (логин и пароль считаются автоматически, для считывания пароля потребуется ввод PIN-кода).

2. Записать в память идентификатора логин и пароль учетной записи. Для этого необходимо выполнить следующее. В поле «Пароль защищен PIN-кодом» снять флаг, и таким образом записать авторизационные данные (кнопка «Записать»). Но в этом случае пароль учетной записи в идентификаторе будет незащищен, и система выдаст предупреждение. Таким образом, для входа в ОС пользователю станет достаточным только предъявление идентификатора (логин и пароль считаются автоматически).
3. Записать в память идентификатора только логин учетной записи пользователя. Для этого не требуется выделение полей хранения паролей. Достаточно нажатия кнопки «Записать». Система потребует ввести дополнительно только PIN-код пользователя данного идентификатора. При входе в ОС после предъявления идентификатора учетная запись будет однозначно идентифицирована с логином данного конкретного пользователя, остальные авторизационные поля пользователю необходимо будет ввести самостоятельно.

Для того, чтобы стереть авторизационную информацию из памяти идентификатора, нужно воспользоваться одним из следующих способов:

- Воспользоваться кнопкой «Очистить» в поле назначения авторизационных данных.
- Отформатировать идентификатор методом, описанным выше. В этом случае помимо удаления системой защиты авторизационных данных из памяти идентификатора администратору безопасности необходимо изменить PIN-коды идентификатора.

Авторизация с записанными данными возможна при входе в ОС после включения компьютера, а также при входе при разблокировке и терминальном подключении.

Вход в ОС ЗАРМ с использованием аппаратного идентификатора — см. «Вход с аппаратным идентификатором».

4.3.7 Определение принадлежности идентификатора

В СЗИ Dallas Lock 8.0 реализован механизм, с помощью которого, предъявив аппаратный идентификатор, можно определить, какому пользователю он принадлежит.

Чтобы открыть окно с информацией об идентификаторе, необходимо сначала его предъявить (приложить к считывателю или вставить в USB-порт). Далее в оболочке администратора на вкладке «Учетные записи» необходимо нажать кнопку «Определить принадлежность аппаратного идентификатора» (рис. 66).

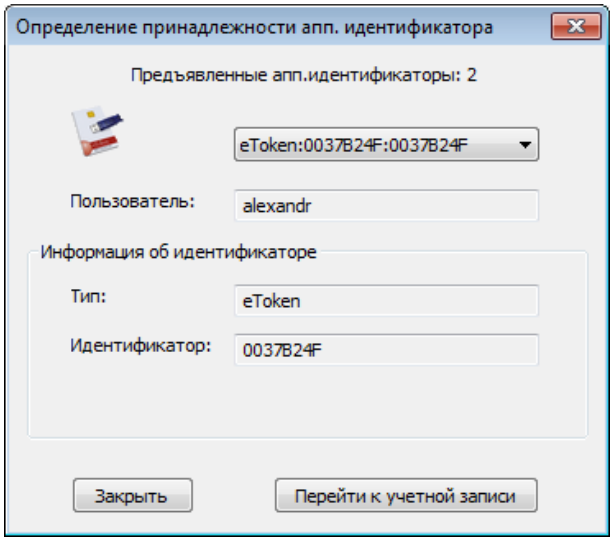


Рис. 66. Окно свойств предъявленного идентификатора

В появившемся окне после выбора из выпадающего списка идентификатора появится информация о его типе и владельце. Если владелец определен, то из данного окна можно перейти к просмотру и редактированию учетной записи пользователя, которому идентификатор назначен.

4.4 Параметры входа

4.4.1 Разрешение и запрет интерактивного и удаленного входов в ОС

СЗИ Dallas Lock 8.0 обеспечивает защиту информации от НСД на ПК в ЛВС через локальный, терминальный и сетевой входы.

Выполнить настройку разрешения или запрета интерактивного, или удаленного входов в ОС данного ПК можно, развернув на вкладке «Параметры безопасности» категорию «Права пользователей». С помощью параметров безопасности «Интерактивный вход: разрешен/запрещен» и «Удаленный вход: разрешен/запрещен» определенным пользователям и группам можно запретить или разрешить локальный или удаленный вход в ОС.

Добавить учетные записи в список разрешенных или запрещенных можно, выбрав параметр и нажав кнопку «Свойства».

При настройке следует учесть, что установленный параметр запрета имеет более высокий приоритет перед установленным параметром разрешения. Также следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

Правило разрешения и запрета действий следующее:

Условие	Результат
Нет никаких запретов и разрешений	Действие запрещено
Есть запись о разрешении и нет записи о запрете	Действие разрешено
Есть запись о запрете	Действие запрещено, несмотря на наличие или отсутствие записи о разрешении

В списке субъектов, для которых устанавливается запрет или разрешение, определяется иерархия в порядке возрастания: группа «Все» → индивидуальная группа → учетная запись (доменная учетная запись «по маске») → пользователь.

Таким образом, чтобы субъекту (например, пользователю) действие было разрешено, то он не должен входить в состав субъекта (например, группы), для которого это действие имеет явный

запрет.

Пример:

Требуется настроить запрет входа в ОС для локальных пользователей (в доменной архитектуре).

Для запрета входа локальных пользователей необходимо изменить параметр «Интерактивный вход: разрешен» убрать учетную запись «Все» и добавить учетную запись «**». Если есть необходимость разрешения входа для пользователей определенного домена, то предварительно нужно создать учетную запись в виде «Имя_домена*» (см. «Регистрация доменных учетных записей по маске»).

4.4.2 Настройка параметров входа

После установки системы защиты, необходимо произвести ее настройку. Под настройкой системы защиты понимается установка значений параметров системы защиты, удовлетворяющих политикам безопасности предприятия.

Для этого необходимо выбрать вкладку «Параметры безопасности».

Настройки, касающиеся входа в систему, установки атрибутов пароля, аппаратных считывателей, регулируются в окне закладки «Вход» (рис. 67).

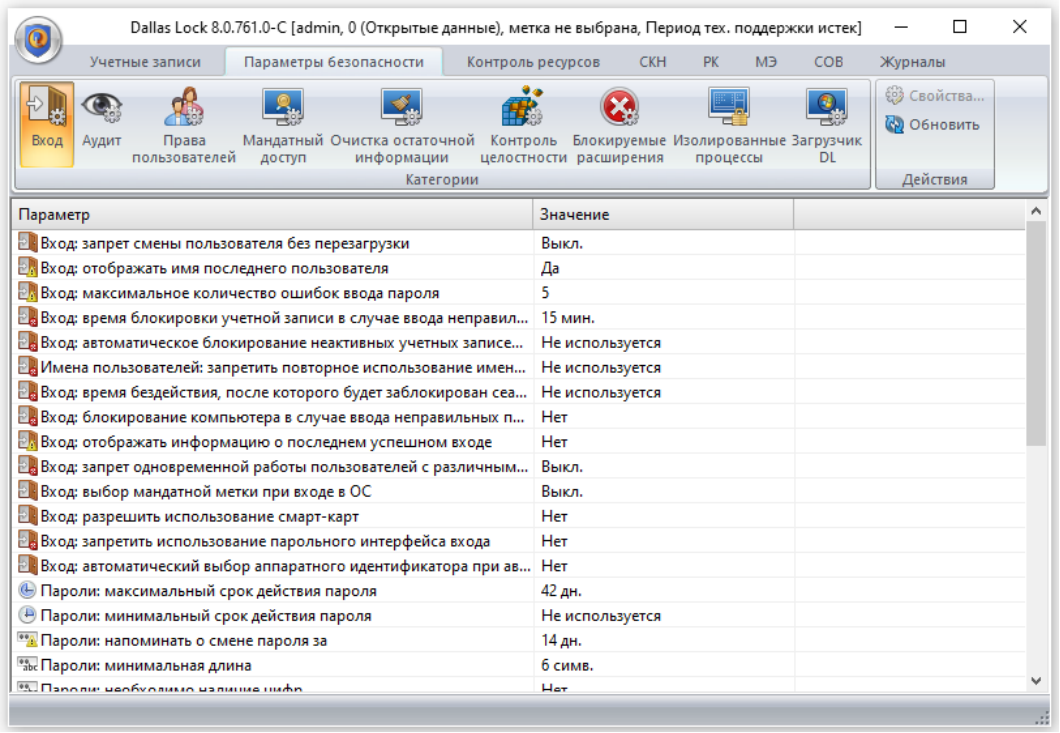


Рис. 67. Список параметров входа

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров на вход.

Вход: запрет смены пользователя без перезагрузки
Включение данного параметра не позволит осуществлять смену учетных записей пользователей без перезагрузки ПК. Если параметр имеет значение «Вкл.», то при выборе завершения сеанса или смены пользователя ПК автоматически уходит в перезагрузку. Если параметр имеет значение «Выкл.», то при выборе завершения сеанса или смены пользователя ПК выйдет из учетной записи и предложит снова ввести авторизационные данные (см. «Запрет смены пользователя без перезагрузки»).
Вход: отображать имя последнего пользователя
Включение данного параметра позволяет отображать в окне авторизации имя учетной записи последнего пользователя, осуществлявшего вход в ОС. Если параметр имеет значение «Да», то в поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет отображаться имя последнего пользователя данного ПК. Если параметр имеет значение «Нет», то поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет пустым.

Настройки данного параметра может перекрывать активизированный параметр «Настройки автоматического входа в ОС» при включении модуля «Загрузчик DL» (для Dallas Lock 8.0-С).

Вход: максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. В выпадающем списке можно выбрать число попыток от 1 до 10.

Если при входе на ЗАРМ или на этапе загрузки ОС пользователь ввел неверный пароль, то система выдаст предупреждение «Указан неверный пароль». Если число ошибок больше допустимого, учетная запись будет заблокирована и пользователь не сможет загрузить компьютер и ОС. При этом система защиты выдаст сообщение «Запись пользователя заблокирована».

Способы блокировки описаны в разделе «Заблокированные пользователи».

Если установлено значение «Не используется», то пользователь может вводить неверный пароль неограниченное число раз.

Вход: время блокировки учетной записи в случае ввода неправильных паролей

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить компьютер и ОС, даже при верном вводе пароля.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Если при настройке опции выбрано значение «Не используется», то разблокировать учетную запись и тем самым позволить пользователю вновь работать на ЗАРМ, может только администратор безопасности.

Вход: автоматическое блокирование неактивных учетных записей пользователей

Данный параметр позволяет настроить и выполнить автоматическую блокировку неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования. При активации данной политики на СБ выполняется блокировка неактивных учетных записей пользователей в рамках ДБ для всех клиентов данного домена.

По умолчанию значение данного параметра: «Не используется».

Есть возможность установить значение параметра: от 1 до 90 дней. По прошествии установленного времени неиспользования неактивная учетная запись блокируется.

Имена пользователей: запретить повторное использование имени пользователя в течение

Включение данного параметра устанавливает запрет на повторное использование имени пользователя при регистрации новой учетной записи. По умолчанию значение данного параметра: "Не используется".

В выпадающем списке возможно выбрать длительность запрета от 1 года до 50 лет, либо установить значение «Навсегда».

Примечание. Если клиент введен в ДБ, то данная политика работает только на уровне СБ.

Вход: время бездействия, после которого будет заблокирован сеанс доступа

Данный параметр определяет время бездействия пользователя, по прошествии которого сеанс доступа данного пользователя будет заблокирован.

По умолчанию значение данного параметра: «Не используется».

Есть возможность из выпадающего списка установить время бездействия от 1 мин до 5 ч.

Вход: блокирование компьютера в случае ввода неправильных паролей

Данный параметр позволяет настроить блокирование компьютера в случае ввода пользователем неправильных паролей.

Параметр может принимать значение «Да» или «Нет» (установлено по умолчанию).

После включения данного параметра безопасности при вводе неправильных паролей компьютер блокируется. В таком случае авторизоваться на этом компьютере может только суперадминистратор. Чтобы разблокировать компьютер, необходимо через контекстное меню BlockIcon выполнить команду «Разблокировать компьютер» (Рис. 68) либо, если компьютер в ДБ, выполнить команду «Разблокировать клиента» в контекстном меню консоли СБ (Рис. 69).

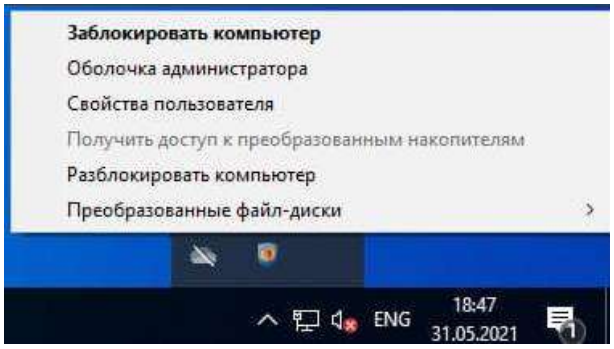


Рис. 68. Контекстное меню BlockIcon

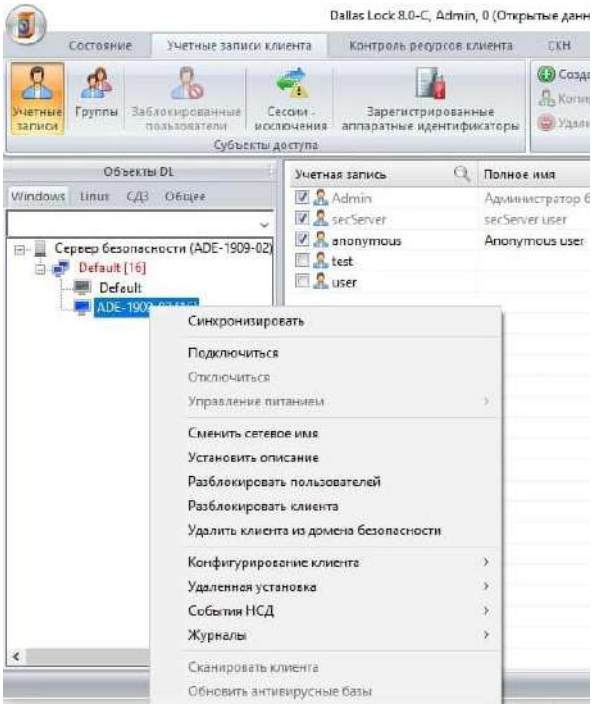


Рис. 69. контекстном меню консоли СБ

Вход: отображать информацию о последнем успешном входе

При включении данного параметра входа (значение «Да») после загрузки ОС в области уведомлений Windows на панели задач будет появляться сообщение с информацией о дате последнего входа пользователя на данный компьютер, типе входа: сетевой, локальный, терминальный, неуспешных попытках входа и состоянии параметров учетной записи пользователя (рис. 70).

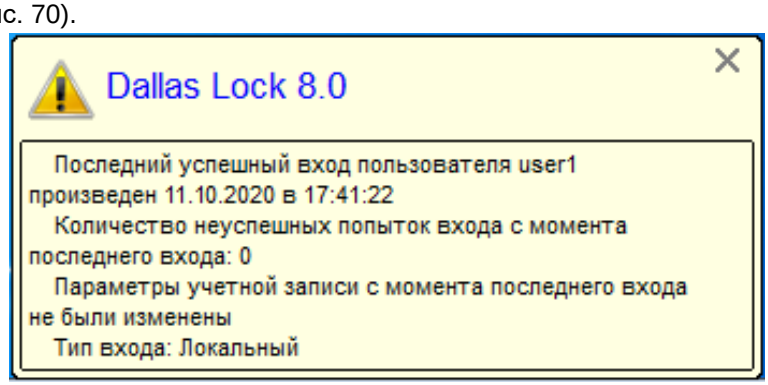


Рис. 70. Всплывающее уведомление о последнем успешном входе

Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа

Данный параметр доступен только для Dallas Lock 8.0 редакции «С»

При включении запрета одновременной работы пользователей с различными уровнями или метками мандатного доступа на данном ПК будет возможна одновременная работа нескольких интерактивных пользователей, зашедших только под одним уровнем доступа или мандатной метки. Причем данный уровень будет определяться по уровню или метке первого пользователя, зашедшего на данный компьютер.

Примечание. Если при включении запрета, есть уже запущенные сессии с различными уровнями доступа или мандатными метками, рекомендуется выполнить перезагрузку компьютера. Если не следовать данной рекомендации, может получиться, что суперадминистратор при блокировании своей запущенной сессии не сможет ее разблокировать в виду вступления в действия имеющегося ограничения.

Вход: выбор мандатной метки при входе в ОС

Включение данного параметра разрешает использование мандатных меток для авторизации в ОС Windows.

Вход: разрешить использование смарт-карт

Включение данного параметра разрешает использование микропроцессорных смарт-карт для авторизации в ОС Windows, при работе ПК в корпоративном домене. Смарт-карты применяются вместе с личными идентификационными номерами (PIN-кодами).

Вход: запретить использование парольного интерфейса входа

При использовании смарт-карт для авторизации в ОС возможно отключить интерфейс входа по имени пользователя и паролю, Включением данного параметра.

Вход: автоматический выбор аппаратного идентификатора при авторизации

Включение данного параметра позволит автоматически выбрать подключенный аппаратный идентификатор при авторизации.

Пароли: максимальный срок действия пароля

Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока СЗИ автоматически предложит пользователю сменить пароль при входе в ОС. Если выбрано значение «Не используется», то время действия пароля не ограничено.

В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

Максимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме:

- Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера этим пользователем система защиты обязательно потребует сменить пароль, даже если срок действия пароля не истек (наивысший приоритет).
- Если администратором для конкретного пользователя ***установлено*** значение: **Пароль без ограничения срока действия**, и отсутствует требование смены пароля при следующем входе, то СЗИ не потребует смены пароля даже в случае превышения максимального срока действия пароля.
- Если администратором для конкретного пользователя ***не установлено*** значение: **Пароль без ограничения срока действия**, и отсутствует требование смены пароля при следующем входе, то СЗИ потребует от данного пользователя сменить пароль по истечении максимального срока действия пароля (низший приоритет).

Пароли: минимальный срок действия пароля

Данным параметром устанавливается минимальный срок действия пароля для всех

пользователей. До истечения установленного срока СЗИ не позволит пользователю сменить свой пароль. При выборе значения «Не используется» минимальный срок действия пароля не ограничен.

В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля.

Минимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме:

- Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера этим пользователем система защиты обязательно потребует сменить пароль (наивысший приоритет).
- Если отсутствует требование смены пароля при следующем входе, то СЗИ не позволит сменить пароль, если не истек установленный минимальный срок действия пароля. При этом на экране отобразится сообщение «Пароль не может быть изменен».
- Флаг в поле «Пароль без ограничения срока действия», установленный в настройках учетной записи, не даст возможности сменить пароль до окончания установленного минимального срока действия пароля.
- Если нарушено соотношение максимального и минимального сроков действия пароля (минимальный срок больше максимального), то СЗИ проигнорирует значение минимального срока действия пароля.

Пароли: напоминать о смене пароля за

С помощью данного параметра система защиты позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль. Если при настройке выбрать значение «Не используется», то напоминаний о необходимости смены пароля не будет.

Напоминание о предстоящей смене пароля будет появляться на экране при загрузке ОС данным пользователем, начиная с того момента, когда до смены пароля (фактически до истечения максимального времени действия пароля) осталось количество дней, равное установленному значению для этой политики.

Примечание. Параметры, устанавливающие срок действия пароля, действуют независимо от аналогичных параметров ОС Windows. В Windows действуют свои политики безопасности, которые также могут потребовать смены пароля, независимо от Dallas Lock.

В Dallas Lock и ОС Windows совпадают следующие парольные политики:

- максимальный срок действия пароля,
- минимальная длина пароля,
- минимальный срок действия пароля,
- пароль должен отвечать требованиям сложности.

Чтобы не возникало конфликта парольных политик ОС Windows и Dallas Lock, нужно сделать данные политики идентичными в ОС и СЗИ, либо отключить политики в ОС.

Пароли: минимальная длина

Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение. При выборе значения «Не используется» устанавливаемый пароль может иметь пустое значение. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

При регистрации нового пользователя и при изменении старого пароля система защиты контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Ввод пароля: введен слишком короткий пароль».

Следует иметь в виду, что если в процессе работы изменено значение длины пароля (например, увеличено), то у зарегистрированных пользователей она останется прежней до первой смены ими пароля.

По умолчанию минимальная длина пароля составляет 6 символов.

Пароли: необходимо наличие цифр

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при смене пароля на «password**d**» выведется сообщение «В пароле должны содержаться цифры». Правильной будет смена пароля, например, с «password» на «password**12**».

Пароли: необходимо наличие специальных символов

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать специальные символы из следующего списка: "`", "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/".

Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример. Если у пользователя имеется пароль «password1», и если выше описанная опция активирована, то при смене пароля на «password**2**» выведется сообщение «В пароле должны содержаться спецсимволы». Правильной будет смена пароля, например, с «password1» на «password#».

Пароли: необходимо наличие строчных и прописных букв

Если данный параметр включен (значение «Да»), то при создании пароля в нем должны присутствовать строчные и прописные буквы. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример: Если у пользователя имеется пароль «password1», и, если выше описанная опция активирована, то при смене пароля на «pacsword1» выведется сообщение «В пароле должны содержаться и строчные, и прописные буквы». Если пользователь сменит пароль «password1» на «pa**C**sword1», то операция успешно завершится.

Пароли: необходимо отсутствие цифры в первом и последнем символе

Если данный параметр включен (значение «Да»), то при создании пароля на месте первого и последнего символа в нем не должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пароли: необходимо изменение пароля не меньше, чем в

Данным параметром задается количество символов, на которое, как минимум, должен отличаться новый пароль от старого, при его смене.

Если данный параметр включен, то при смене пароля через комбинацию клавиш «Ctrl + Alt + Del», новый пароль должен отличаться от старого не менее, чем на указанное количество символов. Сверка старого и нового пароля осуществляется посимвольно.

При смене пароля через оболочку администратора Dallas Lock 8.0 данный параметр не учитывается.

Пример. У пользователя имеется пароль «password1», если в выше описанной опции количество символов указано 2, то при смене пароля «password1» на «password**2**» выведется сообщение «Пароль должен сильнее отличаться от предыдущего». Если пользователь сменит пароль «password1» на «**P**assword**2**», то выведется сообщение «Пароль был успешно изменен» так как отличие старого пароля от нового составляет 2 символа.

Примечание. Следует учесть, что в ОС Windows есть свои, независимые политики сложности пароля. И в некоторых случаях пароль может удовлетворять политикам Dallas Lock, но не удовлетворять политикам Windows. В данном случае такой пароль установить не удастся.

Домен безопасности

Данный параметр позволяет вводить и выводить ПК из ДБ (см. «Ввод защищенного компьютера в ДБ»). Если ПК не введен в ДБ, то параметр имеет значение «Не задан». В свойствах параметра необходимо ввести имя ПК, на котором размещен СБ, и ключ доступа (по умолчанию имеет пустое значение).

После ввода в ДБ значение параметра принимает имя СБ. Для вывода из ДБ необходимо ввести ключ доступа к Серверу безопасности. Об установке ключа доступа к СБ — в разделе «Ключ доступа к СБ».

Сервер конфигураций

Данный параметр позволяет вводить и выводить ПК из СК (см. «Сервер конфигураций»). Если ПК не введен в СК, то параметр имеет значение «Не задан». В свойствах параметра необходимо

ввести имя СК, указан логин и пароль для доступа. После ввода в СК значение параметра принимает имя СК.
Сеть: Ключ защиты сетевого взаимодействия
Данным параметром устанавливается значение ключа защиты сетевого взаимодействия для удаленного входа на другие ЗАРМ (см. «Ключи защиты сетевого взаимодействия»).
Сеть: Время хранения сетевого кэша
Для увеличения скорости работы по сети система защиты Dallas Lock 8.0 предоставляет возможность сохранения сетевого кэша с информацией об имеющихся в сети тех компьютеров, которые защищены Dallas Lock 8.0, и к которым уже было произведено обращение с данного ПК. В выпадающем списке данного параметра можно выбрать время хранения такого сетевого кэша.
Сеть: Список незащищенных серверов
С помощью данного параметра для увеличения скорости работы по сети, чтобы сократить количество обращений, СЗИ предоставляет возможность сохранить постоянный список ПК, которые не защищены СЗИ. Вводятся имена ПК и серверов или их IP-адреса через точку с запятой.
Настройка считывателей аппаратных идентификаторов
С помощью данного параметра производится настройка считывателей электронных идентификаторов. Предварительно необходимо установить соответствующие драйверы и предъявить идентификаторы.
Блокировать компьютер при отключении аппаратного идентификатора
При включении данного параметра всем пользователям, которым назначен аппаратный идентификатор, работа на данном ПК при отключении идентификатора будет заблокирована. Параметр не распространяется на идентификаторы, предъявляемые по касанию.
Блокировать файл-диски при отключении аппаратного идентификатора
Если при создании файл-диска (см. «Преобразованные файл-диски») помимо пароля, используется аппаратный идентификатор, то при отключении идентификатора от ПК, файл-диск также будет отключен. Стоит учитывать, что при изменении настроек аппаратного идентификатора необходимо начать новый сеанс работы пользователя для выполнения корректной блокировки. Параметр не распространяется на идентификаторы, предъявляемые по касанию.
Текст сообщения при входе
В окне данного параметра имеется возможность ввести текст предупреждения, которое будет отображаться пользователю до входа в ОС. Смысл данного текста должен предупреждать о реализации мер по обеспечению безопасности информации, и о необходимости соблюдения установленных правил обработки информации. Нажатие «ОК» пользователем будут означать подтверждение ознакомления.
Использовать авторизационную информацию от СДЗ Dallas Lock
При включении данного параметра автоматически используется авторизационная информация от СДЗ Dallas Lock. Параметр доступен только при установленной аппаратной плате. Для работы параметра необходимо в ОС установить драйвер для СДЗ.
Блокировать автозапуск подключенных устройств
При включении данного параметра автоматически блокируется возможность запуска без команды пользователя (автозапуска) устройства при подключении. По умолчанию установлено значение «Нет».
Блокировать подключение незарегистрированных накопителей USB Flash
Данный параметр позволяет блокировать незарегистрированные USB-Flash накопители. Возможные значения параметра: «Да» или «Нет» (установлено по умолчанию).

При включениии политики пользователю не предоставляется доступ к накопителям, в систему не устанавливаются драйверы накопителей и в реестре не регистрируется информация о подключении, в проводнике пользователь их не увидит.

Исключение для контроля приложений, печати и изолированных процессов

Список файлов, для которых не производится контроль приложений, печати и изолированных процессов.
Список — содержит имена и названия исключений, перечисленные через ";". Имена могут не содержать пути, либо включать в себя последнюю часть пути или полный путь (этот вариант наиболее безопасен). Формат значения параметра: «имя (путь), исключение;».
Список исключений:

- all — для всех компонентов;
- ips — для СОВ;
- print — для печати;
- clipboard — для изолированных процессов.

Если в любом элементе списка в качестве имени указано "*" — настройка будет активной для всех исключений.
Чтобы добавить исключение для процесса необходимо:

1. Перейти на вкладку «Параметры безопасности» → «Вход» → «Исключения для контроля приложений, печати и изолированных процессов». При двойном нажатии на параметр открывается окно «Редактирование параметров безопасности» (Рис. 71).

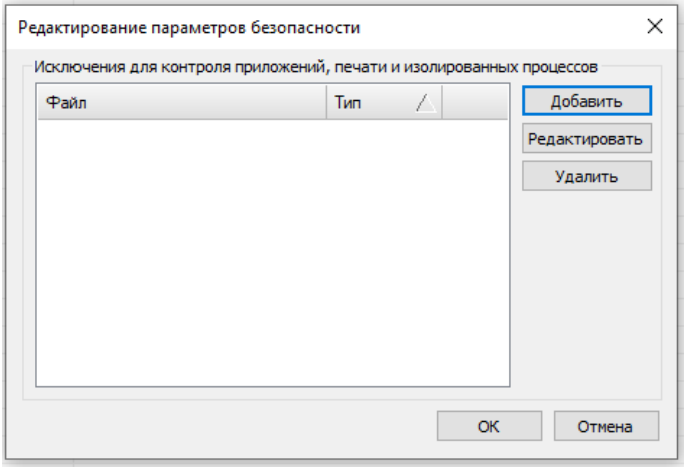


Рис. 71. Редактирование параметров безопасности

2. Нажать кнопку «Добавить», в окне «Исключение для компонента» выбрать файл, для которого создается исключение, и тип исключения (Рис. 72). Нажать «ОК».

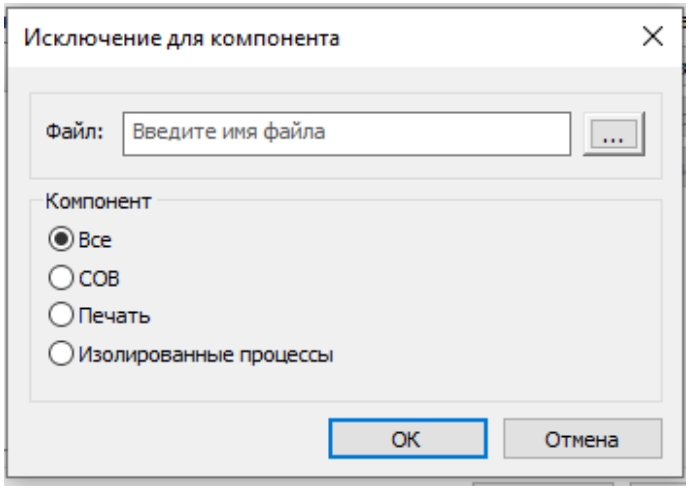


Рис. 72. Исключение для компонента

3. Выбранный файл с типом исключения отображается в окне «Редактирование параметров безопасности», нажать «ОК».

В строке «Значение» параметра «Исключения для контроля приложений, печати и изолированных процессов» будет отображаться выбранный файл и тип исключения.
Для редактирования файла исключения откройте окно «Редактирование параметров

безопасности», выделите необходимый файл, в котором необходимо изменить тип исключения, и нажмите кнопку редактировать. Для удаления процесса в окне «Редактирование параметров безопасности» выделить файл и нажать кнопку «Удалить», подтвердите удаление и нажмите «ОК».

Также добавить процесс в исключения можно, выбрав его во вкладке «Журналы» → «Журнал процессов», и нажав правой кнопкой на процесс «Добавить в исключения» и выбрать для какого компонента создается исключение.

Пример:
«ViPNet Client\Monitor.exe,all;»
«ViPNet Client\Monitor.exe,all;Notepad.exe,clipboard;»
«*,all»

4.4.3 Настройка средств аппаратной идентификации

Система Dallas Lock 8.0 позволяет в качестве средства опознавания пользователей системы использовать аппаратные идентификаторы: **USB-Flash-накопители, электронные ключи Touch Memory (iButton), HID Proximity-карты, USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ; USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен PINPad, Рутокен ЭЦП 3.0, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X).**

При настройке аппаратного идентификатора рекомендуется устанавливать драйверы, поставляемые в комплекте с идентификатором, или скачать их с сайта производителя.

Общие сведения об идентификаторах

Электронный ключ Touch Memory представляет собой микросхему, размещенную в прочном корпусе из нержавеющей стали, по размерам и форме напоминающем батарейку от электронных часов (рис. 73).

Рис. 73. Touch Memory

Фирма-производитель гарантирует, что у ключей Touch Memory не существует двух идентичных изделий (64-разрядный регистрационный номер). Аппаратная идентификация по Touch Memory возможна, только если установлена аппаратная часть. В качестве аппаратной части для работы с Touch Memory могут применяться:

- считыватель COM-A, подключаемый к COM-порту компьютера;
- считыватель COM-P, подключаемый к COM-порту компьютера.

Примечание. Идентификация по Touch Memory с помощью считывателей, подключаемых через COM-порт (COM-A, COM-P) возможна только при подключении через COM-порт, встроенный в системную плату или через кабель-преобразователь от USB на COM-порт.

Бесконтактная HID Proximity-карта представляет собой пластиковую карту со встроенной микросхемой и индивидуальным идентификационным кодом (рис. 74). Предназначена для контроля доступа и безопасной идентификации.

Примечание. Из-за особенностей работы драйверов считывателей HID (IronLogic) есть техническое ограничение на использование данного типа считывателей при авторизации через удаленный рабочий стол.

Рис. 74. Бесконтактная HID Proximity-карта

Для использования подобных карт необходимо наличие специального считывателя (в СЗИ реализована поддержка считывателей HID IronLogic Z-2).

USB-ключ Aladdin eToken Pro/Java представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 75). USB-ключ eToken PRO/Java архитектурно реализован как USB-картридер с встроенной в него микросхемой (чипом) смарт-карты. Ключ выполнен в виде брелока и напрямую подключается к USB-порту компьютера, при этом не требует для своей работы каких-либо дополнительных устройств, кроме USB-порта.

Рис. 75. Aladdin eToken Pro/Java

Смарт-карта Aladdin eToken PRO/SC представляет собой пластиковую карту со встроенной микросхемой (рис. 76). Она предназначена для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами.

Рис. 76. Смарт-карта Aladdin eToken PRO/SC

USB-ключи eToken Pro/Java и смарт-карты eToken Pro/SC имеют идентичную функциональность и выполнены на одной и той же микросхеме смарт-карты. Они одинаково поддерживаются использующими их приложениями.

Для корректной работы eToken (USB-ключей eToken Pro/Java и смарт-карт eToken Pro/SC) необходимо установить драйверы eToken PKI Client, которые находятся на диске с дистрибутивом Dallas Lock 8.0.

USB-ключи и смарт-карты Рутокен (Rutoken) и Рутокен ЭЦП, Рутокен ЭЦП 2.0 — это компактное устройство, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных (рис. 77).

Рис. 77. Rutoken

СЗИ Dallas Lock 8.0 поддерживает работу с моделями Рутокен: Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП Bluetooth, Рутокен ЭЦП PKI, Рутокен Lite, Рутокен S, Рутокен Web, Рутокен PINPad, Рутокен ЭЦП 3.0, Рутокен 2151.

Электронные USB-ключи и смарт-карты JaCarta представляют собой компактные устройства, предназначенные для обеспечения информационной безопасности корпоративных заказчиков и

частных пользователей. Подобно ПК устройства JaCarta содержат процессор и модули памяти, функционируют под управлением своей ОС, выполняют необходимые прикладные программы и хранят информацию. Микроконтроллеры для JaCarta проектируются для решения задач информационной безопасности: они обладают встроенной защищенной памятью, средствами противодействия атакам по питанию, криптографическим акселератором (рис. 78).

Рис. 78. USB-ключ JaCarta

Примечание. Для устройств JaCarta необходимо использовать версии драйверов из комплекта поставки изделия.

Смарт-карта ESMART Token представляет собой пластиковую карту со встроенной микросхемой (Рис. 79). Смарт-карта обеспечивает безопасное хранение и использование цифровых сертификатов, ключей шифрования и электронной подписи. Для работы со смарт-картой ESMART Token требуется наличие считывателя контактных смарт-карт и свободный USB-порт или RS-232 для подключения считывателя.

Рис. 79. Смарт-карта ESMART Token

USB-ключ ESMART Token представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 80). USB-ключ ESMART Token ГОСТ представляет собой комбинацию считывателя и чипа смарт-карты в виде миниатюрного устройства. Устройство подключается к ПК напрямую, отдельный считыватель смарт-карт не требуется.

Рис. 80. USB-ключ ESMART Token

NFC-метка и смарт-карта семейства MIFARE представляют собой брелок (наклейку) и пластиковую карту со встроенным чипом NFC соответственно. Для работы требуется наличие считывателя бесконтактных смарт-карт.

На диске с дистрибутивом системы защиты имеются необходимые драйверы для настройки аппаратной идентификации при работе с различными ОС.

Таблица 1. Список директорий с драйверами на диске с дистрибутивом

Название папки с дистрибутивом		Назначение
Aladdin	Athena для eToken SmartCard	Дистрибутив для установки считывателя смарт-карт eToken от поставщика компании «Аладдин»

	PKI Client	Дистрибутив для установки драйверов традиционного USB-ключа eToken PKI Client от поставщика компании «Аладдин»
ATEN UC-232A USB-COM		Дистрибутив для установки драйверов кабеля-преобразователя от USB на COM-порт Aten UC-232A (для считывателей Touch Memory, подключаемых к COM-порту)
Rutoken		Драйверы идентификаторов Рутокен
USB to Serial RDS		Дистрибутив для установки драйвера считывателя Touch Memory Aladdin RDS-02 USB
JaCarta		Дистрибутивы для установки драйверов идентификаторов JaCarta
HID		Дистрибутив для установки драйвера считывателя HID IronLogic Z-2
ESMART Token		Дистрибутив для установки драйвера идентификаторов ESMART Token
NFC		Дистрибутив для установки драйвера идентификаторов NFC

Настройка считывателей аппаратных идентификаторов

Перед настройкой идентификации с помощью аппаратных средств необходимо установить соответствующие драйверы. Установка драйверов возможна как перед установкой на ПК системы защиты Dallas Lock 8.0, так и после.

Для дальнейшей работы необходима регистрация или настройка считывателей в СЗИ.

1. После того, как считыватель аппаратного идентификатора и драйверы к нему установлены, необходимо войти в оболочку администратора, открыть «Параметры безопасности» → «Вход» → «Настройка считывателей аппаратных идентификаторов». На экране отобразится окно настройки (рис. 81).

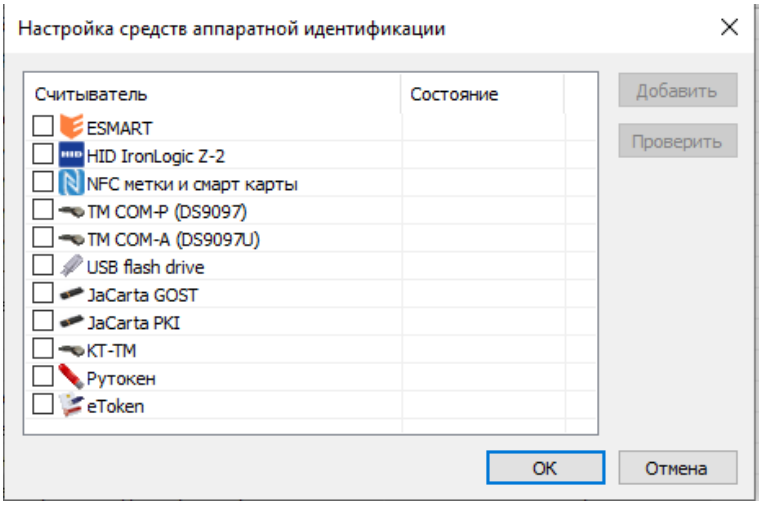


Рис. 81. Окно настройки средств аппаратной идентификации

   Окно имеет поля по настройке считывателей идентификаторов Touch Memory, USB-Flash накопитель, USB-ключи JaCarta, Рутокен, Aladdin eToken, ESMART Token, NFC метки и смарт-карты семейства MIFARE.

2. Выделив необходимый идентификатор, нужно нажать «Добавить» или поставить флаг. Кнопка «Проверить» станет активной.
3. Перед проверкой готовности идентификатора необходимо его предъявить или настроить:
   - Для настройки аппаратных идентификаторов типа Touch Memory и HID необходимо подключить аппаратный считыватель к компьютеру через COM-порт (или USB для HID считывателя) и определить с помощью Диспетчера устройств Windows номер соответствующего COM-порта (рис. 82).

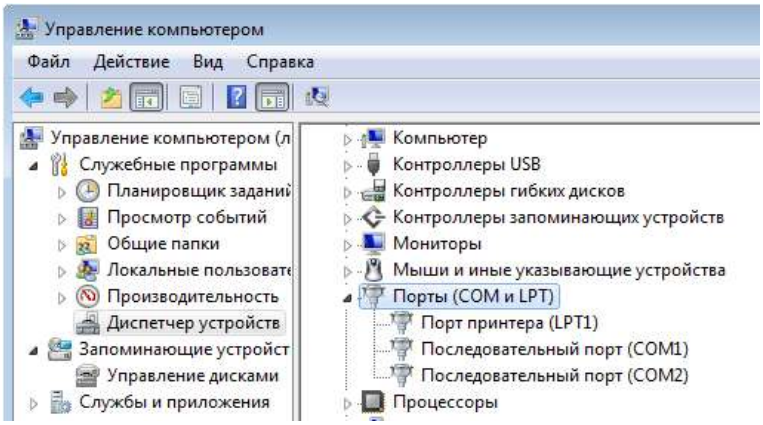


Рис. 82. Окно Диспетчера устройств Windows

В окне настройки средств аппаратной идентификации нужно выбрать название аппаратного идентификатора в списке и нажать кнопку «Добавить». На экране появится окно для выбора, соответствующего COM-порта для подключенного идентификатора (рис. 83). В окне со списком COM-портов нужно установить соответствующий флаг и нажать «ОК».

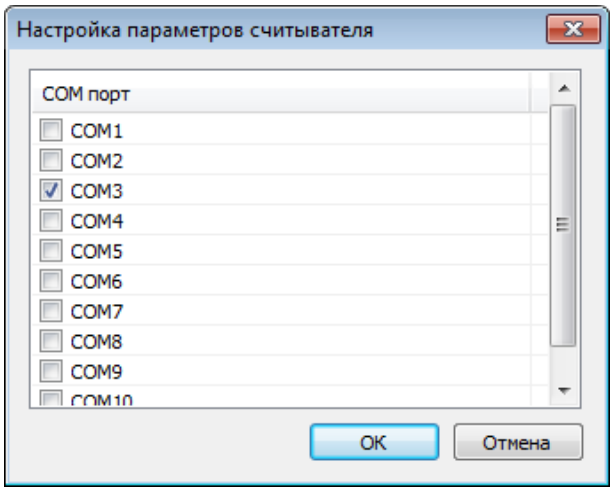


Рис. 83. Выбор COM-порта подключенного считывателя идентификатора

- Для настройки аппаратного идентификатора типа смарт-карта eToken Pro/SC к соответствующему порту необходимо подключить считыватель смарт-карты.
- Для идентификатора типа смарт-карта eToken Pro/SC флаг необходимо поставить в поле «eToken».
- Для идентификатора типа USB-ключ JaCarta флаг необходимо поставить в соответствующее идентификатору поле.
- Для идентификатора типа Рутокен флаг необходимо поставить в поле «Рутокен».
- Для настройки аппаратного идентификатора типа смарт-карта ESMART Token ГОСТ к соответствующему порту необходимо подключить считыватель смарт-карты.
- Для идентификатора типа смарт-карта ESMART Token ГОСТ флаг необходимо поставить в поле «ESMART».
- Для идентификатора типа USB-ключ ESMART Token ГОСТ флаг необходимо поставить в поле «ESMART».
- Для идентификатора типа NFC метки флаг необходимо поставить в поле «NFC метки и смарты карты».

4. После этого необходимо проверить состояние идентификатора, нажав соответствующую кнопку «Проверить» и прикоснувшись идентификатором к считывателю, или (в случае настройки USB-Flash накопителя, eToken, Рутокен, USB-ключа JaCarta, USB-ключа ESMART Token ГОСТ) подключить USB-устройство идентификатора к компьютеру. В случае успешного подключения в строке состояния появится сообщение «Готов».

После настройки подключенных к системе аппаратных идентификаторов их можно назначать в качестве средств идентификации для входа пользователя в настройках учетной записи и для преобразования информации.

Удалить настройки считывателя идентификатора можно, выбрав его из списка и нажав появившуюся кнопку «Удалить».

Примечание. Следует обратить внимание, что аппаратный идентификатор типа eToken NG-FLASH определяется в системе как USB-flash-drive.

Примечание. Для тестирования правильности подключения считывателей Touch Memory и автоматического определения типа считывателя и номера COM-порта рекомендуется использовать программу iButton Viewer version 3.20 от фирмы Dallas Semiconductors.

Следует обратить внимание, что политика безопасности «Настройка считывателей аппаратных идентификаторов» нужна для указания типа подключенных аппаратных идентификаторов в системе. На проверку идентификационной информации пользователя она не влияет. Поэтому, если, например, настроить считыватель, задать пользователю аппаратный идентификатор, а после очистить настройки аппаратных считывателей, то при входе данного пользователя аппаратный идентификатор будет проверяться все равно, и, соответственно, он не сможет войти в систему. Если пользователю задан аппаратный идентификатор, система защиты обязана его проверить, а если проверить нельзя, то допустить пользователя до информационных ресурсов система защиты не имеет права.

Внимание! При работе с аппаратными идентификаторами существуют следующие ограничения:

1. Если пользователю без прав на администрирование присвоен аппаратный идентификатор, то функция ОС «Запуск от имени…» (Run as) этому пользователю будет не доступна.
2. В случаях, когда администратору в качестве аппаратного идентификатора назначена смарт-карта, функция ОС «Запуск от имени администратора» (Run as) для данного администратора будет не доступна.

Примечание. При возникновении ошибок в процессе аутентификации и разблокировки ПК по аппаратным идентификаторам eToken PRO (32/64K) (смарт-карта) и eToken PRO (Java 72K) (смарт-карта) необходимо следующее:

1. Для разблокирования и аутентификации требуется отключить и снова подключить считыватель смарт-карты.
2. Для устранения самой ошибки следует выполнить действия:
   - **2.1.** Зайти в диспетчер устройств.
   - **2.2.** Найти «Устройство чтения смарт-карт».
   - **2.3.** Открыть «Управление электропитанием».
3. Снять флаг с «Разрешить отключение этого устройства для экономии энергии».

4.5 Загрузчик DL

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

Модуль «Загрузчик DL» нужен для предотвращения несанкционированного запуска компьютера до этапа загрузки ОС. Модуль обеспечивает высокую степень защищенности секретной и конфиденциальной информации.

Активированный модуль «Загрузчик DL» позволяет следующее:

1. Администратору безопасности следует назначить PIN-коды пользователям, необходимые для загрузки ПК.
2. Создавать преобразованные области жесткого диска.

Прозрачное преобразование дисков необходимо для защиты работы с данными на жестких дисках в обход системы защиты Dallas Lock 8.0. Данный механизм доступен только при включенном модуле «Загрузчик DL».

Модуль загрузчика DL в терминах Dallas Lock 8.0 называется загрузчиком. Авторизация в загрузчике осуществляется только по PIN-коду, без использования аппаратной идентификации.

4.5.1 Включение модуля «Загрузчик DL»

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

Примечание. До включения загрузчика DL на ПК с системой хранения данных на основе RAID следует предварительно убедиться, что используется UEFI-интерфейс BIOS и не в режиме Legacy. Поддержка Legacy BIOS в такой конфигурации загрузчиком DL не осуществляется.

Примечание. Поддержка программного RAID загрузчиком DL не осуществляется.

Для активации модуля «Загрузчик DL», необходимо в оболочке администратора выбрать вкладку «Параметры безопасности» основного меню, далее — категорию «Загрузчик DL» и нажать кнопку «Включить» (рис. 84).

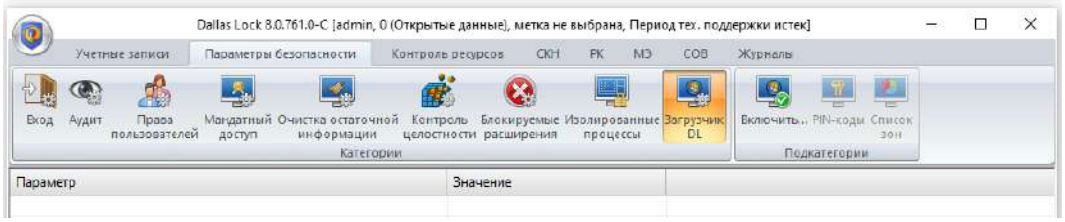


Рис. 84. Включение механизма загрузчика DL

Появится окно включения режима загрузчика DL с вводом параметров, в котором необходимо:

1. Назначить PIN-код для администратора безопасности. Этот PIN-код будет являться средством авторизации в модуле загрузчика DL. Он имеет особый статус: используя его можно выполнить операцию по аварийному восстановлению жесткого диска.

   В качестве PIN-кодов может использоваться любая комбинация символов, удовлетворяющих установленным политикам назначения пароля (см. «Настройка параметров входа»). Можно воспользоваться генератором паролей и ввести сформированный СЗИ пароль в соответствующие поля. При нажатии кнопки  скрытые символы изменятся на явные, подтверждение пароля в этом случае не потребуется и заблокируется.
2. Определить алгоритм преобразования дисков, выбрав его из выпадающего списка. После включения алгоритм изменить не удастся.
3. После установки параметров необходимо нажать «OK». Появится сообщение об успешном включении модуля загрузки и требовании перезагрузить компьютер. Следующий вход на АРМ осуществится с предварительной авторизацией в загрузчике.

Примечание. Включение загрузчика DL может занять до 10 минут.

Для выключения модуля «Загрузчик DL», необходимо на панели подкатегории нажать кнопку «Выключить». Система защиты выключит «Загрузчик DL» и попросит перезагрузить ПК. Записи о созданных в системе PIN-кодах (см. «Создание PIN-кода пользователя») удалятся.

Выключение модуля возможно при условии отсутствия преобразованных областей жесткого диска (см. «Прозрачное преобразование дисков»).

4.5.2 Создание PIN-кода пользователя

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

На вкладке «Параметры безопасности» в категории «Загрузчик DL» в списке основного окна присутствуют записи о созданных PIN-кодах для авторизации в модуле «Загрузчик DL» (рис. 85).

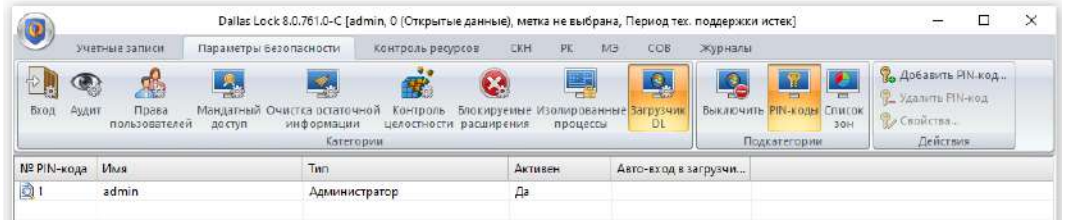


Рис. 85. Вкладка PIN-коды

Чтобы создать новый PIN-код пользователя, необходимо нажать на панели действий кнопку «Добавить PIN». Откроется окно создания PIN-кода (рис. 86).

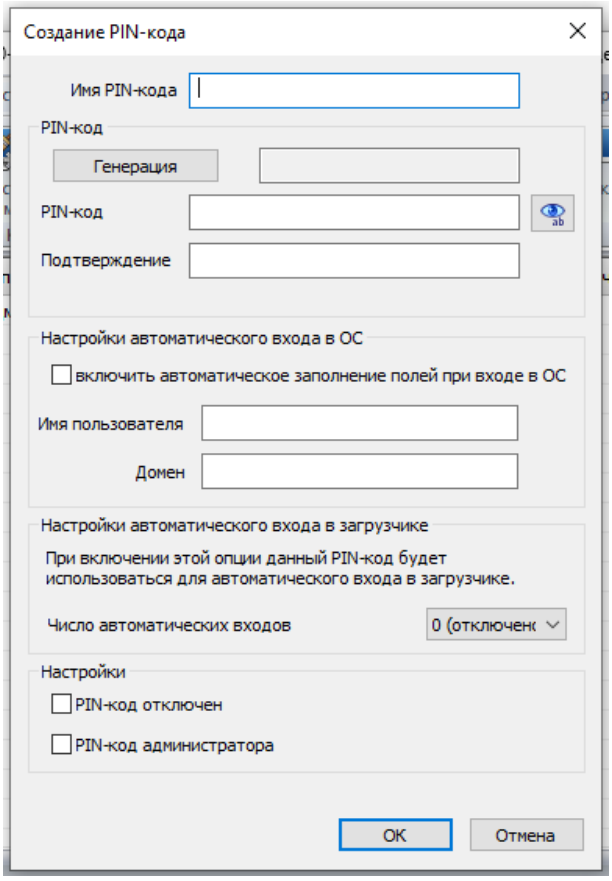


Рис. 86. Окно создания PIN-кода для загрузчика

Окно создания PIN-кода содержит следующие заполняемые поля:

Наименование	Описание
Имя PIN-кода	Произвольное название для идентификации в списке
PIN-код	Значение PIN-кода, которое должно соответствовать установленным в СЗИ парольным политикам. Для изменения PIN-кода необходимо отметить поле «Смена PIN-кода»
Подтверждение	Значение PIN-кода должно совпадать с введенным ранее в поле «PIN-код»
Настройка автоматического входа в ОС	При включении и заполнении параметров этого блока для пользователя, при вводе данного PIN-кода поля для авторизации в Windows («Имя пользователя» и «Домен») будут автоматически заполнены указанными в блоке
Настройка автоматического входа в загрузчике	Данное Включение путем выбора числа входов позволит осуществлять вход в ОС, минуя заполнение поля ввода PIN-кода, т.е. автоматически через загрузчик, но с теми параметрами, которые указаны для данного PIN-кода
PIN-код отключен	Отмеченное флагом поле позволит вместо удаления временно отключить выбранный PIN-код
PIN-код администратора	Отмеченное флагом поле установит статус, с которым для данного PIN-кода станет доступна функция аварийного преобразования в загрузчике

Наименование	Описание
	(см. «Обратное преобразование жесткого диска в аварийном режиме»).

Примечание. Созданные PIN-коды не привязаны ни к одной учетной записи и могут являться средством авторизации в загрузчике для любого пользователя.

Также с помощью кнопки «Генерация» создается случайный PIN-код для пользователя.

Редактирование параметров PIN-кода доступно после двойного клика по имени необходимого PIN-кода в списке. При редактировании откроется окно свойств PIN-кода (рис. 87). В данном окне станет доступным замена старого PIN-кода на новый.

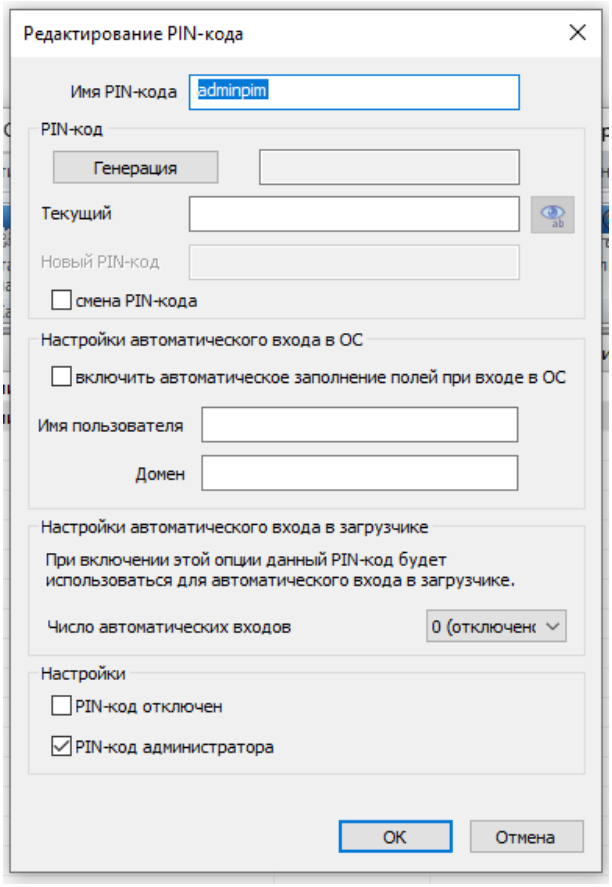


Рис. 87. Окно редактирования PIN-кода

Окно свойств PIN-кода содержит следующие заполняемые поля:

Наименование	Описание
Имя PIN-кода	Произвольное название для идентификации в списке
Текущий PIN-код	Поле доступно при редактировании уже созданного PIN-кода
Новый PIN-код	Значение PIN-кода, которое должно соответствовать установленным в СЗИ парольным политикам. Для изменения PIN-кода необходимо отметить поле «Смена PIN-кода»
Настройка автоматического входа в ОС	При включении и заполнении параметров этого блока для пользователя, при вводе данного PIN-кода, поля для авторизации в Windows («Имя пользователя» и «Домен») будут автоматически заполнены указанными в блоке
Настройка автоматического входа в загрузчике	Данное Включение путем выбора числа входов позволит осуществлять вход в ОС, минуя заполнение

Наименование	Описание
	поля ввода PIN-кода, т.е. автоматически через загрузчик, но с теми параметрами, которые указаны для данного PIN-кода
PIN-код отключен	Отмеченное флагом поле позволит вместо удаления временно отключить выбранный PIN-код
PIN-код администратора	Отмеченное флагом поле установит статус, с которым для данного PIN-кода станет доступна функция аварийного преобразования в загрузчике (см. «Обратное преобразование жесткого диска в аварийном режиме»).

Примечание. Следует учесть, что комбинация символов для каждого PIN-кода должна быть уникальной.

4.5.3 Вход на компьютер при активном загрузчике

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

Вход на ЗАРМ при активном модуле загрузчика происходит с предварительной авторизацией в загрузчике (рис. 88).

Рис. 88. Вход в модуле «Загрузчик DL»

Авторизация в загрузчике происходит без использования устройства «мышь». Для авторизации в загрузчике доступны только клавиши букв и цифр основной, цифр дополнительной клавиатуры, клавиши «Esc», «Backspace», «Enter», «F1», «F2». Переключение раскладки клавиатуры происходит нажатием комбинации клавиш «Ctrl»+«Shift».

Для осуществления входа в загрузчике необходимо ввести PIN-код. Дополнительное нажатие клавиши «F1» отобразит скрытые под значками звездочек символы в явном виде. Действие в поле для клавиши «F2» обязательно должно быть указано как «Загрузка» (данное действие стоит по умолчанию).

После ввода PIN-кода в загрузчике необходимо нажать «Enter». После этого начнется стандартная загрузка ОС.

Далее вход на ПК будет осуществляться под индивидуальной учетной записью пользователя (см. «Вход на защищенный компьютер»).

Примечание. При активном загрузчике Dallas Lock 8.0-C в момент загрузки компьютера к нему не должны быть подключены загрузочные USB-накопители.

Внимание! Если модуль загрузчика DL включен, но при этом он не отработал корректно, например, если была произведена попытка загрузки с CD диска, позволяющего обойти MBR DL и загрузить ОС напрямую, то на экране появится сообщение системы: «Нарушена целостность данных загрузчика», и в журнале системы защиты появится запись аналогичная сообщению.

В этом случае, если для учетной записи, под которой заходит пользователь, включена блокировка при нарушении целостности (она включена по умолчанию), то учетная запись заблокируется, и дальнейший вход в ОС будет невозможен.

В любом случае загрузка ОС в обход загрузчика Dallas Lock 8.0 невозможна, если системный диск был преобразован (см. «Прозрачное преобразование дисков»).

Примечание. Следует учесть, что если используется USB-клавиатура, то для корректной работы данной клавиатуры в модуле загрузчика DL, необходимо включить в BIOS компьютера опцию USB Keyboard Support (значение «Enabled»), в зависимости от устройства данная опция идентична USB Device Legacy Support или USB Legacy Support. В противном случае использование USB-клавиатуры будет невозможно и следует подключить PS/2 клавиатуру.

4.5.4 Дополнительные условия работы модуля «Загрузчик DL»

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

Помимо стандартного BIOS загрузчик Dallas Lock 8.0-C поддерживается ПК с материнскими платами, поддерживающими UEFI–интерфейс и GPT–разметку жесткого диска.

Для некоторых материнских плат и их версий UEFI–интерфейса требуется отключить функцию Secure Boot (выбрать значение «disabled»), которая отключает проверку электронной подписи UEFI–загрузчика Dallas Lock.

В случае установки Dallas Lock 8.0-C на планшетный ПК с сенсорным экраном для ввода PIN-кода модуля загрузчика DL имеется возможность отображения виртуальной клавиатуры.

Виртуальная клавиатура поддерживает ввод латинских и кириллических символов в верхнем и нижнем регистрах, а также ввод цифр и специальных символов.

Все прочие элементы управления интерфейса загрузчика: переключение в режим аварийного восстановления, отображение/скрытие PIN-кода, кнопки авторизации по PIN-коду и скрытия\отображения виртуальной клавиатуры, — также реализованы в виде сенсорных элементов управления.

Условием поддержки сенсорного ввода в загрузчике на планшетных ПК является возможность сенсорного ввода в BIOS (протокол EFI_ABSOLUTE_POINTER_PROTOCOL). Выяснить, имеется ли поддержка сенсорного ввода в BIOS, можно или уточнив данную информацию у производителя или продавца, или самостоятельно осуществив вход в BIOS и проверив возможность изменения настроек с помощью сенсорного ввода.

В случае непредвиденной активации загрузчика на планшетном компьютере, не поддерживающем сенсорный ввод в BIOS, можно обойти ввод PIN-кода в загрузчике, активировав функцию автоматического входа в загрузчике для определенного PIN-кода через оболочку администратора (см. «Создание PIN-кода пользователя»). Но следует учесть, что установленное ограничение количества срабатываний автоматического входа в загрузчике может полностью заблокировать вход на данный планшетный ПК.

Следует помнить, что не стоит включать преобразование диска (полное или частичное), не убедившись, что сам модуль загрузчика DL корректно загружает ПК по PIN-коду.

Примечание. Для корректного обновления ОС Windows 8 до Windows 8.1 (например, через встроенный в Windows магазин приложений Microsoft) необходимо, чтобы на жестком диске ПК не было преобразованных зон.

5 РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ФС

Одной из главных задач любой СЗИ является разграничение доступа. В СЗИ Dallas Lock 8.0 реализована настройка разграничения доступа к объектам ФС и к подключаемым устройствам. Система защиты Dallas Lock 8.0 позволяет гибко и удобно задавать пользователям права на доступ. После задания прав пользователи могут работать только с теми объектами, доступ к которым им разрешен, и совершать над ними только санкционированные операции.

Для разграничения доступа к объектам в Dallas Lock 8.0 предусмотрены два принципа:

- согласно индивидуальному списку доступа к объекту — дискреционный доступ;
- согласно уровню доступа и мандатной метке — мандатный доступ (только для Dallas Lock 8.0 редакции «С»).

Dallas Lock 8.0 позволяет разграничивать доступ ко всем объектам ФС: файлам, папкам, дискам, которые могут располагаться как на локальных дисках, так и на сменных и сетевых. Подробное описание разграничения доступа к объектам ФС приводится ниже.

Dallas Lock 8.0 позволяет разграничивать доступ к подключаемым устройствам (см. «Контроль устройств»).

5.1 Дескрипторы объектов

Дескриптор — это символический идентификатор назначенного для объекта ФС (или устройства) правила доступа.

Глобальные параметры доступа к объектам ФС называют **«глобальными дескрипторами»**, тогда как совокупность всех параметров безопасности (дискреционный и мандатный доступ, аудит, контроль целостности), назначенных на какой-либо объект ФС, называют **дескриптором** этого объекта.

Соответственно, операция назначения каких-либо параметров безопасности на объект ФС (или устройства) называется «**создать дескриптор**», «**назначить дескриптор**» или даже «**повесить дескриптор**».

Дескрипторы объектов в свою очередь делятся на:

- дескрипторы дискреционного доступа — это дескрипторы, содержащие только параметры дискреционного доступа;
- дескрипторы мандатного доступа — это дескрипторы, содержащие только параметры мандатного доступа;
- дескрипторы аудита — это дескрипторы, содержащие только параметры аудита;
- дескрипторы контроля целостности — это дескрипторы, содержащие только параметры контроля целостности.

Также дескрипторы делятся на **локальные дескрипторы** (назначенные локальным объектам ФС или конкретным устройствам), **сетевые дескрипторы** (назначенные объектам ФС, расположенным в сети), **сменные дескрипторы** (назначенные объектам, расположенным на сменных накопителях). Дескрипторы бывают **дескрипторами файлов** (назначенные на файл), **дескрипторами папок** (назначенные на папку), **дескрипторами устройства**, например, **дисков** (назначенные на диск).

В контексте данного руководства под понятием «дескриптор» будет пониматься окно с параметрами доступа выбранного объекта (рис. 89).

Окно дескриптора состоит из закладок: «Общие», «Дискреционный доступ», «Мандатный доступ» (только для Dallas Lock 8.0 редакции «С»), «Аудит», «Контроль целостности». В зависимости от объекта тот или иной дескриптор доступа может отсутствовать, как и соответствующая ему закладка.

Окно дескриптора можно вызвать через контекстное меню объекта (пункт меню «DL80: Права доступа») или через оболочку администратора при назначении прав доступа на объект.

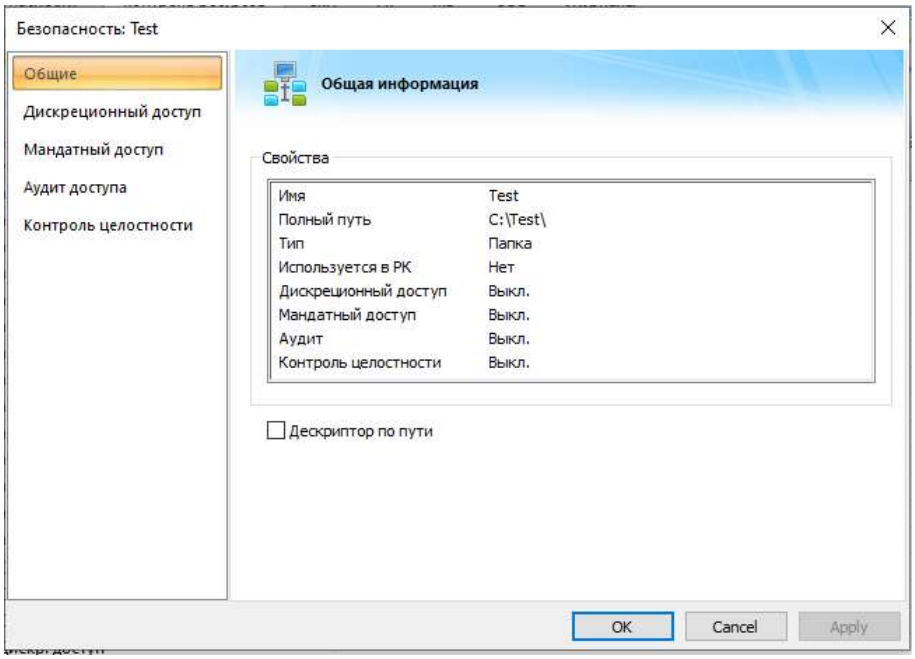


Рис. 89. Дескриптор объекта ФС

Для одновременно выделенных нескольких объектов в открывшемся окне дескриптора будут просматриваться установленные параметры безопасности всех объектов: причем, на закладке «Общие» параметры будут перечислены списком, на других закладках будет иметь место различное состояние (вид) отмеченных параметров:

- — отмеченное флагом поле означает, что данное свойство включено для всех выделенных объектов;
- — затемненное поле означает неопределенность: свойство включено для одних и выключено для других объектов;
- — пустое поле означает, что свойство выключено для всех выделенных объектов.

5.2 Дискреционный доступ

По умолчанию в системе защиты все пользователи имеют доступ ко всем объектам. Механизм дискреционного доступа основывается на предоставлении пользователю прав на определенные операции с объектами ФС. Этот способ разграничения доступа похож на тот, который реализован в Windows на NTFS.

5.2.1 Права доступа

Применительно к правам доступа, всех пользователей, зарегистрированных в системе защиты, можно разделить на 4 вида:

1. **Учетные записи**. Это индивидуальные учетные записи пользователей, для которых установлены индивидуальные (отличные от других пользователей и групп пользователей) права доступа, а также учетные записи, зарегистрированные по маске для доменных пользователей.
2. **Группы пользователей**. Всем пользователям, входящим в одну группу, автоматически назначаются права на доступ, установленные для группы.
3. **Все.** К этому виду относятся все пользователи, для которых не установлены индивидуальные права доступа и которые вместе с тем не входят ни в одну из групп. Такие пользователи автоматически объединяются в группу «Все». Этой группе, как и любой другой, могут быть разрешены/запрещены любые операции с любыми объектами ФС.
4. **Системные пользователи.** Данные пользователи не включены в вид пользователей «Все». Неосторожные блокировки для системных пользователей могут привести к неправоспособности системы.

В СЗИ Dallas Lock 8.0 каждому объекту ФС может быть сопоставлен список, элементами которого могут являться индивидуальные пользователи, учетные записи «по маске», группы пользователей и разряд «Все».

Каждый объект системы защиты характеризуется набором параметров безопасности. Каждый параметр безопасности контролирует определенную операцию (удаление, выполнение, изменение

и другие), которая может быть произведена с объектом. Любая операция с объектом может быть разрешена либо запрещена пользователю. Соответственно каждый параметр может иметь значение «разрешить» или «запретить» (флаги в соответствующих полях).

Права доступа можно задавать либо для индивидуальной учетной записи пользователя, либо для группы, либо для учетной записи пользователя «по маске».

Операции, которые можно производить с объектом в системе защиты, зависят от типа объекта.

- **Локальные диски и сменные накопители:**
  a. **Обзор папки. Чтение содержимого.** Позволяет увидеть все вложенные в данную папку каталоги, подкаталоги, файлы, содержащиеся в корневом каталоге объекта.
  b. **Изменение содержимого.** Изменение находящихся в папке вложенных папок и файлов (запись, удаление, создание).
  c. **Удаление вложенных объектов.**
  d. **Выполнение вложенных объектов.** Выполнение находящихся в папке соответствующих файлов.
  e. **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  f. **Запись разрешений.** Просмотр и редактирование параметров безопасности, установленных для ресурса.
  g. **Низкоуровневое чтение.** Просмотр содержимого диска при использовании прямого доступа к диску.
  h. **Низкоуровневая запись.** Удаление файлов с диска, а также запись на диск модифицированного (измененного) файла, используя прямой доступ к диску.
- **Удаленные диски, каталоги и подкаталоги (папки и подпапки):**
  a. **Обзор папки. Чтение содержимого.** Позволяет увидеть все вложенные в данную папку каталоги, подкаталоги, файлы, содержащиеся в корневом каталоге объекта.
  b. **Изменение содержимого.** Изменение находящихся в папке вложенных папок и файлов (запись, удаление, создание).
  c. **Удаление вложенных объектов.**
  d. **Выполнение вложенных объектов.** Выполнение находящихся в папке соответствующих файлов.
- **Файлы (могут находиться на локальных дисках, на сменных носителях, на сетевых ресурсах):**
  a. **Чтение.** Просмотр содержимого файла любого типа.
  b. **Запись.** Удаление файлов, а также запись на диск модифицированного (измененного) файла.
  c. **Удаление.**
  d. **Выполнение**. Имеет смысл только для программ.
- **Дополнительные параметры для файлов и папок:**
  a. **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  b. **Изменение разрешений**. Просмотр и редактирование параметров безопасности, установленных для ресурса.
- **Ветки реестра:**
  a. **Чтение.** Возможность прочитать содержимое.
  b. **Запись.** Создание и удаление параметров в ветке реестра и ее самой.
  c. **Удаление.**
  d. **Чтение разрешений.** Просмотр значения параметров безопасности, установленных для ресурса.
  e. **Запись разрешений.** Просмотр и редактирование параметров безопасности, установленных для ресурса.

Примечание. Операции «Чтение разрешений» и «Изменение разрешений» доступны текущему пользователю, только если он обладает соответствующими полномочиями на просмотр параметров ресурсов и управление дискреционным доступом соответственно (см. «Полномочия пользователей на администрирование системы защиты»).

Если объект является вложенным, и ему не сопоставлен список пользователей с правами, то права доступа пользователя к данному объекту определяются параметрами корневого объекта.

Если пользователь находится в сопоставленном объекту списке и одновременно входит в состав группы пользователей, находящейся в сопоставленном объекту списке, то действуют параметры доступа, установленные для этого пользователя.

Если пользователь входит в состав нескольких групп, находящихся в сопоставленном объекту

списке, и если для одной из этих групп установлен запрет на совершение данной операции, а также отсутствует индивидуальное сопоставление данного пользователя объекту (нет явно назначенных прав), то пользователю эта операция запрещена.

Если пользователь не находится в сопоставленном объекту списке и не входит ни в одну из сопоставленных объекту (или корневому объекту) групп пользователей, то для него действуют параметры, установленные для группы «Все».

Примечание. Если для какого-то объекта назначить параметры безопасности (права доступа, аудит или контроль целостности) и этот ресурс переименовать, то параметры безопасности сохранятся (за исключением случая назначения дескрипторов для пути, см. «Дескрипторы по пути»).

Примечание. Если сделать копию объекта ФС, на который назначены параметры безопасности, то копия не будет иметь таких же параметров безопасности.

Примечание. В Dallas Lock 8.0 реализован собственный механизм дискреционного доступа, независимый от NTFS. Благодаря этому права доступа Dallas Lock 8.0 могут быть назначены не только на диски, отформатированные под NTFS, но и на диски с другими файловыми системами, сменные накопители, сетевые ресурсы. Более того, механизм дискреционного доступа Dallas Lock 8.0 намного удобнее в настройке и понятнее, чем встроенный в ОС механизм NTFS.

Но нужно помнить, что Dallas Lock 8.0 не заменяет встроенный механизм NTFS, а дублирует его. То есть одновременно работают оба механизма, и чтобы пользователь получил доступ к объекту, Dallas Lock 8.0 и NTFS должны разрешить доступ. Если же хоть один из этих механизмов откажет в доступе, пользователь не сможет работать с объектом ФС. Об этой особенности важно помнить. Если возникнет ситуация, при которой в Dallas Lock 8.0 доступ к объекту разрешен, но фактически доступа нет, то первым делом следует проверить, какие права NTFS установлены на этот объект.

Также эту ситуацию легко отследить, если на объект назначить аудит отказов доступа. В случае если доступ будет блокироваться NTFS при включенном параметре «Аудит: заносить в журнал ошибки ОС», в журнале напротив записи будет отображен особый значок (с буквой «w»), а если доступ блокируется установленной системой защиты — то стандартный значок отказа. Рекомендуется при использовании Dallas Lock 8.0 разграничивать доступ к ФС только средствами Dallas Lock 8.0, а механизм разграничения доступа NTFS не использовать.

5.2.2 Механизм определения прав доступа пользователя к ресурсам ФС

При попытке пользователя совершить с объектом ФС компьютера любую операцию система защиты Dallas Lock 8.0 анализирует назначенные права доступа согласно иерархии назначенных параметров на объекты снизу-вверх, то есть проверка происходит, начиная с локальных параметров объекта; глобальные параметры проверяются в последнюю очередь. При этом локальные настройки имеют приоритет над глобальными настройками.

Причем при проверке прав дискреционного доступа назначенные права прибавляются. Это означает, что происходит проверка значения (наличие флагов «запретить»/«разрешить») для каждого наименования прав (обзор, выполнение, чтение, запись и пр.), и, если право не имеет состояния «запретить»/«разрешить» на нижнем уровне, то система проводит проверку и присваивает значение состоянию, исходя из более высокого уровня параметров, к которому относится данный объект.

Если право имеет различные состояния «запретить»/«разрешить» на разных уровнях, например, «запретить» для файла и «разрешить» для более глобального уровня, папки, в которую вложен файл, то приоритетным будет право локального уровня «запретить».

Приоритеты параметров в Dallas Lock 8.0 представляют собой следующую иерархию:

Таблица 2. Приоритеты параметров дескрипторов

Тип параметров	Название параметра	Приоритет
Локальные параметры	Параметры файлов	**Самый высокий**
	Параметры конкретных экземпляров накопителей	

	Параметры отдельных веток реестра	
	Параметры папок (приоритет меняется в зависимости от иерархии папок)	**Высокий**
Глобальные параметры (список глобальных параметров на вкладке «Контроль ресурсов» → «Глобальные»)	«Параметры CD-ROM дисков по умолчанию» «Параметры открытых USB-Flash накопителей по умолчанию» «Параметры открытых FDD-дисков по умолчанию» «Параметры преобразованных USB-Flash накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН) «Параметры преобразованных FDD-дисков по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)	**Средний**
	«Параметры открытых сменных накопителей по умолчанию» «Параметры преобразованных сменных накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН) «Параметры фиксированных дисков по умолчанию» «Параметры сети по умолчанию» «Параметры реестра по умолчанию»	**Низкий**
	«Параметры ФС по умолчанию»	**Самый низкий**

Отдельными категориями в списке параметров выделены преобразованные (только для Dallas Lock 8.0 с модулем СКН) и открытые сменные накопители (FDD-диски, USB-Flash накопители). Данное разграничение имеет смысл, если в Dallas Lock 8.0 настраивается доступ к преобразованным сменным накопителям (см. «Преобразование сменных накопителей»). В случае, когда нет преобразованных накопителей, все сменные накопители считаются открытыми и права должны назначаться именно для таких параметров.

В системе защиты реализован механизм назначения дискреционных прав как на глобальные параметры (раздел «Дискреционный доступ для глобальных параметров»), так и на локальные объекты ФС (раздел «Дискреционный доступ для локальных объектов ФС и веток реестра»).

Таким образом, система защиты последовательно выполняет следующие действия проверки:

1. Если для данного объекта ФС пользователю назначены права, то возможность совершения запрошенной операции устанавливается исходя из этих прав. Если параметру, контролирующему данную операцию, присвоено значение «Разрешить», то операция выполняется. Если параметру присвоено значение «Запретить», операция блокируется.
2. Если для данного объекта ФС не назначены права для данного пользователя, но права назначены для одной из групп, в которую входит пользователь, то для определения возможности совершения запрашиваемой операции аналогично используются права этой группы.
3. Если для данного объекта ФС не назначены права ни конкретно для данного пользователя, ни для какой-либо из групп, в которые входит этот пользователь, то для определения возможности совершения запрошенной операции используются права, назначенные группе «Все».
4. Если же права не назначены ни для пользователя, ни для какой-либо группы, куда этот пользователь входит, ни для группы «Все», то система защиты проверяет, входит ли данный объект в состав другого объекта (папка/диск). Если входит, то повторяются действия 1-3 для объекта, содержащего данный объект. Если объект не входит в состав другого объекта ФС, то система защиты переходит к проверке глобальных параметров по иерархии, представленной в таблице.
5. Анализ глобальных параметров осуществляется по той же самой схеме, что и локальных. Проверяются права, назначенные для пользователя. Если они не назначены, то для групп, куда этот пользователь входит, и если права не назначены для таких групп, то проверяются права группы «Все». Если же и для группы «Все» не назначены права, то аналогично проверяются права глобальных параметров, имеющих более низкий приоритет. Если осуществлялась

проверка глобальных параметров самого низкого приоритета, то выполнение операции разрешается.

Пример

Пусть существует файл, расположенный по пути «C:\Docs\balans.txt». Также есть следующие пользователи, каждый из которых входит только в одну группу:

- «Оператор», в группе «Пользователи»;
- «Аудитор», в группе «Пользователи»;
- «Админ», в группе «Администраторы».

На файл «C:\Docs\balans.txt» назначены права:

- группа «Все» — доступ запрещен;
- группа «Пользователи» — разрешено чтение;
- пользователь «Оператор» — разрешен полный доступ.

В результате распределения системой прав на данный объект, пользователи будут иметь следующие возможности для совершения операций с объектом:

- пользователь «Оператор» будет иметь полный доступ к файлу «C:\Docs\balans.txt» (права для пользователя будут проверяться первыми, и они имеют более высокий приоритет, чем права, заданные для групп);
- пользователь «Аудитор» будет иметь доступ только на чтение (для него не назначено отдельных прав, но он входит в группу «Пользователи»);
- пользователь «Админ» не получит доступа к этому файлу (для него не назначено отдельных прав, он не входит в группу «Пользователи», поэтому для него будут использоваться права, назначенные для группы «Все»).

5.2.3 Дискреционный доступ для глобальных параметров

Список глобальных параметров ФС расположен на вкладке «Контроль ресурсов» → «Глобальные» оболочки администратора Dallas Lock 8.0 (рис. 90).

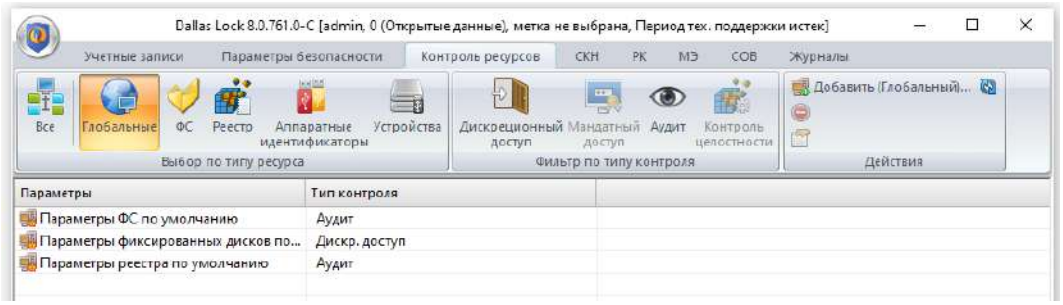


Рис. 90. Назначение глобальных параметров безопасности

Глобально права дискреционного доступа можно назначить:

Таблица 3. Глобальные дескрипторы

Назначение	Название параметра в Dallas Lock 8.0
на все ресурсы ФС	«Параметры ФС по умолчанию»
на жесткие диски, в том числе на устройства типа внешний жесткий диск USB	«Параметры фиксированных дисков по умолчанию»
на все сетевые ресурсы	«Параметры сети по умолчанию»
на файл-диски, которые были преобразованы	«Параметры преобразованных файл-дисков по умолчанию»
на все типы сменных накопителей, которые не были преобразованы, кроме CD-ROM дисков (по умолчанию)	«Параметры открытых сменных дисков по умолчанию»
на все приводы компакт-дисков на данном компьютере	«Параметры CD-ROM дисков по умолчанию»
на все сменные USB-Flash накопители, которые не были преобразованы (по умолчанию)	«Параметры открытых USB-Flash накопителей по умолчанию»
на все Floppy-диски на данном компьютере, которые не были преобразованы (по умолчанию)	«Параметры открытых FDD-дисков по умолчанию»

Назначение	Название параметра в Dallas Lock 8.0
на все типы сменных накопителей, которые были преобразованы	«Параметры преобразованных сменных накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все сменные USB-Flash накопители, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных USB-Flash накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все Floppy-диски на данном компьютере, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных FDD-дисков по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
для всего реестра	«Параметры реестра по умолчанию»
на все типы аппаратных ключей	«Параметры аппаратных ключей по умолчанию»

Чтобы установить дискреционный доступ, необходимо выделить параметр и нажать кнопку «Свойства» на панели действий. Откроется окно редактирования параметров безопасности — дескриптор объекта, в котором необходимо выбрать закладку «Дискреционный доступ» (рис. 91).

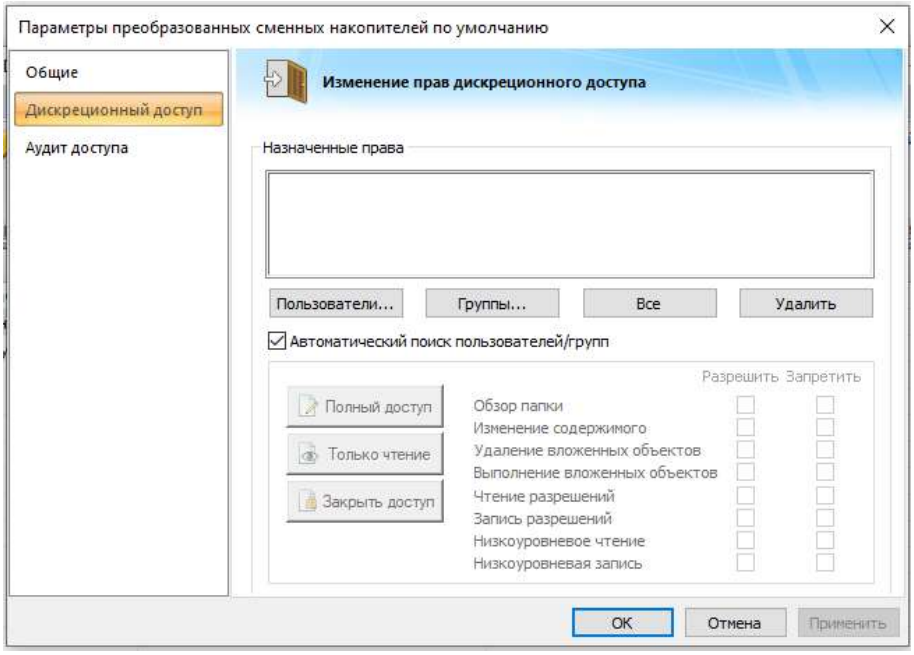


Рис. 91. Назначение прав дискреционного доступа

Чтобы назначить определенные дискреционные права для пользователей, необходимо:

1. Выбрать определенные учетные записи пользователей или групп. После нажатия кнопок «Пользователи» или «Группы» появятся типовые диалоговые окна с возможностью поиска учетных записей. Для выбора доменных учетных записей в поле «Размещение» необходимо выбрать имя домена, после чего появится список всех доменных учетных записей, зарегистрированные в Dallas Lock 8.0 будут выделены особенным образом.
2. Для каждой учетной записи, пользователя или группы в списке необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту ФС (рис. 92).

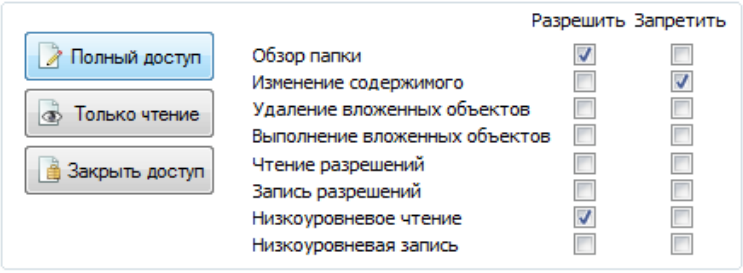


Рис. 92. Список прав дискреционного доступа

3. Далее нажать «Применить» и «ОК».

Примечание. Если в процессе назначения запрета на чтение на CD-ROM диски выполняется подключение CD-ROM диска, то данные права в зависимости от скорости монтирования диска могут не отработать. Соответственно, назначение прав на CD-ROM диски и эксплуатирование СЗИ в части контроля за данными типами носителей следует разносить во времени хотя бы несколько десятков секунд.

5.2.4 Дискреционный доступ для локальных объектов ФС и веток реестра

Для того, чтобы назначить дискреционный доступ для конкретного объекта ФС или ветки реестра, необходимо:

1. Открыть его дескриптор безопасности, используя оболочку администратора Dallas Lock 8.0 или контекстное меню объекта (для объектов ФС).
   - Открыть дескриптор с помощью контекстного меню значка объекта ФС можно, выбрав пункт меню «DL8.0: Права доступа» (рис. 93).

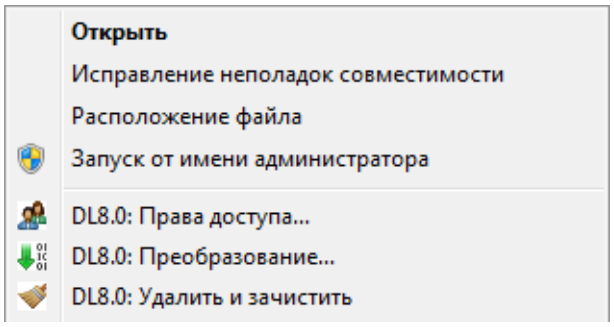


Рис. 93. Контекстное меню

   - Открыть дескриптор безопасности объекта ФС или ветки реестра через оболочку администратора Dallas Lock 8.0. Для фильтра «Дискреционный доступ» на вкладке «Контроль ресурсов» в меню действий выбрать «Добавить (Глобальный)», «Добавить (ФС)» или «Добавить (Реестр)» в зависимости от типа ресурса (рис. 94).

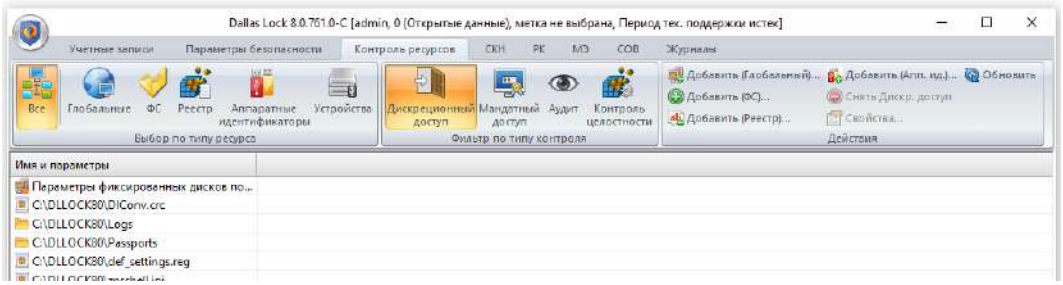


Рис. 94. Окно дискреционного доступа

В появившемся окне проводника (как в проводнике Windows) необходимо найти нужный ресурс, объект ФС или выбрать ветку реестра и нажать кнопку «Выбрать» или «Принять» (Рис. 95,рис. 96, Рис. 97). Для выбранного объекта откроется окно дескриптора.

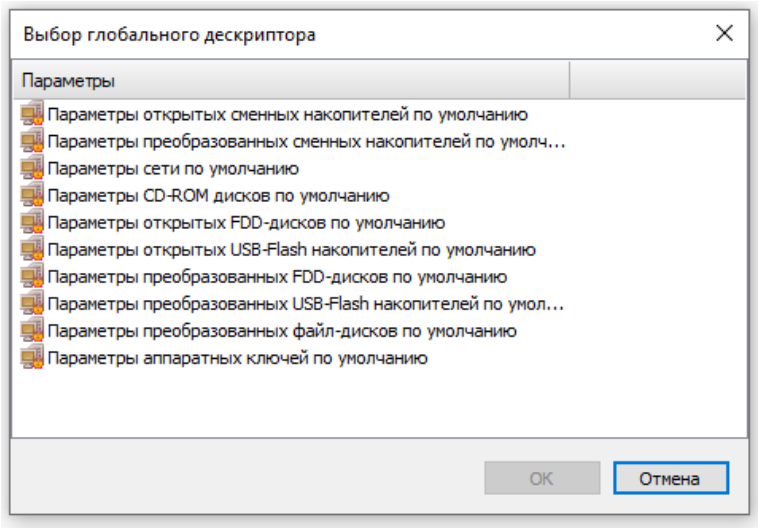


Рис. 95. Окно выбора глобального дескриптора

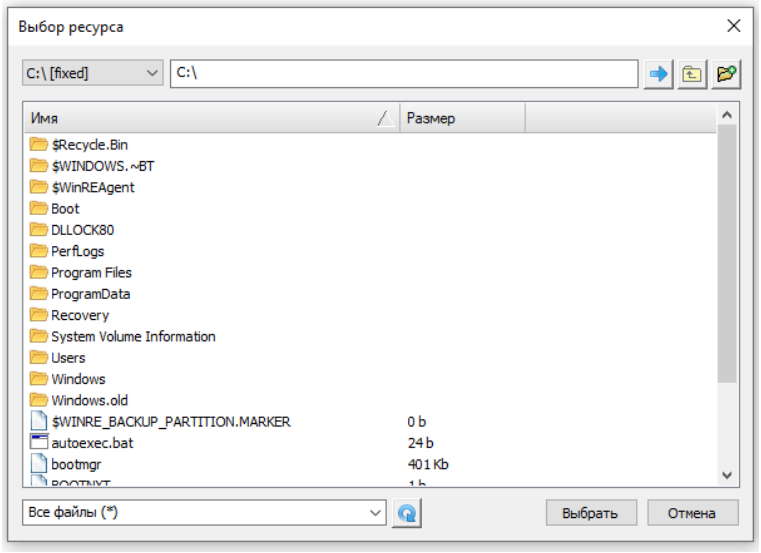


Рис. 96. Окно выбора объекта ФС

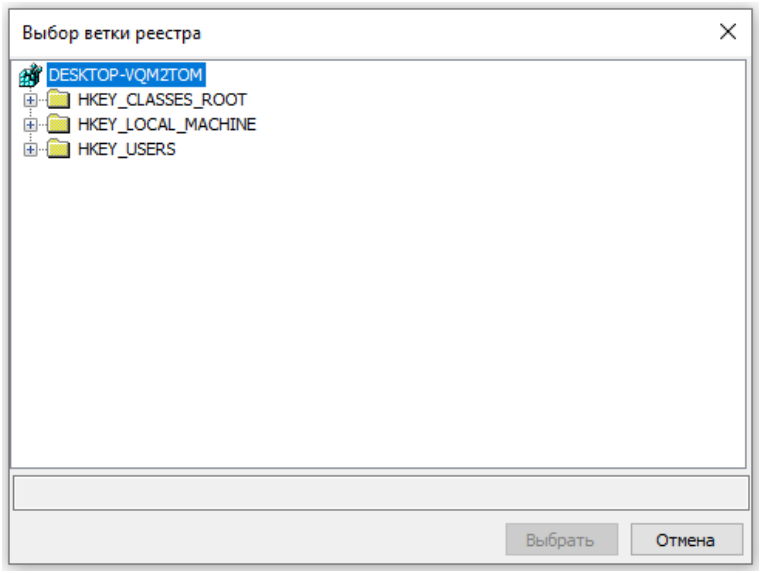


Рис. 97. Окно выбора ветки реестра

2. В окне дескриптора безопасности необходимо выбрать закладку «Дискреционный доступ» (рис. 98).

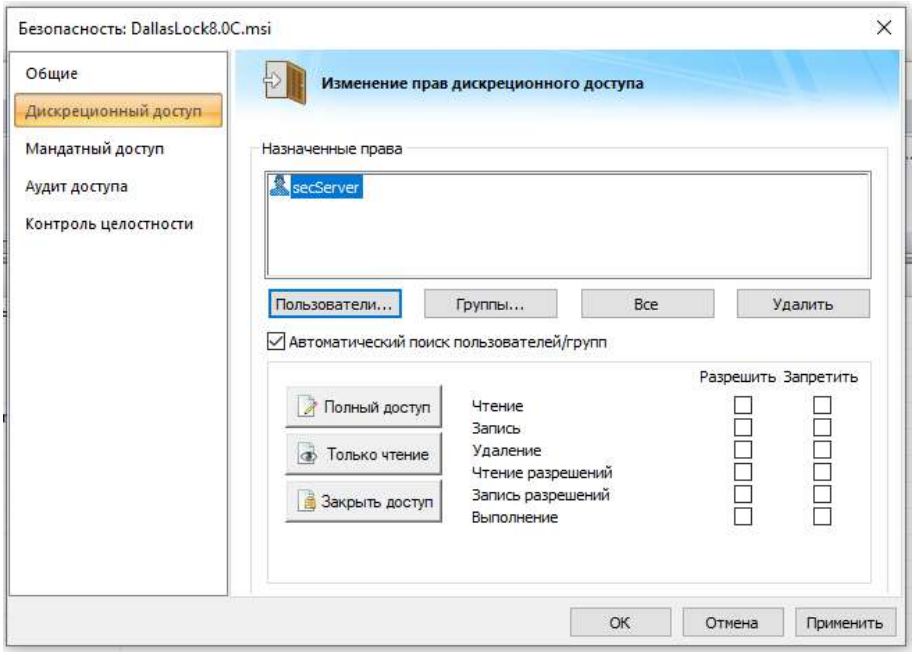


Рис. 98. Назначение прав дискреционного доступа

В соответствии с дискреционным принципом доступа каждому ресурсу ФС может быть сопоставлен список пользователей и/или групп пользователей. Каждому пользователю (группе) из списка можно разрешить или запретить определенную операцию с данным ресурсом.

3. Чтобы назначить определенные дискреционные права для определенных пользователей, необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп.
4. Для выбранных пользователей/групп необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту (рис. 99).

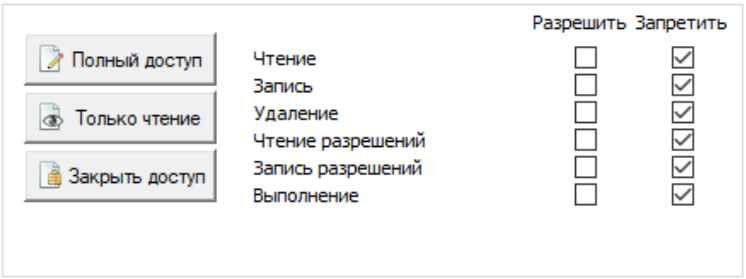


Рис. 99. Список прав дискреционного доступа

Объекты, на которые назначен дискреционный доступ, автоматически появятся в списке объектов в окне категории «Дискреционный доступ» на вкладке «Контроль ресурсов».

При выборе категории «Все» на вкладке «Контроль ресурсов» также появится список, содержащий параметры всех объектов глобальных, локальных или сетевых на которые назначены какие-либо права доступа, а также контроль целостности и аудит.

Внимание! Введено ограничение в части назначения контроля целостности на защищаемые объекты размером свыше 5 Гб, поскольку это может повлиять на производительность работы СЗИ Dallas Lock 8.0 и привести к сбою в штатной работе СЗИ

Права доступа к сетевым ресурсам

Подобно тому, как можно назначать права доступа на локальные ресурсы компьютера, в системе Dallas Lock 8.0 права доступа можно назначать и на сетевые ресурсы.

В этом качестве модель безопасности Dallas Lock 8.0 отличается от модели безопасности, принятой в Windows.

Локально установленная ОС Windows контролирует только локальные ресурсы. Система защиты Dallas Lock 8.0 позволяет ограничивать доступ также и к сетевым ресурсам. Причем, если на удаленном компьютере, на который идет запрос, тоже установлена система защиты Dallas Lock 8.0,

то права доступа будут проверяться два раза. Первый раз — локально установленной системой защиты Dallas Lock 8.0 перед тем, как запрос отправится в сеть, и второй раз — удаленно установленной Dallas Lock 8.0, на которую придет запрос из сети.

Права доступа на сетевые ресурсы назначаются так же, как и на локальные:

- нужно найти объект через проводник Windows и воспользоваться контекстным меню;
- или через оболочку администратора — ввести в форме поиска объекта полный сетевой путь.

При назначении доступа к сетевым ресурсам необходимо помнить следующее: фильтр ФС Dallas Lock 8.0, который отвечает за контроль доступа к ФС, получает путь к объекту в виде строки, которую он и анализирует. И если для локальных ресурсов в этом нет никаких проблем, то при работе с сетевыми ресурсами об этом нужно помнить, так как задать путь к одному и тому же сетевому ресурсу можно различными способами: используя имя компьютера, используя IP-адрес, используя IP-адрес в шестнадцатеричном виде и т. д.

Например, пусть имеется некоторый компьютер SERVER512 с IP-адресом 192.168.8.92, на котором расположена папка, открытая для общего доступа, с именем «sharedDocuments». Тогда пути «\\SERVER512\sharedDocuments\письмо.docx» и «\\192.168.8.92\sharedDocuments\письмо.docx» указывают на один и тот же документ.

Но с точки зрения Dallas Lock это разные пути, и поэтому, если назначены права на один из них, при обращении по другому пути права действовать не будут.

Поэтому, если необходимо разграничить доступ к сетевым ресурсам для какого-либо пользователя, то нужно, обязательно, в глобальном дескрипторе «Параметры сети по умолчанию» (вкладка «Контроль ресурсов» → категория «Глобальные») запретить этому пользователю все действия и разрешить их для конкретных ресурсов. Иначе ограничения можно будет легко обойти.

Примечание. Для удобства использования сетевых ресурсов реализована возможность сохранения авторизационных данных пользователя при первом подключении к сетевому ресурсу. Сохранение производится при включении чекбокса «Запомнить учетные данные».

5.2.5 Дискреционный доступ к аппаратным идентификаторам

В оболочке администрирования для управления дискреционным доступом к аппаратным идентификаторам пользователю должны быть назначены права «Параметры безопасности: Управление» и «Ресурсы: Управление дискреционным доступом», для аудита — «Параметры безопасности: Просмотр».

Для управления дискреционным доступом к аппаратным идентификаторам с помощью КСБ пользователю должна быть назначена роль, для которой установлены привилегии контроля ресурсов «действия с ресурсами» и «просмотр списков контролируемых ресурсов и их параметров» (см. «Ролевая модель учетных записей СБ»).

Для того, чтобы назначить дискреционный доступ для конкретного аппаратного идентификатора, необходимо:

1. В оболочке администратора перейти на вкладку «Контроль ресурсов» и выбрать тип ресурса «Все» или «Аппаратные идентификаторы». Выбрать фильтр по типу контроля «Дискреционный доступ» и нажать кнопку «Добавить (Апп. ид.)…» (рис. 100).

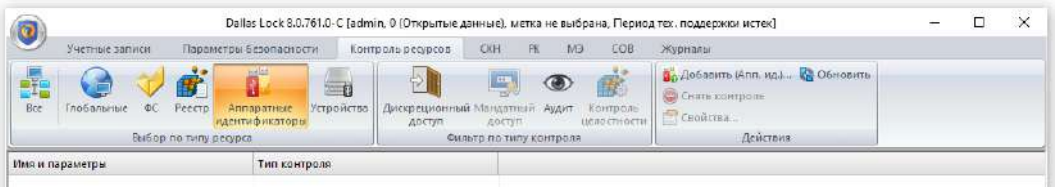


Рис. 100. Дискреционный доступ к аппаратным идентификаторам

В появившемся окне из выпадающего списка выбрать аппаратный идентификатор (рис. 101).

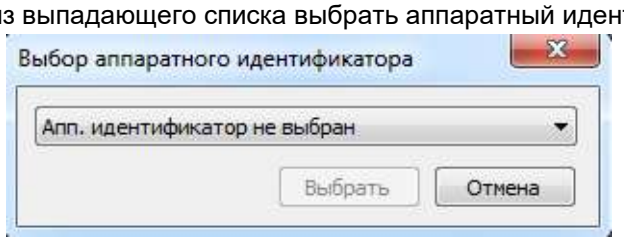


Рис. 101. Выбор аппаратного идентификатора

2. В окне дескриптора безопасности необходимо выбрать закладку «Дискреционный доступ» (рис. 102).

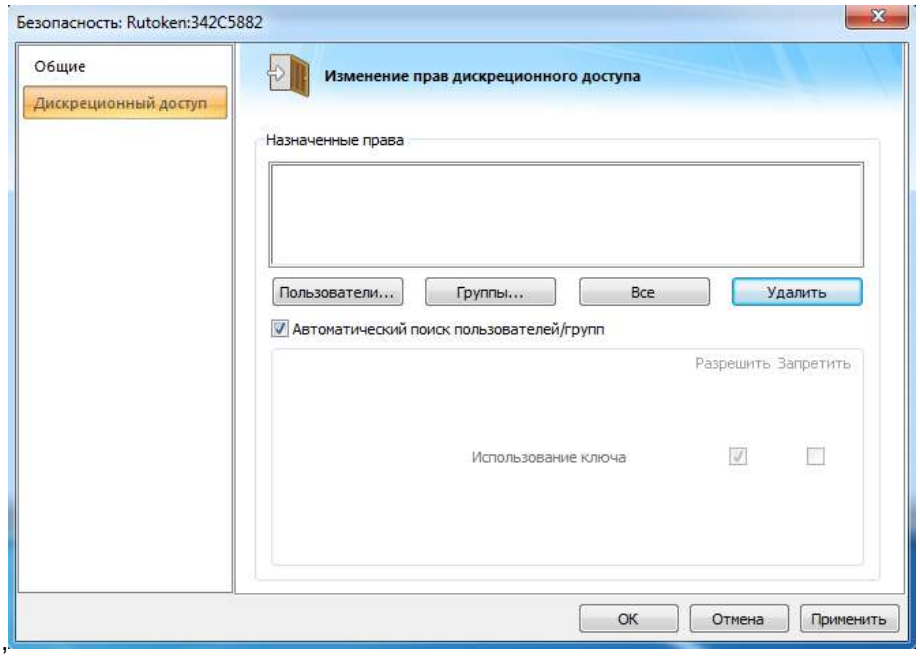


Рис. 102. Назначение прав дискреционного доступа

Каждому пользователю (группе) из списка можно разрешить или запретить использование данного ключа.

3. Чтобы назначить определенные дискреционные права для определенных пользователей, необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп.

4. Для выбранных пользователей/групп необходимо указать, разрешено или запрещено использование ключа.

Аппаратные идентификаторы, на которые назначен дискреционный доступ, автоматически появятся в списке ресурсов типа «Аппаратные идентификаторы», а также в категории «Все».

Примечание. При использовании аппаратных идентификаторов реализован следующий механизм разграничения доступа к ним:

- если аппаратный идентификатор был подключен во время работы пользователя, которому, согласно правилу управления данным аппаратным идентификатором или глобальному дескриптору, не назначен доступ к данному аппаратному идентификатору, происходит блокирование подключенного аппаратного идентификатора для всех пользователей;
- если аппаратный идентификатор был подключен до входа пользователя, которому, согласно правилу управления данным ключом или глобальному дескриптору, не назначен доступ к данному аппаратному идентификатору, происходит блокирование подключенного аппаратного идентификатора после входа пользователя в систему для всех пользователей.

Разблокировка аппаратных идентификаторов, заблокированных в описанных ситуациях, происходит автоматически при отключении аппаратного идентификатора, либо при выходе пользователя из системы.

Примечание. Не рекомендуется использовать одновременно больше одного аппаратного считывателя Jacarta/eToken, так как в большинстве случаев это излишне. Если потребовалось подключить несколько считывателей Jacarta/eToken, и при этом они одновременно считывают один и тот же аппаратный идентификатор, то подсистема СЗИ Dallas Lock 8.0 определит данный АИ как два разных идентификатора (уникальность идентификатора определяется парой: считыватель и ID аппаратного идентификатора), и прописывать права доступа нужно для каждого определившегося идентификатора.

Свойства дескриптора можно вызвать, нажав кнопку «Свойства» на панели действий, либо в контекстном меню дескриптора.

В КСБ редактирование параметров дескриптора доступно при выборе действия на том уровне, на котором дескриптор создавался, поэтому при выборе действия «Свойства» на уровне ниже или выше происходит открытие окна настройки дескриптора без возможности редактирования

параметров.

5.2.6 Низкоуровневый доступ к диску и сменным накопителям

Если пользователю не разрешен низкоуровневый доступ к диску и сменным накопителям, то он не сможет запускать программы, использующие прямой доступ к данным носителям информации на ЗАРМ. Тем самым обеспечивается предотвращение НСД к информации и к работе с данными носителями информации при помощи таких программ.

Под сменными накопителями подразумеваются те устройства, которые распознаются ОС как сменный/съемный (removable). Это USB-Flash накопители, карты памяти, Floppy- и компакт-диски и прочие.

Жесткие диски, подключаемые через устройство Mobile Rack или USB-порт, физически являются сменными, но логически, для ОС, являются фиксированными.

Для того, чтобы назначить дискреционные права на низкоуровневый доступ к диску или сменному накопителю, необходимо установить соответствующий набор разрешений/запретов для дескриптора или глобального параметра (рис. 103).

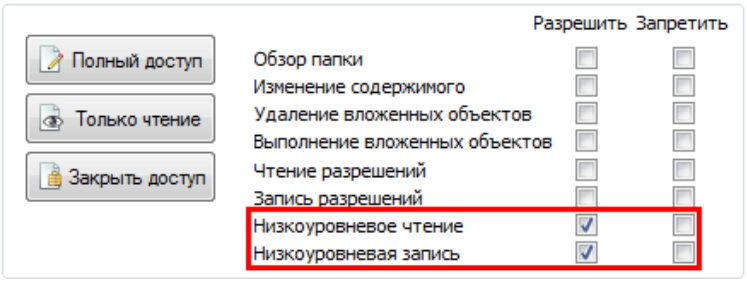


Рис. 103. Список прав дискреционного доступа

5.2.7 Дескрипторы по пути

Как отмечалось выше, если на объект ФС установлен дескриптор, то при переименовании этого объекта, дескриптор останется на нем. Если удалить объект, дескриптор удалится тоже. То есть дескриптор «привязан» к объекту.

Но в ряде случаев это бывает неудобно. Например, при работе с Microsoft Word. Программа MS Word устроена таким образом, что когда в ней открывается какой-либо документ, после редактирования и сохранения изменений, она выполняет последовательность следующих действий:

- переименовывает исходный документ,
- создает новый документ под первоначальным именем,
- удаляет переименованный исходный документ.

Что происходит с дескриптором, если он назначен на документ, при его редактировании? Он переименовывается и удаляется вместе с исходным документом. Система Dallas Lock 8.0 исправно работает в соответствии с заложенными в ней принципами. Но для пользователя это выглядит как ошибка: на документ были назначены права, пользователь его отредактировал, права исчезли. Возникает противоречивая ситуация.

Чтобы таких ситуаций не возникало, необходимо назначать права не на документы, а на папки, в которых эти документы находятся.

Но это бывает неудобно, например, когда в одной папке должны лежать несколько документов с разными правами. В этом случае на эти документы нужно назначать дескрипторы по пути. Их отличие от обычных дескрипторов в том, что они не переименовываются и не удаляются вместе с объектом. Они «привязаны» к конкретному пути и могут существовать даже, если по этому пути никаких документов не находится.

Для того, чтобы создать дескриптор по пути, нужно в окне редактирования параметров объекта на вкладке «Общие» установить флаг в поле «Дескриптор по пути» (рис. 104).

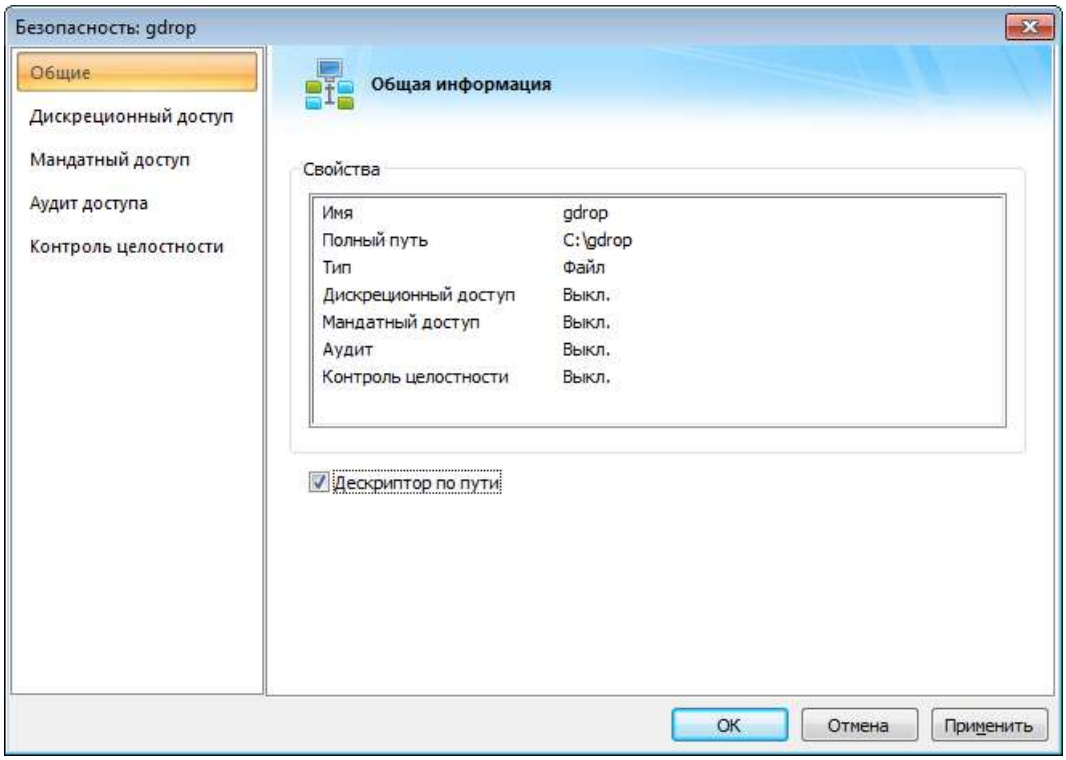


Рис. 104. Назначенный дескриптор по пути

Дескрипторы по пути выделены в списке контролируемых объектов голубым значком , обычные дескрипторы отмечены белым значком, глобальные — оранжевым, дескрипторы папок отмечены значком в виде папки, дескрипторы сетевых ресурсов и веток реестра также отличаются.

Без необходимости использовать дескрипторы по пути не рекомендуется.

5.3 Мандатный доступ

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Согласно мандатному принципу управления доступом, каждому объекту можно присвоить уровень доступа и мандатную метку. Для учетной записи пользователя также назначается уровень доступа и мандатная метка, которые определяют объекты, к которым может быть доступ. Мандатный принцип управления доступом делится на две категории:

1. Иерархическая категория — осуществляется сравнение уровней доступа объекта и пользователя. В Dallas Lock 8.0 уровни доступа имеют номера от 0 до 7. Чем больше номер, тем выше уровень доступа. Если не указан уровень доступа, то считается, что объект имеет уровень доступа 0 («Открытые данные»). Если уровень доступа присвоить родительскому объекту (папке, диску), то все объекты, находящиеся внутри, будут иметь тот же уровень доступа, за исключением тех случаев, когда им явно присвоен другой уровень доступа.

   Для удобства работы, уровням доступа можно присваивать имена. По умолчанию первым пяти уровням доступа (от 0 до 4) присвоены наименования:
   - 0 (Открытые данные);
   - 1 (Конфиденциальные данные);
   - 2 (Персональные данные);
   - 3 (Секретные данные);
   - 4 (Совершенно секретно).

   Согласно данному присвоению уровней доступа, пользователь, имеющий допуск уровня «Конфиденциальные данные», не может получить доступ к объекту с уровнем доступа «Секретные данные». В то же время, пользователь с допуском уровня «Секретные данные» имеет право доступа к объекту с уровнем «Конфиденциальные данные».
2. Неиерархическая категория — осуществляется сравнение мандатных меток объекта и пользователя. В случае совпадения мандатных меток объекта и пользователя пользователь получает доступ к объекту. В случае несовпадения мандатных меток объекта и пользователя доступ блокируется. Например, пользователь, имеющий мандатную метку «Метка 1», не может получить доступ к объектам с мандатными метками «Метка 2», «Метка 3» и т. д. Данный

пользователь может получить доступ только к объектам с мандатной меткой «Метка 1». По умолчанию в Dallas Lock 8.0 мандатные метки отсутствуют.

5.3.1 Переименование уровней доступа и мандатных меток

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

В Dallas Lock 8.0 используется 7 уровней доступа. Имена этих уровней доступа можно сменить на другие, на работу системы защиты это никак не повлияет. Для системы защиты имеет значение только номер.

Для того, чтобы переименовать уровень доступа, необходимо в оболочке администратора на вкладке основного меню «Параметры безопасности» выбрать категорию «Уровни доступа». Далее необходимо выделить уровень и с помощью кнопки или контекстного меню выбрать действие «Свойства» (рис. 105). В появившемся окне нужно ввести новое наименование и нажать «ОК».

Переименование мандатных меток производится аналогичным образом в категории «Мандатные метки».

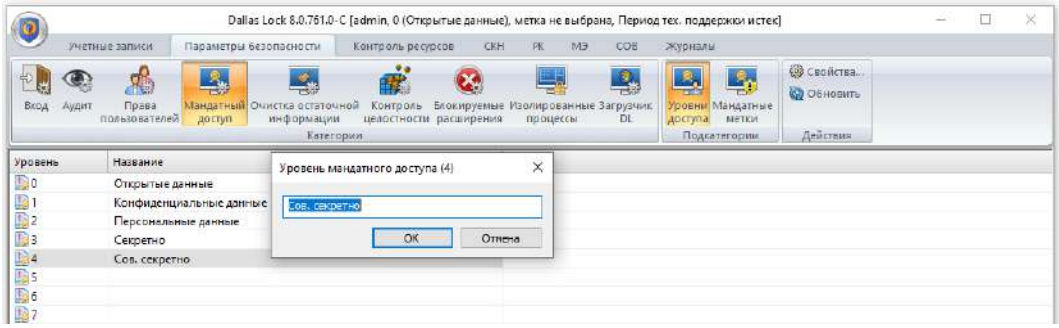


Рис. 105. Список уровней мандатного доступа

5.3.2 Уровни и метки доступа пользователей

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

При создании учетной записи для каждого пользователя устанавливается уровень доступа от 0 до 7 и мандатная метка:

- Пользователи, имеющие уровень доступа 0, имеют доступ только к объектам ФС, имеющим уровень доступа 0. Пользователи, имеющие уровень доступа 1, имеют доступ только к объектам ФС, имеющим уровень доступа 0 и 1. Имеющие уровень доступа 2 — только к объектам с уровнем доступа 0, 1, 2 и т. д. Пользователи уровня 7 имеют доступ ко всем объектам.
- Пользователи, имеющие мандатную метку «Метка 1», имеют доступ только к объектам ФС, имеющим мандатную метку «Метка 1».

Назначать уровень доступа и мандатную метку дискам и каталогам, а также устанавливать для пользователей уровень доступа и мандатную метку к конфиденциальной информации может только тот пользователь, который наделен соответствующими полномочиями на администрирование системы защиты.

Примечание. Первый вход на ЗАРМ под учетной записью пользователя, которому назначен уровень доступа или мандатная метка, необходимо произвести под нулевым уровнем («открытые данные») или без метки соответственно. При этом входе в системной папке ОС формируется профиль пользователя, необходимый для корректной работы в последующем под другими уровнями.

Также следует учесть, что для работы с конфиденциальной информацией следует установить уровень или метку доступа на все ресурсы, необходимые пользователю для доступа к работе, в том числе на папку, отвечающую за содержимое его рабочего стола.

Для корректной работы некоторых программ под уровнями мандатного доступа выше 0 может также потребоваться выполнить их первый запуск в сессии пользователя с нулевым уровнем («открытые данные») и без метки.

5.3.3 Назначение мандатного доступа на объекты

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Для того, чтобы назначить мандатный доступ на объект ФС, необходимо выполнить следующее:

1. Открыть его дескриптор безопасности, используя оболочку администратора Dallas Lock 8.0 (на вкладке основного меню «Контроль ресурсов» выбрать тип ресурса и двойным кликом на объекте вызвать окно дескриптора или через контекстное меню объекта (пункт «Права доступа»).
   В дескрипторе объекта необходимо открыть вкладку «Мандатный доступ» (рис. 106).

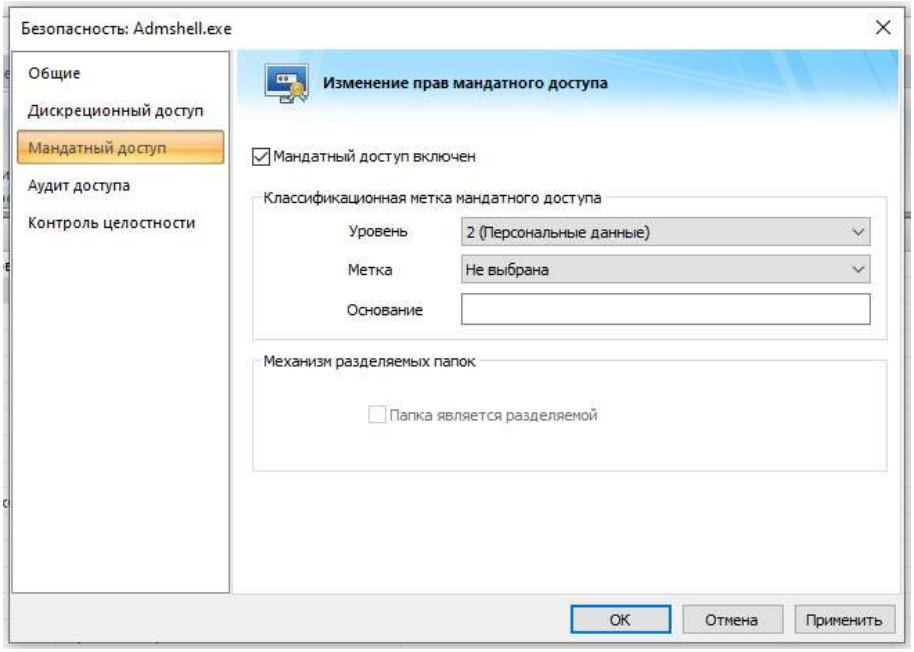


Рис. 106. Назначение прав доступа на объект ФС

2. Далее необходимо включить мандатный доступ, поставив флаг в поле «Мандатный доступ включен».
3. В выпадающих списках выбрать необходимые уровень доступа и мандатную метку.
4. Опционально заполнить поле «Основание».
5. Нажать кнопку «Применить» и «ОК».

Если мандатный доступ назначается на папку, то Включение механизма разделяемых папок (флаг в поле «Папка является разделяемой») определит для этой папки особый статус (см. «Механизм разделяемых папок»).

По умолчанию у объекта ФС отсутствует мандатная метка, а уровень доступа равен 0 («Открытые данные»). Для того, чтобы у пользователя имелась возможность повышать уровень доступа и изменять мандатную метку файлов/папок, нужно чтобы его учетная запись обладала правом «Параметры безопасности: управление».

Примечание. Пользователь не может назначить объекту ФС уровень доступа выше, чем назначенный для данной учетной записи уровень доступа. Также пользователь не может назначить объекту ФС мандатную метку, если учетной записи не назначена данная мандатная метка.

В окне категории «Мандатный доступ» («Контроль ресурсов» → «Мандатный доступ») контроля ресурсов формируется список всех установленных дескрипторов мандатного доступа на любых ресурсах (локальных, сетевых, сменных), установленных на данном защищенном ПК (рис. 107).

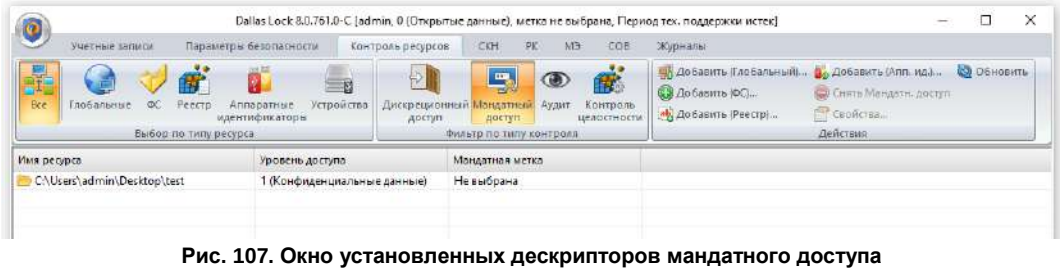


Рис. 107. Окно установленных дескрипторов мандатного доступа

5.3.4 Механизм разграничения мандатного доступа

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Когда пользователь осуществляет попытку доступа к объекту ФС, система защиты определяет уровень доступа и мандатную метку данного объекта. Затем они сопоставляются с текущими правами данного пользователя:

Условие	Результат
Уровень доступа объекта больше текущего уровня допуска пользователя	Доступ блокируется
Уровень доступа объекта равен текущему уровню допуска пользователя	Доступ разрешается
Уровень доступа объекта меньше текущего уровня допуска пользователя	Доступ разрешается, но только на чтение, попытки записи блокируются
Мандатная метка объекта совпадает с установленной для пользователя мандатной меткой	Доступ разрешается
Мандатная метка объекта не совпадает с установленной для пользователя мандатной меткой	Доступ блокируется

Примечание. Уровень доступа и мандатную метку возможно комбинировать, но необходимо учитывать то, что доступ предоставляется в соответствии с ограничениями выбранного уровня доступа. Например, если уровень доступа объекта меньше текущего уровня доступа пользователя, при этом выбрана любая метка, то доступ разрешается, но только на чтение и попытки записи будут блокироваться.

Внимание! Если включен режим удаления в корзину, то удаление объектов, имеющих мандатную метку или мандатный уровень больше нуля, будет блокироваться (так как удаление в корзину фактически представляет собой операцию переноса). Для удаления таких объектов необходимо в свойствах корзины включить опцию «уничтожать файлы сразу после удаления, не помещая их в корзину» либо при удалении удерживать клавишу «Shift». Объекты с меткой ноль могут быть удалены в корзину (в этом случае файл не удаляется, а переносится в корзину).

5.3.5 Механизм разделяемых папок

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Пользователь может сохранять созданные файлы только в папках, для которых определены уровень доступа и мандатная метка равные текущим правам допуска данного пользователя.

Некоторым программам, например, MS Office, требуется производить запись в свою системную папку под любым уровнем мандатного доступа, иначе программа работать не будет.

В системе защиты Dallas Lock 7.7 это решалось настройкой механизма процессов-исключений и механизма «папки для временных файлов». Но эти механизмы имели свои недостатки, например, процессы-исключения добавляли потенциальную возможность утечки информации, а объекты в папках для временных файлов удалялись в процессе завершения работы пользователя.

Для удобства, корректной и безопасной работы в системе защиты Dallas Lock 8.0 реализован особый механизм разделяемых папок.

Разделяемая папка — это папка, которая имеет одно конкретное расположение, но в зависимости от уровня, под которым входит пользователь, он физически попадает в папку со своим уровнем доступа.

Таким образом, если некоторую папку пометить как разделяемую, то в ней можно будет создавать любые файлы независимо от текущего уровня доступа. И в процессе завершения сеанса работы все объекты в этой папке будут сохранены.

Примечание. Разделение папок следует делать по принципу минимальной достаточности. Чем выше по иерархии системного раздела будет сделано разделение папки, тем выше вероятность ухудшения совместимости со сторонним ПО и снижения стабильности работы системы. В частности, не следует делать разделяемым профиль пользователя, так как функционирования стороннего ПО всегда удается добиться более конкретными настройками СЗИ.

Для того, чтобы пометить папку как разделяемую, нужно в контекстном меню «Права доступа» данной папки выбрать вкладку «Мандатный доступ», включить мандатный доступ и поставить флаг в поле «Папка является разделяемой» (рис. 108), нажать кнопки «Применить» и «ОК».

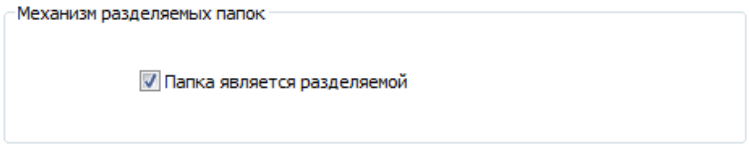


Рис. 108. Включение механизма разделяемой папки

Устанавливать мандатный уровень для разделяемой папки не требуется. В некоторых случаях, если необходимо разделить папку в профиле пользователя, то лучше сделать это, войдя в ОС под учетной записью суперадминистратора.

Внимание! Создание разделяемых папок требует фактического копирования этих папок в нескольких экземплярах, поэтому не рекомендуется создавать их с большим объемом данных.

Примечание. Разграничивать доступ объектам, находящимся в разделяемых папках, невозможно, так как они не предназначены для хранения конфиденциальных данных.

Примечание. Включение свойства разделяемости на папку, для которой назначено разграничение доступа, невозможно (включая разделение доступа через права NTFS).

Удалить или переименовать папку, которая помечена как разделяемая невозможно. Попытка ее удаления или переименования без снятия свойства разделяемости не будет завершена, и будет выведено соответствующее предупреждение.

Чтобы удалить или переименовать такую папку, необходимо отключить свойство разделяемости папки в параметрах доступа. После снятия соответствующего флага и нажатия кнопки «Применить» появится сообщение о том, что после подтверждения операции все конфиденциальные данные (не только те, что видны на данном мандатном уровне) будут удалены. Только после этого папку можно удалить или переименовать.

Примечание. Включение свойства разделяемости на диск С невозможно. При включении данного механизма на другой жесткие диск может появляться сообщение о поврежденной Корзине, но на работу системы защиты или ОС это не влияет.

5.3.6 Текущий уровень и метка доступа пользователя

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

При входе в ОС пользователь может выбрать:

- Уровень доступа, не превышающий установленный для него уровень доступа. Если пользователь имеет уровень доступа 5, то он может войти в систему с уровнями 0, 1, 2, 3, 4 или 5. Если пользователь выберет уровень доступа, превышающий собственный уровень доступа, то Dallas Lock 8.0 выдаст сообщение об ошибке «Мандатный уровень указан неверно».
- Мандатную метку, совпадающую с установленной для него мандатной меткой. Если пользователю установлены мандатные метки «Бухгалтеры» и «Футболисты», то он может войти в систему используя только данные мандатные метки. Если пользователь выберет

другие мандатные метки, не совпадающие с установленными, то Dallas Lock 8.0 выдаст сообщение об ошибке «Мандатная метка указана неверно».

Сменить текущие права доступа, с которыми пользователь вошел в систему, можно двумя способами:

1. Завершить текущий сеанс работы пользователя, и начать новый, выбрав при входе соответствующий уровень и метку доступа.
2. Воспользоваться пунктом «Свойства пользователя» из контекстного меню значка блокировки на панели задач BlockIcon (рис. 109).

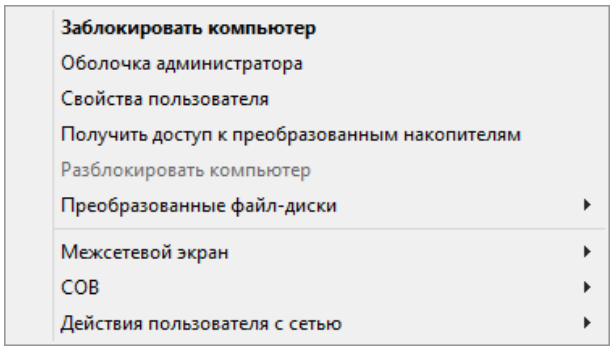


Рис. 109. Контекстное меню значка блокировки

Примечание. Переключение мандатной метки через BlockIcon доступно только для суперадминистратора.

Смена мандатного уровня возможна в появившемся окне свойств текущего пользователя в поле выбора уровня доступа (рис. 110).

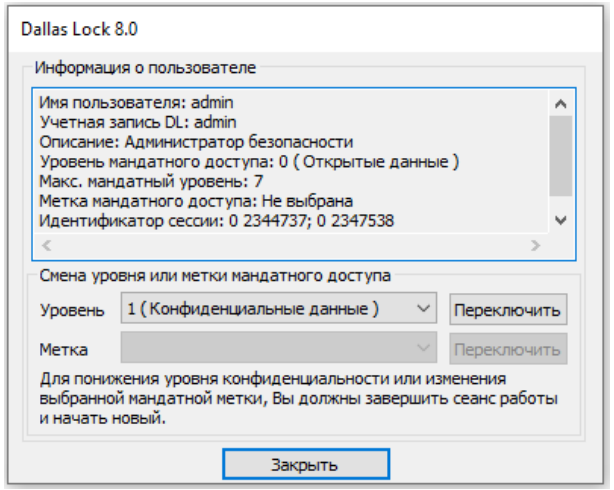


Рис. 110. Выбор уровня доступа в дополнительном окне значка блокировки

Чтобы поднять текущий мандатный уровень, необходимо нажать кнопки «Переключить» и «Закрыть», — уровень доступа изменится на следующий. Следует внимательно использовать данную функцию. С помощью данного окна можно поднять уровень доступа, но опустить нельзя. Опустить текущий уровень доступа можно, только начав новый сеанс работы.

Примечание. Измененные свойства сессий (повышенный уровень и/или назначенная метка) работает применительно к:

1. Текущей локальной интерактивной сессии.
2. Инициированным начиная с данного момента сессиям.

Соответственно, воздействовать таким образом на ранее запущенные на удаленных машинах сетевые сессии нельзя.

Примечание. Если уровень доступа повысить с помощью BlockIcon, то будет запрещен доступ к сетевым папкам или дискам с назначенным уровнем доступа. Для доступа необходимо или переподключить сетевые диски или выйти из системы и войти заново с необходимым уровнем доступа.

Примечание. При мандатном доступе к сетевым ресурсам (мандатный принцип управления доступом доступен только для Dallas Lock 8.0 редакции «С»), на которые назначен уровень доступа выше «Открытые данные», необходимо выбирать соответствующий уровень доступа перед входом в ОС. В противном случае при повышении уровня доступа через BlockIcon, будет повышаться только уровень доступа локальной сессии пользователя, уровень доступа удаленной сессии останется прежним.

Примечание. Для корректной работы подсистемы мандатного доступа в Windows 10 версии 1903 и выше требуется отключить системную политику, отвечающую за сохранение активности сессии пользователя после перезагрузки ОС. Способ отключения политики через системные настройки: отобразить оснастку Редактора локальной групповой политики, выбрать «Конфигурация компьютера» → «Административные шаблоны» → «Компоненты Windows» → «Параметры входа Windows» → параметр «Автоматически выполнять вход и блокировать последнего текущего пользователя после перезагрузки», установить значение «Отключено». Способ отключения через реестр: в ветку HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System добавить параметр DisableAutomaticRestartSignOn (REG_DWORD) со значением 1.

5.3.7 Служебный пользователь

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

На защищенном СЗИ компьютере одновременный вход нескольких интерактивных пользователей с различными уровнями или метками мандатного доступа по умолчанию разрешен.

С помощью соответствующего параметра в параметрах входа[10] можно включить запрет на одновременную работу нескольких интерактивных пользователей, зашедших под разными уровнями или метками мандатного доступа.

Некоторые приложения при установке создают свои учетные записи пользователей, и при загрузке ОС осуществляется автоматический вход данных пользователей для того, чтобы приложения могли работать. Например, при использовании программы VipNet или VMware. В списке сессий на вкладке «Учетные записи» будет присутствовать запись об интерактивной сессии данного пользователя.

По умолчанию для данных учетных записей уровень мандатного доступа определен как «Открытые данные», а мандатная метка отсутствует. И если политиками безопасности предприятия определено, что одновременный вход пользователей с различными уровнями доступа или мандатными метками запрещен (включен запрет в параметре «Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа»), то для корректной работы ПО на данном ПК необходимо поставить особое свойство «Служебный пользователь» для учетной записи данного пользователя.

[10] «Вход: запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа».

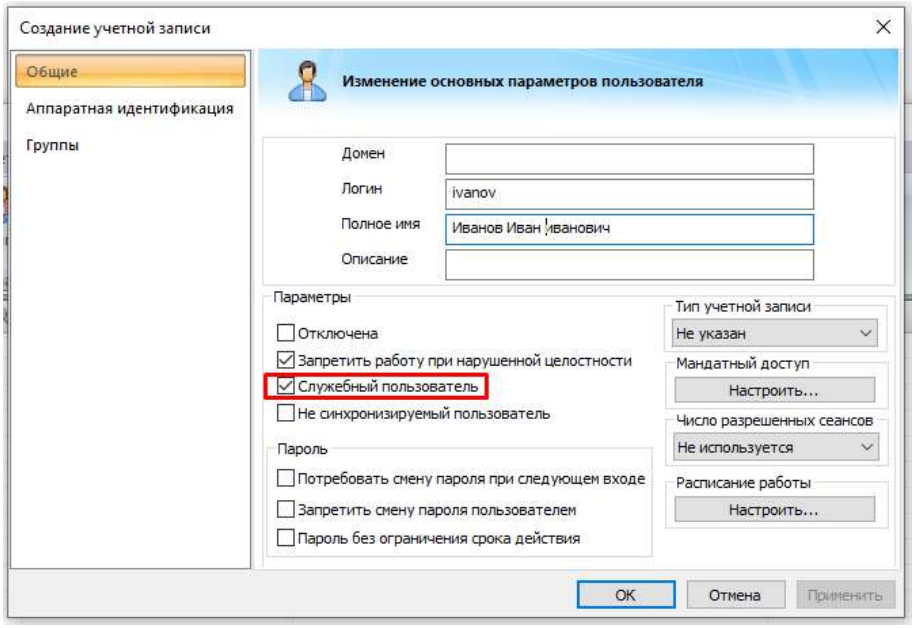


Рис. 111. Включение параметра «Служебный пользователь»

Если пометить учетную запись как «Служебный пользователь», то для нее не будут действовать ограничения на вход с различными уровнями или метками мандатного доступа.

5.3.8 Пример настройки мандатного доступа по сети

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Допустим, в ЛВС имеется несколько защищенных Dallas Lock 8.0 компьютеров, на одном из которых расположена папка, открытая на удаленный доступ «…\\имя_сетевого_ресурса\Secretno». На удаленном компьютере необходимо настроить мандатный доступ для работы с этой папкой.

Для этого необходимо на сетевом ресурсе назначить мандатный доступ к данной папке «Secretno» (рис. 112).

Имя ресурса	Уровень доступа	Мандатная метка
C:\Secretno\	3 (Секретно)	Не выбрана

Рис. 112. Пример настроенной сетевой папки на локальном ресурсе для мандатного доступа

На удаленном компьютере для сетевой папки «…\\имя_сетевого_ресурса\Secretno» назначить такой же мандатный доступ (рис. 113).

Имя ресурса	Уровень доступа	Мандатная метка
NET:\\SECSERVER\Secretno\	3 (Секретно)	Не выбрана

Рис. 113. Пример настроенной сетевой папки для мандатного доступа на удаленном ПК

На рис. 113 для папки по пути «NET:\\SECURITYS\Secretno\» присвоен уровень доступа 3 «Секретно», а мандатная метка не выбрана. В данном случае для пути прописано NetBIOS-имя ПК. Проверка доступа будет происходить по строке, и поэтому, если будут назначены права, используя путь с IP-адресом компьютера, то для пути с использованием NetBIOS-имени эти права работать не будут, необходимо дополнительно назначить мандатный доступ на данную папку, открыв ее по IP-адресу компьютера (рис. 114). И наоборот.

Имя ресурса	Уровень доступа	Мандатная метка
NET:\\192.168.130.193\Secretno	3 (Секретно)	Не выбрана

Рис. 114. Сетевая папка на клиенте с настроенным мандатным доступом через IP ПК

5.3.9 Настройка мандатного доступа для корректной работы пользователя с ПО

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

В мандатном режиме доступа для корректной работы пользователей с установленным ПО требуются определенные настройки в Dallas Lock 8.0-С.

Настроить мандатный доступ для работы с ПО пользователю можно либо стандартным способом (с помощью механизма разделяемых папок), либо воспользовавшись автоматической настройкой.

Настройка мандатного доступа с помощью механизма разделяемых папок

Данный механизм доступен только для Dallas Lock 8.0 редакции «С».

Для того, чтобы настроить мандатный доступ с помощью механизма разделяемых папок, необходимо:

1. Определить уровень доступа для учетной записи пользователя.
2. Включить полный аудит отказов для параметров по умолчанию (вкладка «Контроль ресурсов» → «Глобальные» → «Параметры ФС по умолчанию»).
3. Включить «мягкий» режим контроля доступа, для этого нужно:
   - Открыть окно настройки неактивного режима (кнопка  основного меню → «Настройка режимов работы» → «Настроить неактивный режим») и нажать кнопку «Мягкий режим» (см. «Мягкий режим»).
4. Перезагрузить компьютер.
5. Зайти под учетной записью выбранного пользователя под его уровнем доступа.
6. Запустить необходимые приложения (например, MS Office Word или Excel) и выполнить необходимые операции.
7. Перезапустить ОС и зайти под учетной записью администратора безопасности.
8. В оболочке администратора открыть «Журнал ресурсов» (вкладка основного меню «Журналы»). В нем настроить и применить фильтр для просмотра отказов доступа необходимого пользователя (рис. 115).

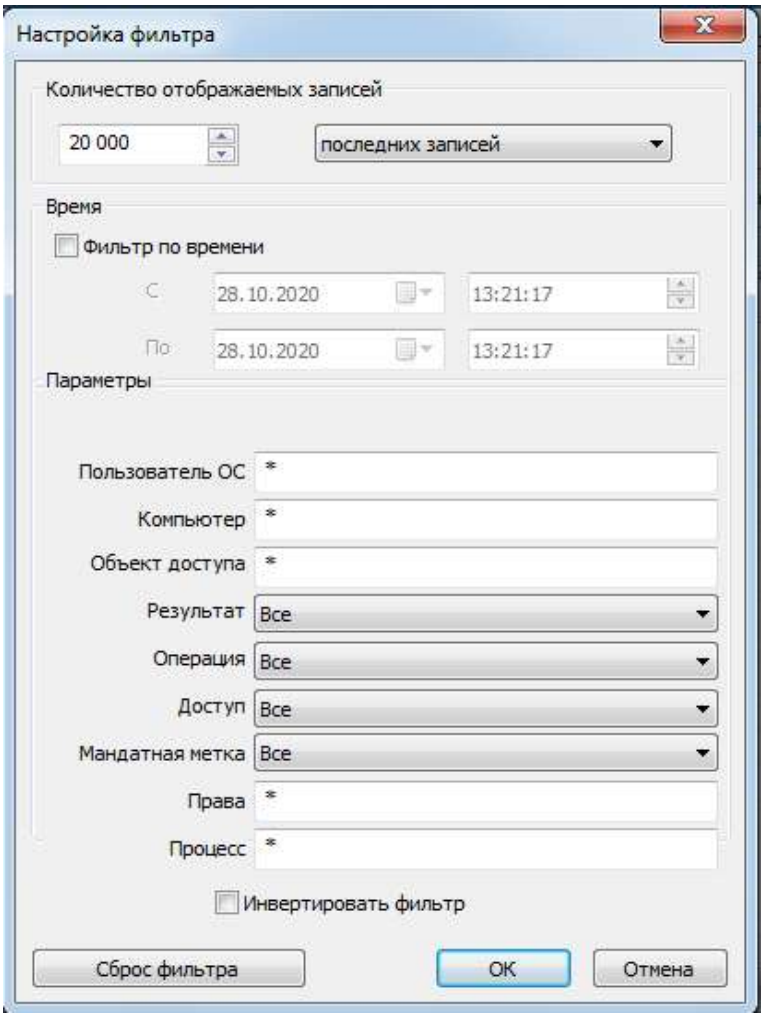


Рис. 115. Фильтр записей журнала доступа к ресурсам пользователя

9. Определить системную папку, из которой запускаются необходимые для пользователя приложения, и на данную папку назначить свойство разделяемости (см. «Механизм разделяемых папок») (рис. 116).

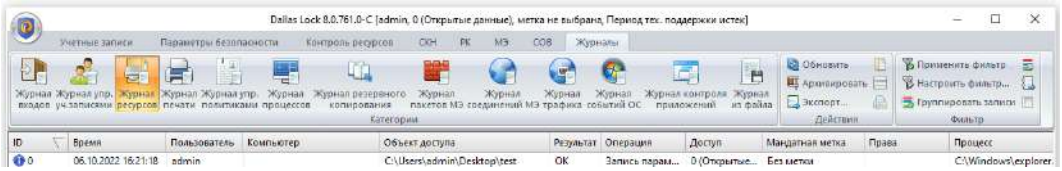


Рис. 116. Записи журнала доступа для определения разделяемой папки

10. Мягкий режим следует отключить.

Автоматическая настройка мандатного доступа

Данный параметр доступен только для Dallas Lock 8.0 редакции «С»

В автоматическом режиме настройка мандатного доступа представляет собой применение шаблона мандатного доступа с помощью отдельной функции.

Шаблоны мандатного доступа хранятся в папке по пути C:\DLLOCK80\MandatTemplates и представляют собой особые файлы конфигурации Dallas Lock 8.0-C. Каждый имеющийся в данной папке шаблон предназначен для определенной программы или версии программы.

Примечание. Перед автоматической настройкой мандатного доступа рекомендуется сохранить конфигурацию (см. «Сохранение конфигурации»).

В отношении пользователей, для которых работа с программами настраивается с помощью

мандатного доступа, необходимо выполнение следующих условий:

- Учетная запись должна быть зарегистрирована в СЗИ.
- Должен быть осуществлен вход на ЗАРМ под учетной записью данного пользователя под нулевым уровнем вне зависимости от того, какой уровень доступа ему назначен. При этом входе в системной папке ОС формируется профиль пользователя, необходимый в последующем для корректной работы под другими уровнями и для настройки шаблонов.
- Для доменных пользователей необходимо, чтобы был осуществлен вход под той доменной учетной записью, для которой произведется настройка шаблона.

Чтобы применить шаблон мандатного доступа необходимо выполнить следующее:

1. Необходимо нажать кнопку основного меню и в списке дополнительных функций последовательно выбрать «Конфигурация» → «Шаблоны мандатного доступа» (рис. 117).

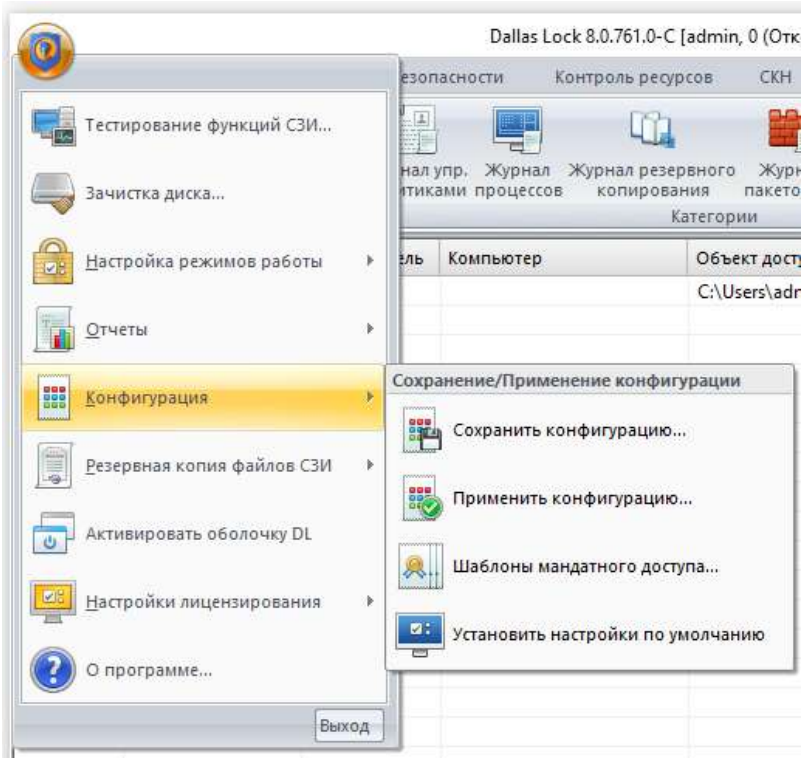


Рис. 117. Выбор автоматической настройки мандатного доступа

2. Появится окно со списком имеющихся шаблонов настройки мандатного доступа для определенных программ (рис. 118). В данном окне необходимо выбрать шаблон и нажать «ОК».

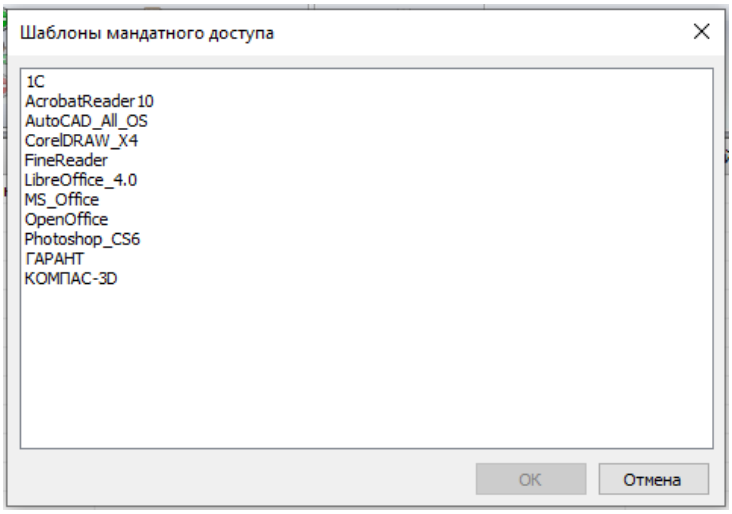


Рис. 118. Выбор шаблона для автоматической настройки

3. После выбора шаблона появится окно со списком учетных записей, для которых возможна настройка выбранного шаблона. Необходимо отметить нужных пользователей и нажать «ОК» (рис. 119).

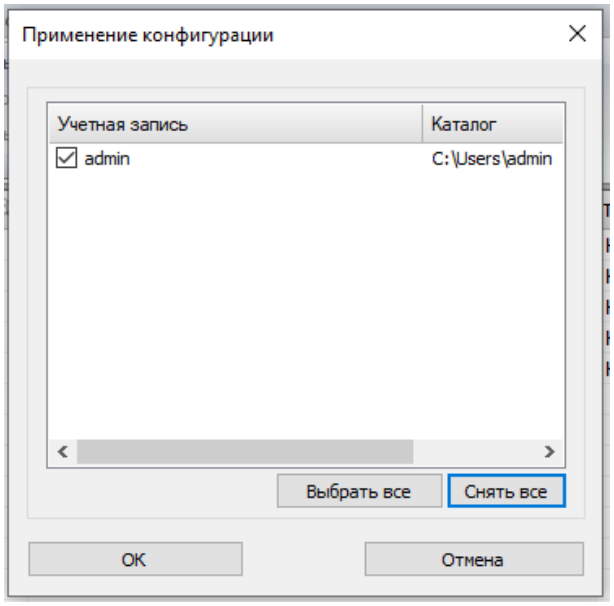


Рис. 119. Выбор учетных записей для настройки шаблона

После этого запустится настройка контроля доступа. В результате появится отчет о настройке.

В итоге применения шаблона выбранный пользователь сможет работать с программой в соответствии с правилами разграничения мандатного доступа (см. «Механизм разграничения мандатного доступа»).

В списке настроенных ресурсов («Контроль ресурсов» → «Мандатный доступ») появятся записи о новых конфигурациях.

Отменить настройки, сформированные для мандатного доступа пользователей и ПО, можно следующими способами:

- применением сохраненного перед настройкой файла конфигурации;
- возвратом к настройкам по умолчанию (в этом случае будут обновлены и удалены и другие настройки параметров);
- сняв свойство разделяемости и отключив мандатный доступ для ресурсов, на которые они были назначены в процессе применения шаблона, через список настроенных ресурсов.

5.4 Дополнительные режимы доступа

5.4.1 Режим обучения

В Dallas Lock 8.0 реализован особый механизм контроля доступа к ресурсам — «режим обучения». Он позволяет одновременно фиксировать события о запрете доступа и автоматически назначать права на ресурсы, к которым доступ блокируется.

Чтобы включить режим обучения, необходимо нажать кнопку  основного меню и в списке дополнительных функций выбрать «Настройка режимов работы» → «Включить режим обучения» (рис. 120).

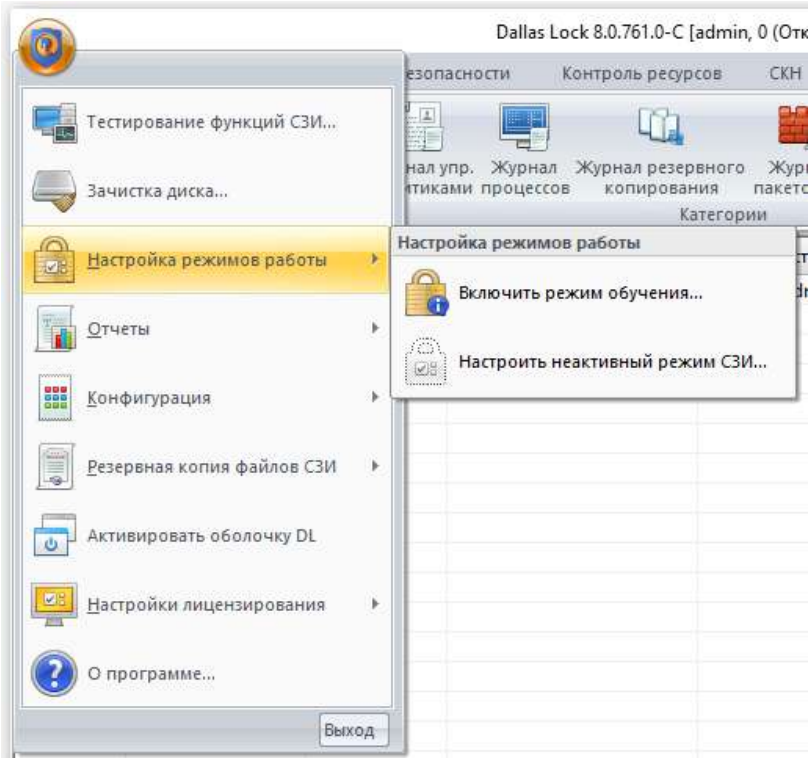


Рис. 120. Включение режима обучения

Появится окно подтверждения включения данного режима (рис. 121).

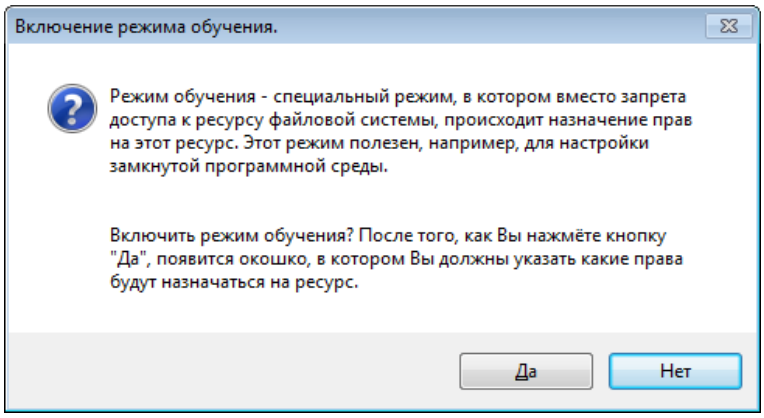


Рис. 121. Включение режима обучения

После включения режима обучения появится окно дескриптора доступа, в котором необходимо указать, какие параметры безопасности и какому пользователю должны быть автоматически назначены на ресурсы, к которым блокируется доступ. В процессе работы на необходимые для работы объекты ФС будет происходить назначение тех дескрипторов, которые настроены при включении режима обучения, тем самым определяется настройка ЗПС (подробный пример см. «Замкнутая программная среда»).

Для включения/выключения режима обучения пользователь должен быть наделен правами на деактивацию системы защиты (вкладка «Параметры безопасности» → «Права пользователей» → параметр «Деактивация системы защиты»).

Примечание. Одновременное использование «мягкого» режима и «режима обучения» невозможно.

Событие включения (выключения) режима обучения фиксируется в журнале управления политиками.

5.4.2 Неактивный режим

В Dallas Lock 8.0 реализован особый механизм контроля доступа к ресурсам — «неактивный

режим». Его суть заключается в полном отключении подсистем СЗИ Dallas Lock 8.0.

Чтобы включить и настроить неактивный режим, необходимо нажать кнопку основного меню и в списке дополнительных функций выбрать «Настройка режимов работы» → «Настроить неактивный режим» (рис. 122).

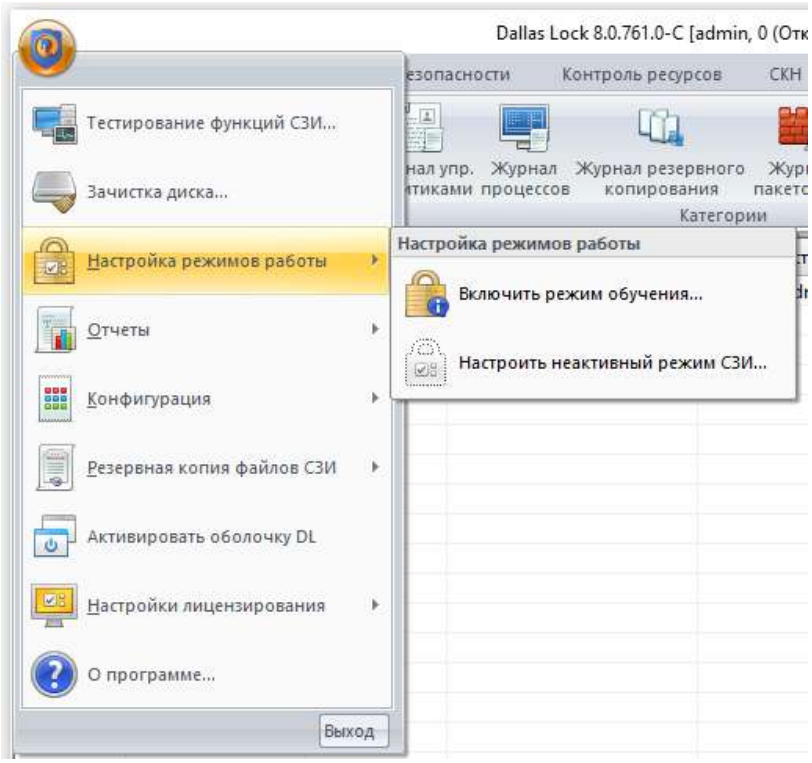


Рис. 122. Включение неактивного режима

Появится окно настройки неактивного режима (рис. 123), в котором необходимо определить, контроль каких подсистем отключить, а каких оставить.

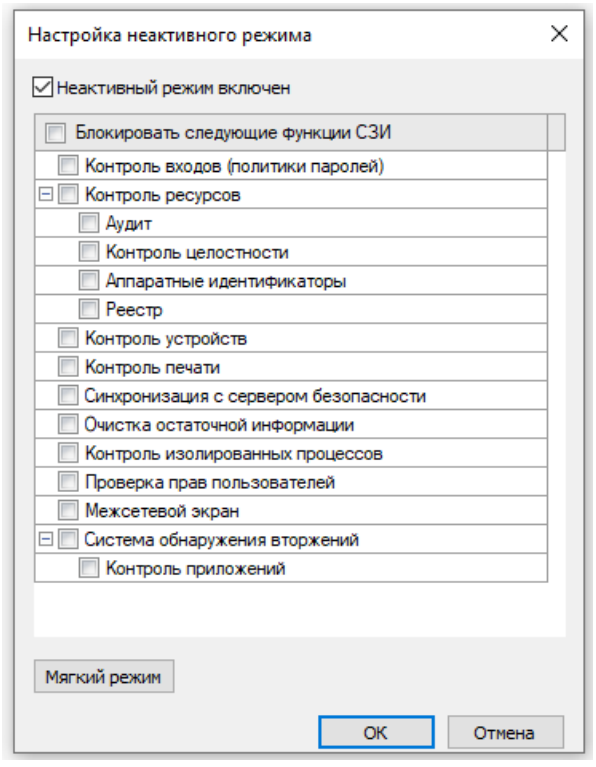


Рис. 123. Настройка неактивного режима

Примечание. При активации поля «Контроль целостности» деактивируется возможность блокировки изменения файла HOSTS (вкладка «СОВ» → «Параметры СОВ» → «Контроль приложений»).

В неактивном режиме Dallas Lock 8.0 минимально влияет на работу ОС. Включение данного режима может быть полезно для упрощения диагностики несовместимости Dallas Lock 8.0 со сторонним программным или аппаратным обеспечением, инфраструктурой сети и т. д.

Для включения/выключения неактивного режима пользователь должен быть наделен правами на деактивацию системы защиты (вкладка «Параметры безопасности» → «Права пользователей» → параметр «Деактивация системы защиты»).

Мягкий режим

Включение и настройка мягкого режима производится посредством неактивного режима, поэтому для того, чтобы включить и настроить «мягкий режим», необходимо нажать кнопку  основного меню и в списке дополнительных функций выбрать «Настройка режимов работы» → «Настроить неактивный режим».

Далее откроется окно «Настройка неактивного режима», где в правом нижем углу расположена кнопка «Мягкий режим». Она позволяет включать комбинацию настроек, при которых при обращении к ресурсам, доступ к которым запрещен, доступ все равно разрешается, но в журнал ресурсов заносится сообщение об ошибке. Для этого необходимо настроить права доступа и назначить аудит отказов на необходимые объекты, и включить мягкий режим.

События включения и выключения неактивного режима фиксируются в журнале управления политиками.

Внимание! Включение режимов **«**режим обучения» и «неактивный режим» достаточно рискованно для обеспечения информационной безопасности, так как любой пользователь получает доступ к любому объекту ФС. Поэтому важно отключать эти режимы, когда в них нет необходимости.

Для напоминания о том, что включены данные режимы, при входе пользователя после загрузки ОС в области уведомлений Windows будет появляться всплывающее предупреждение (рис. 124).

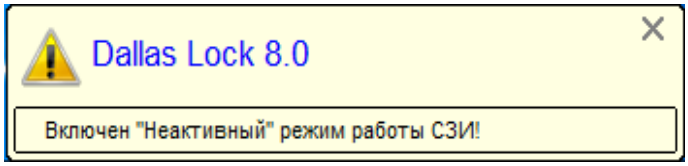


Рис. 124. Предупреждение о включенном неактивном режиме

5.4.3 Замкнутая программная среда

На одной рабочей станции может быть несколько пользователей, которые могут работать с разными программами в соответствии с политиками безопасности.

Для усиленных мер безопасности в системе Dallas Lock 8.0 существует механизм «Замкнутой программной среды» (ЗПС, иногда говорят: «Изолированная программная среда» — ИПС), который позволяет явно указать, с какими программами пользователь может работать (соответственно, со всеми остальными программами пользователь работать не может).

Для реализации механизма замкнутой программной среды необходимо произвести ряд настроек. Общий смысл настроек состоит в том, чтобы установить глобальный запрет на выполнение всех программ, а потом разрешить запуск только тех приложений, которые необходимы данному пользователю для работы. Для организации ЗПС используются механизмы дискреционного контроля доступа, в частности, право «Выполнение».

Для создания замкнутой программной среды рекомендуется все права назначать не для конкретного пользователя, а для специально созданной группы. В этом случае, если создать нового пользователя с теми же ограничениями на использования программ, достаточно будет добавить его в ту же самую группу, а не выполнять все настройки заново.

Первый вход только что созданного пользователя должен осуществляться без ограничений ЗПС, так как при первом входе в системной папке создается профиль пользователя. Таким же образом,

если на компьютере установлен Microsoft Office, то, при первом входе нового пользователя до включения ограничений ЗПС, нужно запустить какое-либо приложение Microsoft Office, так как он производит локальную установку в профиль. Только после того, как профиль пользователя создан, нужные приложения установлены и инициализированы, можно начинать настройку ЗПС (либо добавлять пользователя в группу с ЗПС-ограничениями).

Нужно помнить, что исполняемыми файлами считаются не только файлы с расширениями «*.exe», но и все другие файлы, которые открываются с флагами на выполнение. Это, прежде всего, «*.dll», «*.sys», «*.scr» и прочие. Таким образом, если необходимо разрешить пользователю работать с Microsoft Word, то недостаточно будет ему разрешить запускать файл «WINWORD.EXE». Ведь «WINWORD.EXE» использует также множество «*.dll» файлов, которые тоже нужно разрешить данному пользователю для запуска.

Примечание. Рекомендуется установить запрет на запись для всех разрешенных к выполнению программ. Тем самым блокируется возможность модификации и удаления этих программ.

Ниже приведены описания настройки ЗПС различными способами. Одним из альтернативных способов настройки может быть следующий. После глобального запрета запуска всего в глобальных параметрах, для пользователя (группы) необходимо разрешить запуск всего из папки «C:\WINDOWS». Главное — отключить возможность для этого пользователя (группы) менять содержимое этой папки. В папке Windows находятся важные системные файлы, доступ к которым необходим для корректной работы ОС. При этом способе настройки ничто не мешает отдельно запретить запуск некоторых файлов из папки Windows.

Настройка ЗПС с использованием неактивного режима

Для настройки ЗПС с использованием неактивного режима в системе защиты Dallas Lock 8.0 существует дополнительный механизм «Права для файлов». Пример такой настройки ЗПС описан ниже.

Пусть пользователь, для которого нужно организовать ЗПС, уже создан и инициализирован (к примеру, он называется zps). Далее для настройки ЗПС необходимо выполнить следующие шаги по настройке:

1. Создать специальную группу, например, ZPS-gr, и включить пользователя zps в группу ZPS-gr.
2. Для группы ZPS-gr в глобальных настройках запретить запуск всего (вкладка «Контроль ресурсов» → «Глобальные» → «Параметры ФС по умолчанию») (рис. 125).

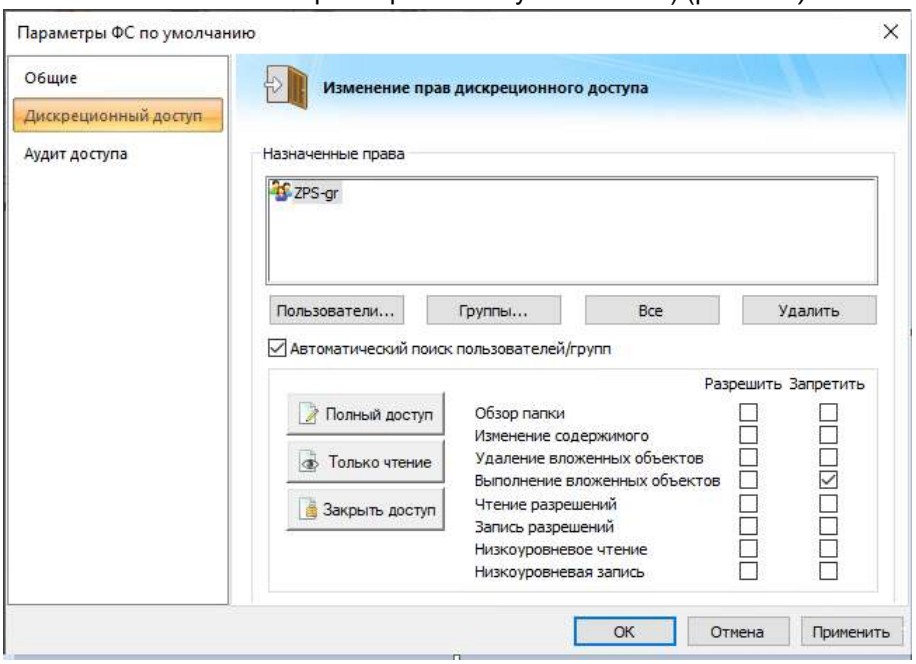


Рис. 125. Глобальный запрет запуска программ для настройки ЗПС

3. В дескрипторе «Параметры ФС по умолчанию» включить полный аудит отказов (рис. 126).

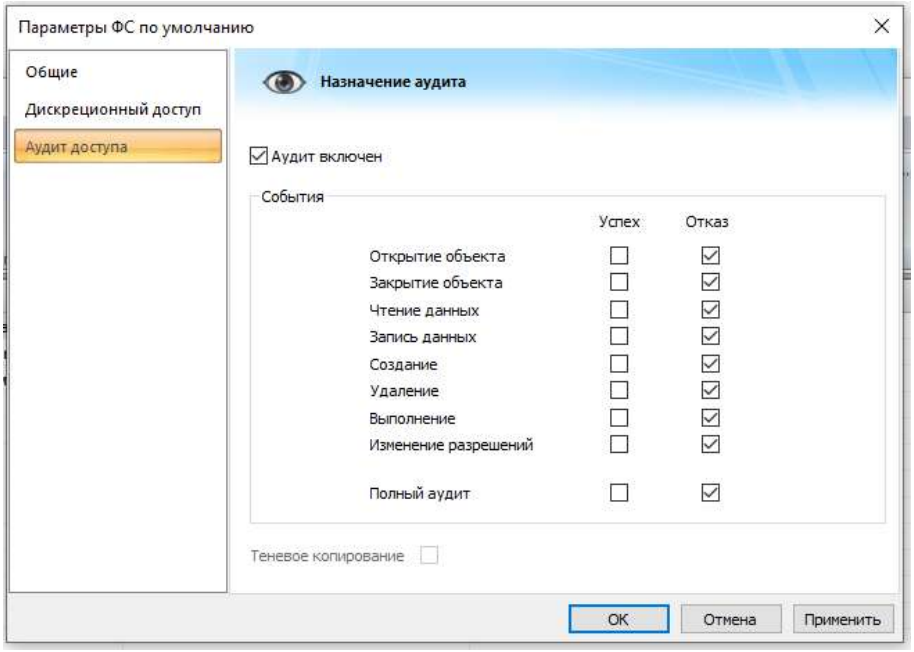


Рис. 126. Включение аудита доступа

4. Далее необходимо настроить неактивный режим работы СЗИ (пункт меню кнопки основного меню «Настройка режимов работы» → «Настроить неактивный режим»). В окне настройки необходимо включить «Мягкий режим» контроля доступа. Дополнительно желательно очистить (архивировать) журнал ресурсов.
5. Отправить компьютер в перезагрузку.

Примечание. Необходимо именно перезагрузить компьютер. Просто завершить сеанс работы одного пользователя и зайти под другим недостаточно — при загрузке компьютера используется другой набор исполняемых модулей. При смене пользователя событие загрузки ОС не попадет в журнал ресурсов, и в результате настройки ЗПС данным способом этот пользователь не сможет осуществить вход.

6. Осуществить вход в ОС под учетной записью пользователя zps. Запустить все те приложения, с которыми пользователь имеет право работать (но не запускать ничего лишнего).
7. Следует помнить, что не для всех приложений является достаточным просто их запуск. Некоторые сложные приложения на своем старте загружают не все исполняемые модули, а только необходимые, остальные модули они подгружают динамически, в процессе работы. Поэтому после запуска приложения лучше выполнить все основные действия приложения для работы.
8. На этом этапе в журнале доступа к ресурсам формируется список файлов, которые нужны данному пользователю для работы.
9. Далее следует осуществить смену пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора СЗИ, открыть журнал ресурсов.
10. Настроить и применить фильтр журнала доступа к ресурсам: пользователь — «zps», результат — «ошибка» (рис. 127).

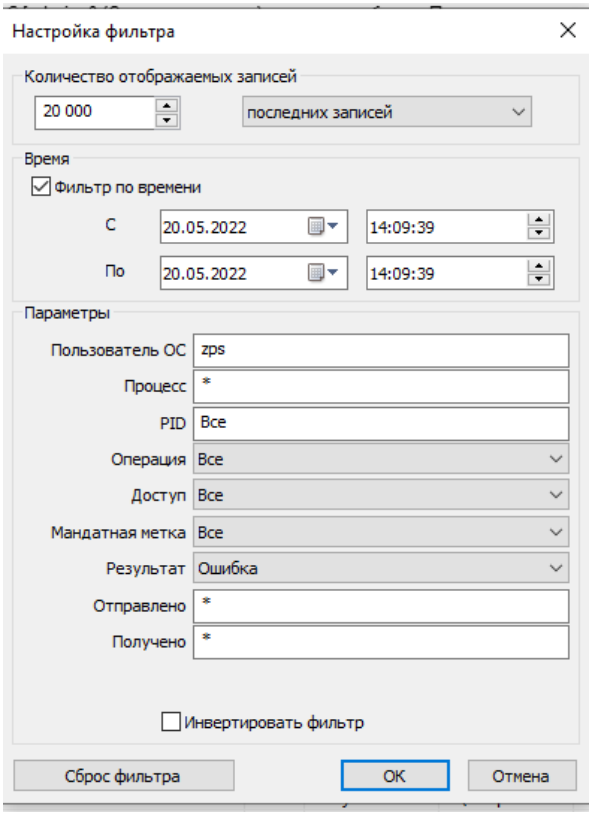


Рис. 127. Фильтр журнала доступа к ресурсам

11. Далее необходимо выделить поле с записями журнала и выбрать на панели действий «Права для файлов» (или нажать эту кнопку в появившемся отдельном окне выбранной записи журнала или выбрать из контекстного меню) (рис. 128).

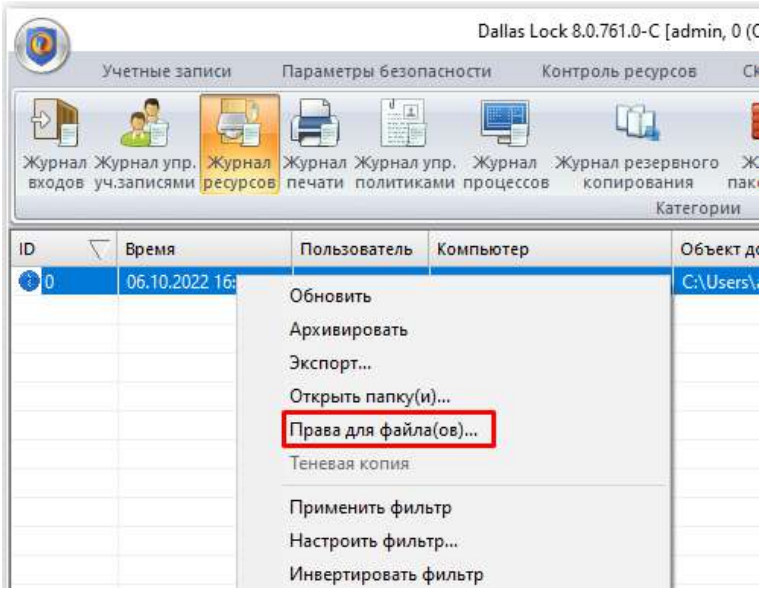


Рис. 128. Контекстное меню в журнале доступа к ресурсам

12. В появившемся окне редактирования дескриптора безопасности назначить дискреционные права для группы ZPS-gr «только чтение» и нажать «ОК» (рис. 129).

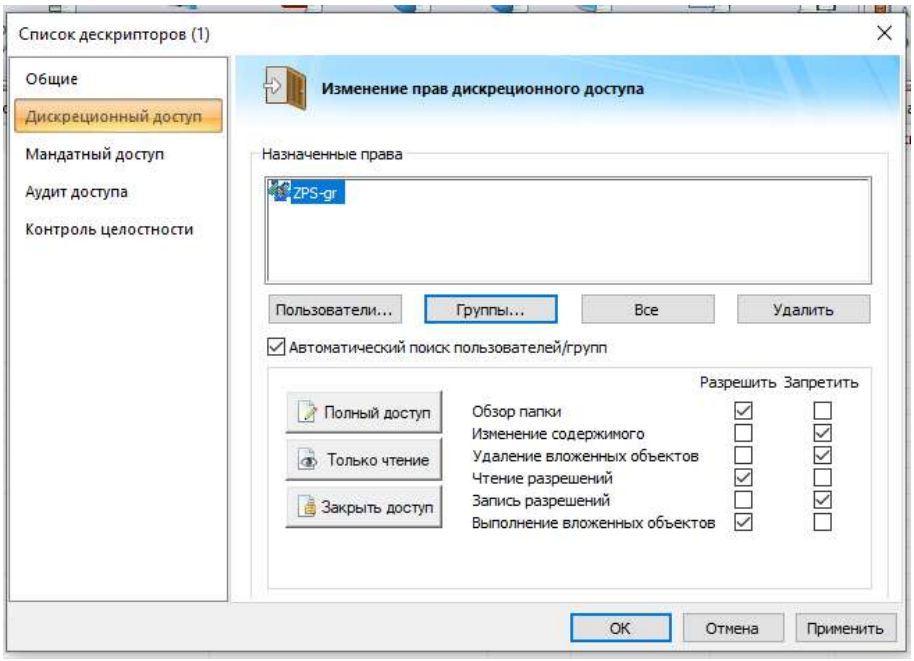


Рис. 129. Назначение дискреционных прав для файлов

После нажатия кнопки «ОК» система защиты попросит пользователя выбрать еще одно действие для настройки параметров безопасности (рис. 130).

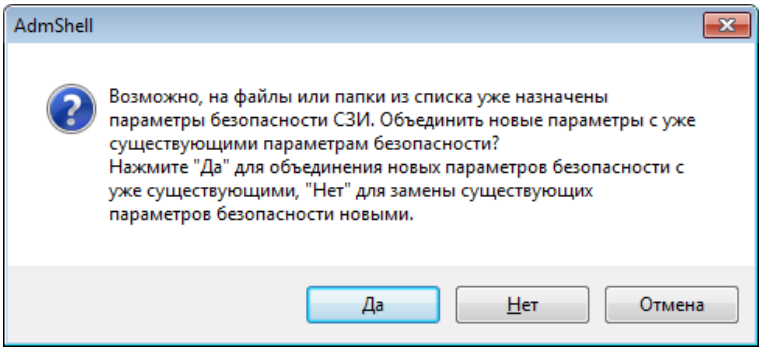


Рис. 130. Настройка параметров безопасности

13. В этом случае, если назначаются права на доступ к ресурсам для группы ZPS-gr впервые, то параметры безопасности будут созданы независимо от выбранного значения «Да» или «Нет». Если же необходимо добавить параметр (например, право запускать еще какую-либо программу), то в этом случае следует нажать кнопку «Да», чтобы добавить параметр и не потерять существующие.

14. Таким образом, замкнутая программная среда организована. Теперь необходимо отключить «мягкий режим» и зайти пользователем zps. Этот пользователь сможет работать только с необходимыми программами.

Следует помнить, что вполне вероятна ситуация, когда не все нужные для работы пользователя исполняемые файлы занеслись в список. Так как некоторые приложения вызывают какие-либо другие исполняемые файлы только при активизации определенных функций. Если после включения ЗПС у пользователя zps какое-либо приложение стало работать неправильно — это можно сразу же увидеть в журнале доступа к ресурсам. Скорее всего, для какого-либо еще исполняемого файла необходимо добавить право на исполнение (действие «Права для файлов» → «Только чтение») для данного пользователя (группы).

Настройка ЗПС с использованием режима обучения

Пусть пользователь, для которого нужно организовать замкнутую программную среду, уже создан и инициализирован (к примеру, он называется zps). Далее для настройки ЗПС, необходимо выполнить следующие шаги по настройке:

1. Как и в примере по настройке ЗПС с использованием неактивного режима (описано выше), необходимо создать специальную группу, например, ZPS-gr, включить пользователя zps в группу ZPS-gr и для группы ZPS в глобальных настройках запретить запуск всего (рис. 125).

2. В списке дополнительных функций кнопки основного меню  необходимо включить «Настройка режимов работы» → «Включить режим обучения».
3. Далее, в появившемся окне дискреционного доступа назначить для выбранной группы параметр безопасности «только чтение». Это просто сделать, нажав саму кнопку «только чтение» (рис. 131).

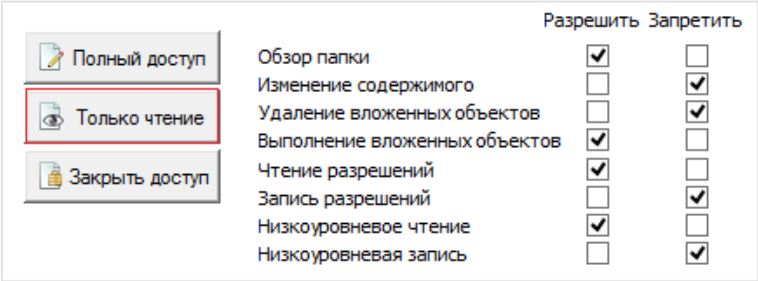


Рис. 131. Настройка прав доступа для режима обучения

4. Теперь необходимо перезагрузить компьютер и осуществить вход под учетной записью пользователя zps.
5. Поработать немного под этим пользователем, запустив необходимые приложения. В процессе работы в режиме обучения на запущенные приложения назначается дескриптор в соответствии с произведенной настройкой при включении режима.
6. В период пока включен режим обучения, пользователю zps становятся доступны для запуска все необходимые приложения.
7. Чтобы выключить режим обучения для пользователя, необходимо завершить его сеанс, зайти под учетной записью администратора и выбрать в дополнительном меню «Настройка режимов работы» → «Выключить режим обучения». После выключения доступ к приложениям будет определяться в соответствии с назначенными правами в процессе режима обучения.

5.5 Графическая оболочка Dallas Lock

5.5.1 Включение и выключение оболочки

Вместо стандартной графической оболочки пользователя Windows (англ. Windows shell), программы, которая отвечает за создание рабочего стола, панели задач и меню «Пуск», в СЗИ Dallas Lock 8.0 может использоваться специальная защищенная оболочка.

Оболочка Dallas Lock позволяет создавать защищенный рабочий стол без меню «Пуск» и панели задач, позволяя пользователю запускать только «ярлыки» приложений, определенные администратором. Такой режим может использоваться в дополнении к режиму «Замкнутая программная среда», чтобы предоставить пользователю максимально ограниченный интерфейс, предназначенный только для выполнения профессиональных задач.

Для включения оболочки Dallas Lock 8.0 необходимо в списке дополнительных функций кнопки  основного меню выбрать пункт «Активировать оболочку DL» (рис. 132).

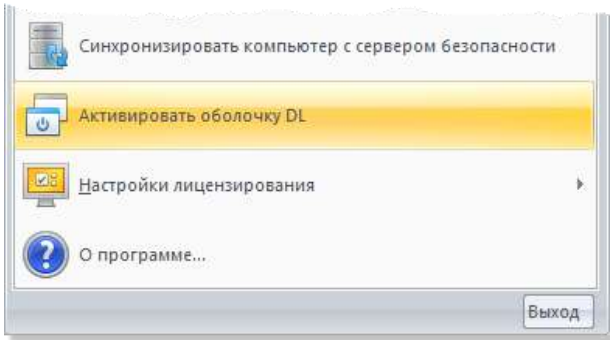


Рис. 132. Выбор установки оболочки Dallas Lock

Оболочка Dallas Lock будет применена для всех пользователей в ОС после завершения сеанса (выхода из системы) (рис. 133).

Рис. 133. Оболочка Dallas Lock

В правой части защищенного рабочего стола располагается список запущенных приложений, позволяющий пользователю переключаться между приложениями. Этот список является упрощенной версией диспетчера задач стандартной оболочки.

Основным механизмом ограничения оболочки Dallas Lock является блокировка меню «Пуск» и контекстного меню рабочего стола. Однако, пользователи, нажав комбинацию клавиш «Ctrl + Alt + Del», могут запустить диспетчер задач и уже из него попытаться выполнить любое приложение (при наличии прав на запуск).

Чтобы исключить возможность запуска диспетчера задач и избежать лишних попыток пользователя перебирать приложения с правами на запуск, необходимо заблокировать диспетчер задач. Блокировка реализуется через групповые политики Windows. Настроить групповую политику для группы компьютеров можно через групповые политики AD, если используется домен AD, либо самостоятельно отредактировав локальную групповую политику локального компьютера. Оболочка Dallas Lock предоставляет возможность запустить редактор групповых политик и отключить диспетчер задач локально. Для этого в запущенной оболочке необходимо выбрать пункт «Отключить диспетчер задач», после чего появится окно подтверждения действия (рис. 134).

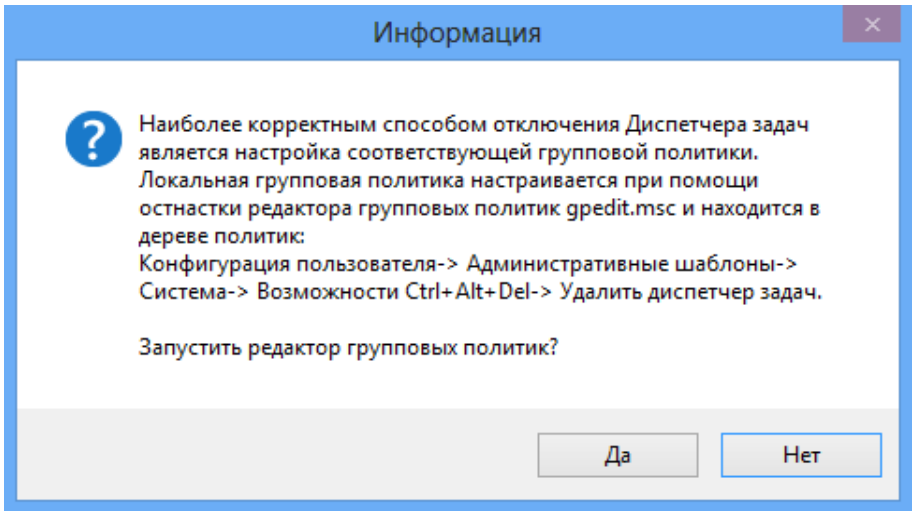


Рис. 134. Окно запуска редактора групповых политик

Следует учесть, что данная групповая политика применяется ко всем пользователям, работающим на данном компьютере.

Для применения нового значения необходимо завершить сеанс и снова войти в систему. Если политика настраивается через контроллер домена AD, то для ускорения применения политики на рабочих станциях перед выходом пользователя (с правами администратора) из системы требуется запустить утилиту gpupdate. После применения данной политики при попытке запуска диспетчера задач будет появляться сообщение «Диспетчер задач отключен администратором».

Для выключения оболочки Dallas Lock и включения графической оболочки Windows необходимо зайти в систему с правами администратора безопасности, и в списке дополнительных функций оболочки администратора, как и при включении, выбрать пункт «Активировать оболочку Explorer» и перезагрузить компьютер. Стандартная оболочка Windows станет доступной для всех пользователей.

5.5.2 Настройка оболочки

Все настройки оболочки Dallas Lock хранятся в файле «Zpsshell.ini» в системной папке «C:\Windows». Настройки позволяют определить внешний вид защищенного рабочего стола, список общих ярлыков для всех пользователей, а также список уникальных ярлыков для каждого пользователя (в том числе для доменных пользователей).

Изначально файл настроек содержит в себе пример настройки с установкой различных приложений для нескольких разных пользователей. Все настройки располагаются в различных секциях данного ini-файла и состоят из имени параметра и значения. Опираясь на примеры представленных настроек в данном файле, можно сформировать их для любого необходимого пользователя системы.

Среди общих настроек можно выбрать настройки фона оболочки, изменив его цвет или прописав путь к выбранному рисунку фона, а также изменить размер и расположение ярлыков и надписей. Следует помнить, что настройка параметров оболочки Dallas Lock доступна только пользователю с правами администратора и доступом к системной папке Windows. После изменения настроек для их применения необходимо завершение сеанса или перезагрузка.

5.6 Блокировка работы с файлами по расширению

В системе защиты Dallas Lock 8.0 реализована функция блокировки доступа к файлам по их расширению. Эта функция может быть полезна, к примеру, для того, чтобы запретить сотрудникам работу с файлами, не имеющими отношения к их профессиональным обязанностям (mp3, avi и т. д.).

Для того, чтобы добавить расширение, на которое распространяется запрет, необходимо:

1. Запустить оболочку администратора и на вкладке «Параметры безопасности» зайти в категорию «Блокируемые расширения» (рис. 135).

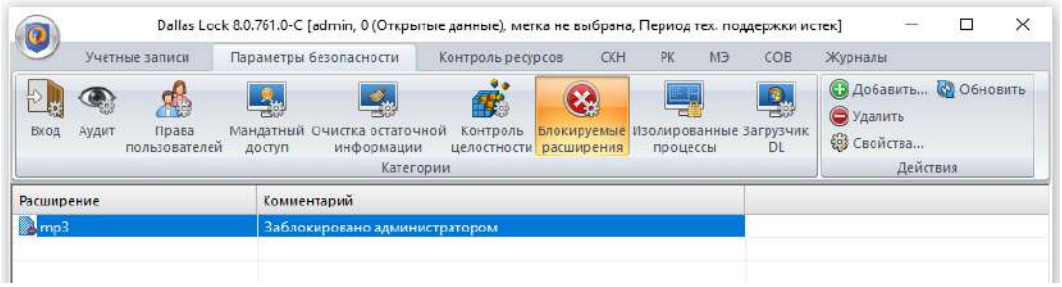


Рис. 135. Категория параметров безопасности Блокируемые расширения

   В окне программы появится поле со списком запрещенных расширений файлов (последовательности символов, добавляемых к имени файла и предназначенных для идентификации формата файла) и панель действий, содержащая инструменты по добавлению, удалению или редактированию свойств необходимых блокируемых администратором расширений.

2. Нажать кнопку «Добавить», в результате чего выведется окно «Заблокированные расширения файлов» (рис. 136).

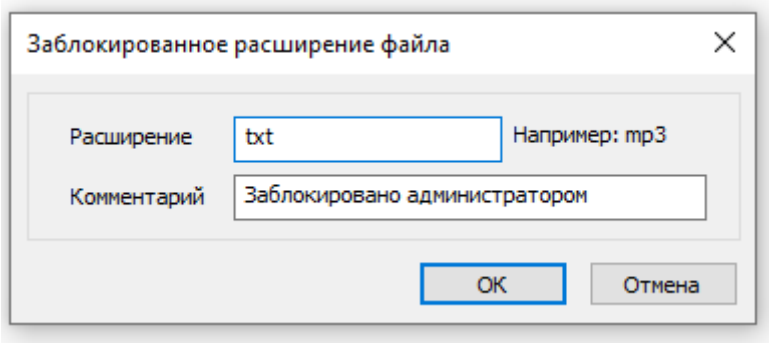


Рис. 136. Окно задания блокировки расширения

3. В данном окне нужно ввести необходимое расширение, комментарий к нему и нажать кнопку «OK». В разделе «Блокируемые расширения» добавится указанное расширение.

Функция «Блокируемые расширения» будет распространяться на всех пользователей кроме пользователя, выполнившего установку СЗИ, суперадминистратора. При попытке пользователя открыть файл с заблокированным расширением, появится соответствующее предупреждение.

Внимание! Следует учесть, что добавление в список блокируемых расширений, таких как exe, dll, sys, может привести к неработоспособности ОС (исключение составит работа под учетной записью суперадминистратора).

6 ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА

6.1 Изолированные процессы

Для исключения потенциального канала утечки конфиденциальной информации через программы-клиенты терминального доступа в СЗИ реализован механизм изолированных процессов.

Если процесс помечен как изолированный, то в этот процесс нельзя ничего скопировать через буфер обмена и из него нельзя ничего скопировать в другой процесс. Таким образом, механизм изолированных процессов позволяет исключить ситуацию, в которой злоумышленник использует терминальное подключение к какому-либо удаленному ПК и через буфер обмена копирует информацию.

Примечание. Для контроля уровня доступа данных, находящихся в буфере обмена, применяется мандатный принцип (только для Dallas Lock 8.0 редакции «С») разграничения доступа (см. «Мандатный доступ»).

Чтобы пометить процесс как изолированный, необходимо в основном меню оболочки администратора на вкладке «Параметры безопасности» выбрать категорию «Изолированные процессы» (рис. 137).

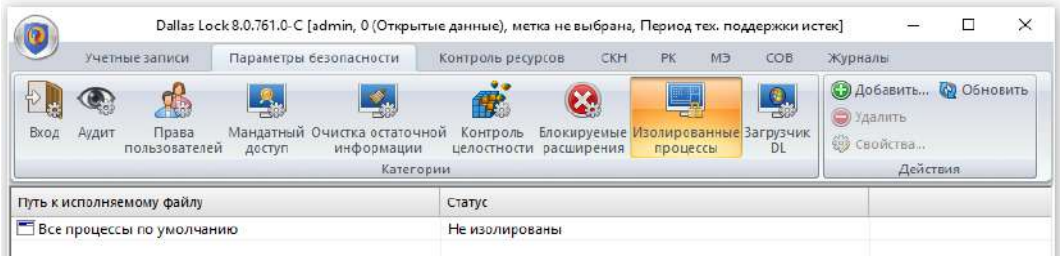


Рис. 137. Категория параметров безопасности Изолированные процессы

В окне программы появится поле со списком изолированных процессов и панель действий, содержащая инструменты по добавлению, удалению или редактированию пути к процессу, который необходимых изолировать.

В списке процессов первым всегда стоит глобальный параметр, определяющий политику для всех процессов на данном ПК — все процессы являются изолированными или не изолированными. Также данным списком через заданный полный путь к соответствующему исполняемому файлу определяются отдельные процессы.

Механизм настройки политики изолированных процессов следующий:

1. Устанавливается, что все процессы по умолчанию изолированы, и есть список не изолированных процессов.
2. Или устанавливается, что все процессы по умолчанию не изолированы, и есть список изолированных процессов.

По умолчанию активен режим, в котором все процессы не изолированы. Чтобы изменить его, необходимо кликнуть на параметр «Все процессы по умолчанию» и в окне изменения свойств отметить поле «Все процессы по умолчанию изолированы».

Чтобы добавить новый процесс в список, необходимо выбрать действие «Добавить». Появится проводник программы, с помощью которого необходимо выбрать исполняемый файл процесса и нажать «Выбрать», после чего он появится в списке изолированных/не изолированных (в зависимости от выбранной политики безопасности).

Также можно изолировать процесс, выбрав его в журнале процессов и нажав действие «Изолировать процесс» (рис. 138). Путь к исполняемому файлу данного процесса также появится в списке на вкладке «Параметры безопасности» → «Изолированные процессы».

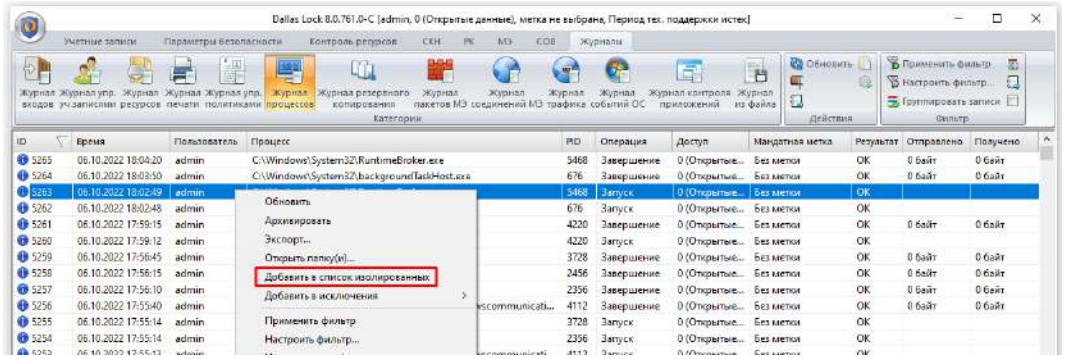


Рис. 138. Определение изолированного процесса через журнал процессов

После редактирования списка изолированных процессов новая конфигурация будет применена только для последующих сеансов работы пользователей.

Действия по изменению списка изолированных процессов фиксируются в журнале управления политиками.

6.2 Средства аудита

Важным средством обеспечения безопасности является механизм протоколирования. СЗИ должна фиксировать все события, касающиеся безопасности.

В процессе работы системы защиты Dallas Lock 8.0 события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журналах. Ведение журналов в свою очередь регулируется параметрами аудита, задаваемыми пользователями с правами на управление аудитом. Система защиты позволяет осуществлять гибкую настройку аудита и выбирать, какие действия пользователя по отношению к каким ресурсам необходимо регистрировать. Можно протоколировать все действия, касающиеся администрирования системы защиты.

Просмотр и редактирование параметров аудита возможны в категориях «Аудит» и «Права пользователей» на одной из основных вкладок «Параметры безопасности» оболочки администратора.

6.2.1 Параметры аудита

С помощью подсистемы аудита в СЗИ Dallas Lock 8.0 происходит регистрация событий и их группировка, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы.

Чтобы настроить параметры аудита, необходимо в основном меню оболочки администратора на вкладке «Параметры безопасности» выбрать категорию «Аудит». В списке имеются следующие параметры:

Таблица 4. Настраиваемые параметры безопасности подсистемы аудита

Журнал входов в систему
Включение журнала позволяет протоколировать в нем события, связанные с входом, выходом, разблокировкой пользователей на ПК, включая как локальные, так и сетевые, в том числе терминальные входы и выходы. Параметр может принимать значение «вкл» или «выкл».
Журнал ресурсов
Включение журнала позволяет протоколировать в нем события по доступу к ресурсам ФС, программно-аппаратной среды и к устройствам (при включенном параметре «Аудит устройств» см. ниже). А также события очистки остаточной информации (при включении «Аудит: событий зачистки»). Возможен аудит действий пользователей как с локальными ресурсами, так и с сетевыми. Сюда же заносятся события непосредственно по управлению доступом к ресурсам (в случае, когда на объект назначается любой дескриптор доступа, аудита, контроля целостности). Параметр может принимать значение «вкл» или «выкл».
Журнал управления политиками безопасности
Включение журнала позволяет протоколировать в нем действия по настройке параметров системы защиты и по изменению прав пользователей.

Параметр может принимать значение «вкл» или «выкл».
Журнал управления учетными записями
Включение журнала позволяет вести в нем учет действий по созданию, удалению, редактированию учетных записей пользователей. Параметр может принимать значение «вкл» или «выкл».
Журнал печати
Включение журнала позволяет протоколировать в нем события печати на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.). Параметр может принимать значение «вкл» или «выкл».
Журнал запуска/завершения процессов
Включение журнала позволяет протоколировать в нем события запусков/завершения процессов в ОС. Параметр может принимать значение «вкл» или «выкл».
Журнал резервного копирования
Включение журнала позволяет фиксировать в нем события по управлению заданиями резервного копирования, а также по запуску и завершению восстановления из резервных копий и удалению резервных копий.
Служебный журнал МЭ (заблокированные пакеты в формате Pcap)
Включение данного журнала необходимо для создания файла со списком заблокированных пакетов в формате pcap (в случае возможных проблем детектирования пакетов) и может понадобиться при обращении в службу технической поддержки. Параметр может принимать значение «вкл» или «выкл».
Журнал пакетов МЭ
Включение журнала позволяет фиксировать все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера. Параметр может принимать значение «вкл» или «выкл». Настройка правил осуществляется аналогично настройке правил МЭ (см. «Правила МЭ»).
Журнал соединений МЭ
Включение журнала позволяет фиксировать сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами. Параметр может принимать значение «вкл» или «выкл». Настройка правил осуществляется аналогично настройке правил МЭ (см. «Правила МЭ»).
Журнал трафика фильтрации МЭ
Включение журнала позволяет фиксировать проходящий сетевой трафик через контролируемые МЭ узлы сети.
Журнал событий ОС
Включение журнала позволяет фиксировать все важные события безопасности, генерируемые ОС и прикладным ПО.
Журнал трафика СОВ
Включение журнала позволяет фиксировать проходящий сетевой трафик через контролируемые СОВ узлы сети.
Журнал контроля приложений СОВ
Включение журнала позволяет фиксировать все события об активности приложений, их целостности и наборе загружаемых ими компонентов.
Фоновое выполнение резервного копирования
Влючение данного параметра (значение «Вкл.») позволяет понизить для задач резервного копирования приоритет выполнения потоков, обрабатывающих задачи резервного копирования.

Фиксировать в журнале входов неправильные пароли

Включение данного параметра позволяет фиксировать значения неверно введенных паролей в журнале входов (при условии, что журнал входов включен).

Параметр может принимать значение «да» или «нет».

Внимание! При значении параметра «да» возникает риск использования информации, содержащейся в столбце «Неверный пароль», для скрытой компрометации паролей пользователей. Ошибки пользователей при вводе пароля неминуемо приведут к раскрытию части пароля, что может значительно облегчить для злоумышленника задачу его подбора.

Заносить в журнал исходящие попытки входа на удаленные компьютеры

Включение данного параметра позволяет регистрировать события исходящей попытки входа пользователя на удаленный компьютер через ЛВС в журнале входов (при условии, что журнал входов включен).

Параметр может принимать значение «вкл» или «выкл».

Заносить в журнал события запуска и остановки ОС

Включение данного параметра позволяет регистрировать события, связанные с запуском/завершением работы ОС, события запуска/остановки ядра защиты СЗИ, в журнале управления политиками (при условии, что данный журнал включен).

Заносить в журнал события запуска и остановки модулей администрирования DL

Включение данного параметра позволяет регистрировать события, связанные с запуском/завершением работы модулей администрирования СЗИ (Dallas Lock, СБ, КСБ, МСБ) в журнале управления политиками (при условии, что данный журнал включен). Параметр может принимать значение «да» или «нет».

Аудит устройств

Включение данного параметра позволяет регистрировать события по доступу к подключаемым на данный ПК устройствам в Журнале ресурсов (при условии, что журнал ресурсов включен). Сами события настраиваются непосредственно в окне редактирования параметров дескриптора устройства (класса устройств).

Аудит USB-накопителей: Заносить в журнал попытки подключения/отключения

Включение данного параметра позволяет регистрировать попытки подключения определенных USB-устройств на данном ПК в Журнале ресурсов согласно выбранному значению:

- Незарегистрированных USB-накопителей.
- Зарегистрированных USB-накопителей.
- Всех USB-накопителей.

Для разрешения редактирования настроек политики необходимо включить параметр «Блокировать подключение незарегистрированных накопителей USB-Flash»

Аудит событий зачистки

Включение данного параметра позволяет регистрировать события зачистки остаточной информации в следующих случаях:

- при включенных параметрах зачистки (см. «Параметры очистки остаточной информации»);
- при зачистке по запросу пользователя (пункт контекстного меню «Удалить и зачистить», см. «Удаление файлов и зачистка остаточной информации по команде»);
- при зачистке накопителя (функция «Зачистка диска»).

Аудит доступа: Заносить в журналы ошибки ОС

Включение данного параметра позволяет вести учет ошибок доступа ОС Windows в журнале ресурсов (при условии, что журнал ресурсов включен). Так как Dallas Lock 8.0 не подменяет механизмы контроля доступа к ресурсам ОС, а добавляет свои, то любое действие над ФС вначале попадает для проверки в драйвер защиты СЗИ, и, если этот драйвер разрешает данное действие, оно передается дальше ОС. ОС может отказать уже по своим причинам —

эти отказы и протоколируются. В большинстве случаев аудит этих ошибок не требуется.
Аудит доступа/запуска: Вести аудит системных пользователей
Включение данного параметра позволяет вести учет действий системных пользователей (SYSTEM, LOCAL SERVICE, NETWORK SERVICE и пр.) в журнале ресурсов (при условии, что журнал ресурсов включен). В большинстве случаев, аудит этих пользователей не требуется.
Печать/редактировать штамп
Включение и настройка параметров данной политики аудита позволяет на распечатываемых документах добавлять штамп (см. «Добавление штампа на распечатываемые документы»).
Создавать теневые копии распечатываемых документов
Включение данного параметра (значение «да») позволяет сохранять копии распечатываемых документов в отдельной папке по пути: «C:\DLLOCK80\Logs\PrintCopy». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства (см. «Теневые копии распечатываемых документов»).
Разрешить печать из-под уровней доступа
Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа, работая под которыми, пользователи могут осуществлять печать документов (только для Dallas Lock 8.0 редакции «С»).
Добавлять штамп при печати под уровнями
Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа пользователей, при работе под которыми на распечатываемые документы будет добавляться штамп, который настроен параметром «Добавлять штамп» (только для Dallas Lock 8.0 редакции «С»).
Выгрузка журналов
Настройка данного параметра в дополнительном окне позволяет: • экспортировать журналы Dallas Lock 8.0 в журнал событий Windows; • экспортировать журналы Dallas Lock 8.0 в SIEM систему с возможностью выбора из выпадающих списков формата выгрузки (Syslog, CEF или LEEF) и кодировки выгрузки (UTF-8 или CP1251). Для обоих типов экспорта возможно задать список экспортируемых журналов и определить период выгрузки журналов в диапазоне от 10 сек. до 24 часов.
Максимальное кол-во записей в журналах
Настройка данного параметра позволяет установить максимальное количество записей в определенном журнале. Параметр может принимать значение «Не используется» или «100–20000».
Периодическая архивация журналов
Включение данного параметра позволяет управлять периодами автоматической архивации журналов. После настройки данного параметра, все журналы по расписанию архивируются, все записи из них сохраняются в файл в системной папке «C:\DLLOCK80\Logs», записи журналов очищаются, и они начинают вестись заново. По умолчанию параметру задано значение «Не используется». Границы возможного временного интервала архивации варьируются от 1 часа до 1 года.

Для настройки аудита доступа к ресурсам недостаточно просто установить этому параметру значение «Включен» в окне редактирования параметров безопасности. Необходимо указать, какие именно операции по доступу, к каким именно ресурсам должны быть запротоколированы.

Примечание. Аудит доступа к ресурсам нужно настраивать очень внимательно, так как в системе постоянно происходит множество событий, связанных с доступом к ресурсам ФС. К примеру, в процессе загрузки ОС происходит несколько тысяч таких событий. Если назначить аудит всех событий ФС, то журналы будут переполняться очень быстро, и в полученных журналах будет крайне сложно разобраться, а также будет иметь место замедление работы ПК. Поэтому рекомендуется назначать аудит только для необходимых ресурсов и событий.

6.2.2 Полномочия на просмотр и управление параметрами аудита

Предоставить пользователю право на просмотр или управление параметрами аудита можно с помощью настройки параметров на вкладке «Параметры безопасности» → «Права пользователей» (рис. 139).

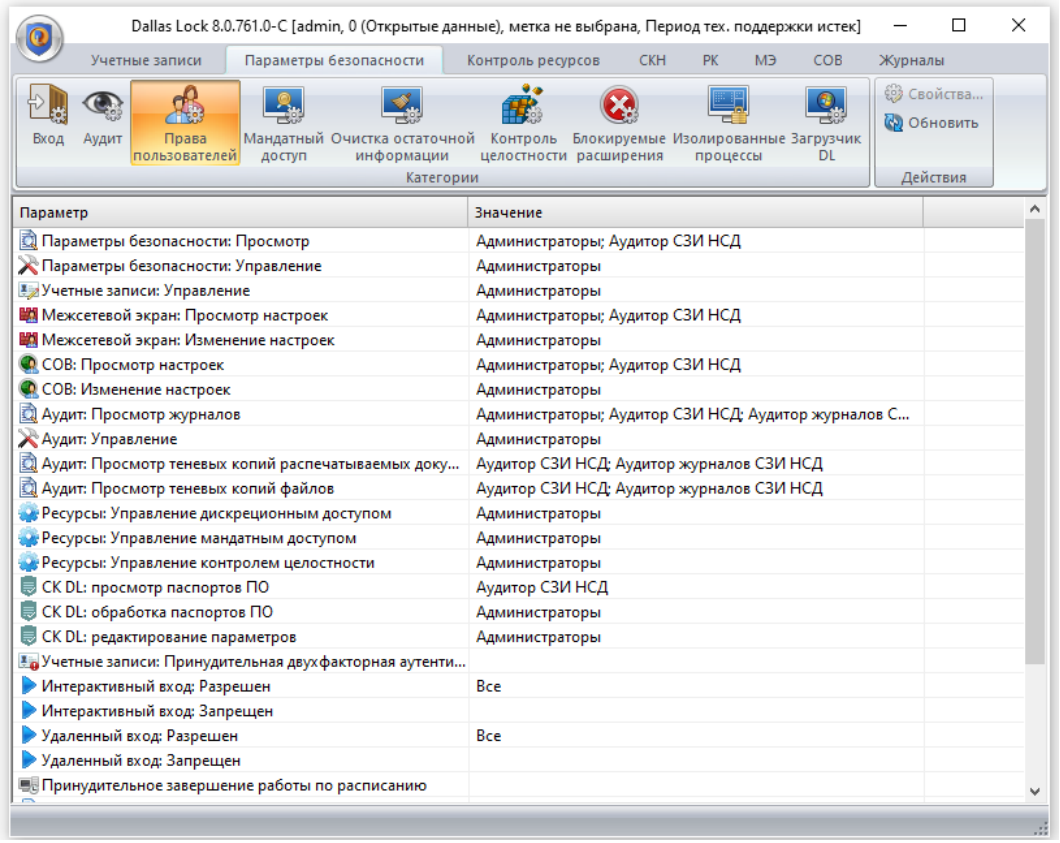


Рис. 139. Редактирование прав пользователей

Каждому пользователю, зарегистрированному в СЗИ, могут быть предоставлены следующие права аудита:

Таблица 5. Права пользователей на аудит

Право	Параметр безопасности («Параметры безопасности» → «Права пользователей»)
Право на просмотр теневых копий распечатываемых документов (копии создаются при условии, что включен параметр аудита «Создавать теневые копии распечатываемых документов», см. «Теневое копирование»)	«Аудит: просмотр теневых копий распечатываемых документов»
Право на просмотр теневых копий файлов (см. «Теневое копирование»)	«Аудит: Просмотр теневых копий файлов»
Право на просмотр только журналов в оболочке администратора СЗИ	«Аудит: Просмотр журналов»
Право на управление аудитом (назначение и редактирование назначенных параметров)	«Аудит: Управление»
Право на просмотр установленных параметров аудита (в том числе журналов)	«Параметры безопасности: Просмотр»

Для того, чтобы назначить право аудита пользователю, необходимо включить пользователя, учетную запись или группу пользователей в список для выбранного параметра. Для этого нужно выбрать параметр, нажать кнопку «Свойства» и добавить пользователей (или группы), воспользовавшись диалоговыми окнами СЗИ (рис. 140).

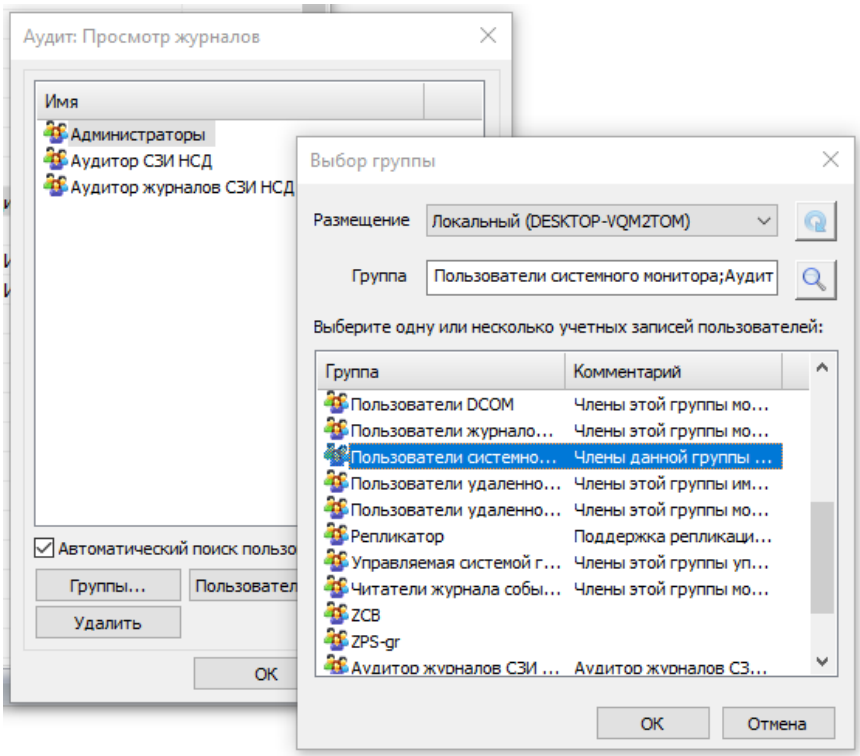


Рис. 140. Выбор пользователей для назначения просмотра параметров аудита

Для объектов у пользователей, не входящих в соответствующий список, нет возможности назначить аудит событий. При попытке просмотра назначенных параметров аудита пользователями, не входящими в список, установленный параметром для просмотра, выведется предупреждающее сообщение. Также будут заблокированы попытки просмотра теневых копий распечатываемых документов и теневых копий документов при копировании их на съемные и сетевые накопители.

В Dallas Lock 8.0 по умолчанию реализовано создание двух групп пользователей с предустановленными правами аудита: группа «Аудитор СЗИ» и группа «Аудитор журналов СЗИ». Члены этих групп автоматически получают права либо на просмотр установленных параметров аудита, в том числе журналов («Аудитор СЗИ»), либо на просмотр только журналов СЗИ («Аудитор журналов СЗИ»).

6.3 Аудит доступа

Аудит доступа к ресурсам в системе защиты настраивается как для глобальных, так и для локальных объектов.

Аудит событий настраивается по принципу назначения дескриптора аудита для объекта. Для этого в дескрипторе объекта имеется закладка «Аудит доступа» со списком операций, которые могут быть запротоколированы в системе защиты.

Примечание. Следует обратить внимание на то, что параметры настройки аудита не наследуются, а заменяются. То есть если, например, для папки «C:\Documents» назначить аудит успешного чтения, а в параметрах безопасности папки «C:\Documents\Secret» установить только аудит успехов записи, то для объектов из папки «C:\Documents\Secret» будет вестись аудит только успешной записи. Аудита успехов чтения для папки «C:\Documents\Secret» вестись не будет. Так как параметры аудита папки «C:\Documents\Secret» полностью перекрывают параметры аудита папки «C:\Documents». Благодаря такой особенности можно, например, снимать аудит с определенных объектов, находящихся в папке, для которой ведется аудит. Для этого достаточно у этого объекта в параметрах аудита выставить флаг «Аудит включен» и не ставить ни одного флага, отвечающего за события.

6.3.1 Аудит глобальных параметров

Список глобальные параметры ФС расположен на вкладке «Контроль ресурсов» → «Глобальные» оболочки администратора Dallas Lock 8.0.

Глобально параметры аудита можно задать:

Таблица 6. Глобальные дескрипторы

Назначение	Название параметра в Dallas Lock 8.0
на все ресурсы ФС	«Параметры ФС по умолчанию»
на жесткие диски, в том числе на устройства типа внешний жесткий диск USB	«Параметры фиксированных дисков по умолчанию»
на все сетевые ресурсы	«Параметры сети по умолчанию»
на файл-диски, которые были преобразованы	«Параметры преобразованных файл-дисков по умолчанию»
на все типы сменных накопителей, которые не были преобразованы, кроме CD-ROM дисков (по умолчанию)	«Параметры открытых сменных накопителей по умолчанию»
на все приводы компакт-дисков на данном компьютере	«Параметры CD-ROM дисков по умолчанию»
на все сменные USB-Flash накопители, которые не были преобразованы (по умолчанию)	«Параметры открытых USB-Flash накопителей по умолчанию»
на все Floppy-диски на данном компьютере, которые не были преобразованы (по умолчанию)	«Параметры открытых FDD-дисков по умолчанию»
на все типы сменных накопителей, которые были преобразованы	«Параметры преобразованных сменных накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все сменные USB-Flash накопители, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных USB-Flash накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все Floppy-диски на данном компьютере, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных FDD-дисков по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
для всего реестра	«Параметры реестра по умолчанию»
для всех аппаратных идентификаторов	«Параметры аппаратных ключей по умолчанию»

Чтобы назначить события аудита для параметра, необходимо:

1. Выделить глобальный параметр и нажать «Свойства». Откроется окно редактирования параметров — дескриптор объекта. Необходимо выбрать вкладку «Аудит доступа» (рис. 141).

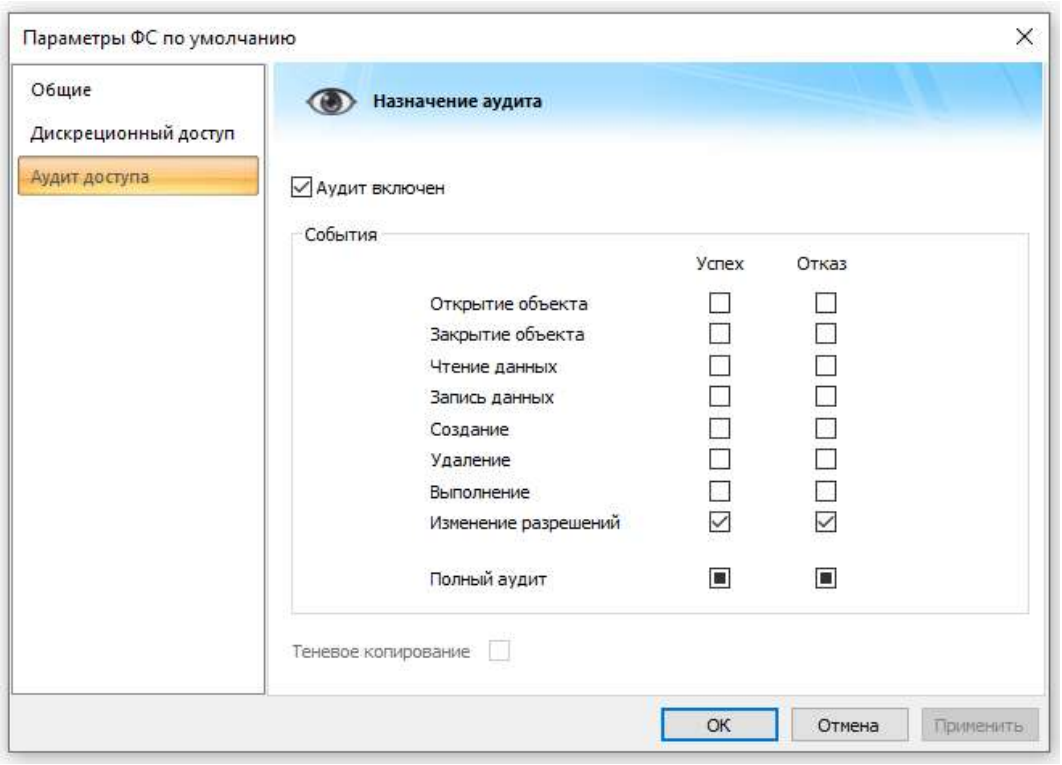


Рис. 141. Окно назначения аудита на ресурс ФС

3. Перед выбором событий необходимо включить аудит: отметить флагом поле «Аудит включен».
4. В зависимости от того, успешное или неудачное событие нужно зарегистрировать, выставить флаг в полях «Успех» или «Отказ» для операции.

   Отмеченные события будут заноситься в журнал ресурсов. Если одновременно отметить и «Успех», и «Отказ», то в журнал, соответственно, будут заноситься и успешные события, и неуспешные.

   Отмеченное флагом поле «Полный аудит» позволяет автоматически расставить значения успеха или отказа во всех полях и вести аудит по всем позициям.

6.3.2 Аудит локальных объектов ФС и веток реестра

Чтобы установить событие аудита для конкретного объекта ФС или ветки реестра, необходимо выполнить следующие действия:

1. Открыть дескриптор безопасности объекта, используя оболочку администратора Dallas Lock 8.0 («Контроль ресурсов» → «Все», выбрать фильтр по типу контроля «Аудит» и нажать кнопку «Добавить (Глобальные)», «Добавить (ФС)» или «Добавить (Реестр)», или через контекстное меню объекта (пункт «Права доступа» для объекта ФС) (рис. 142).

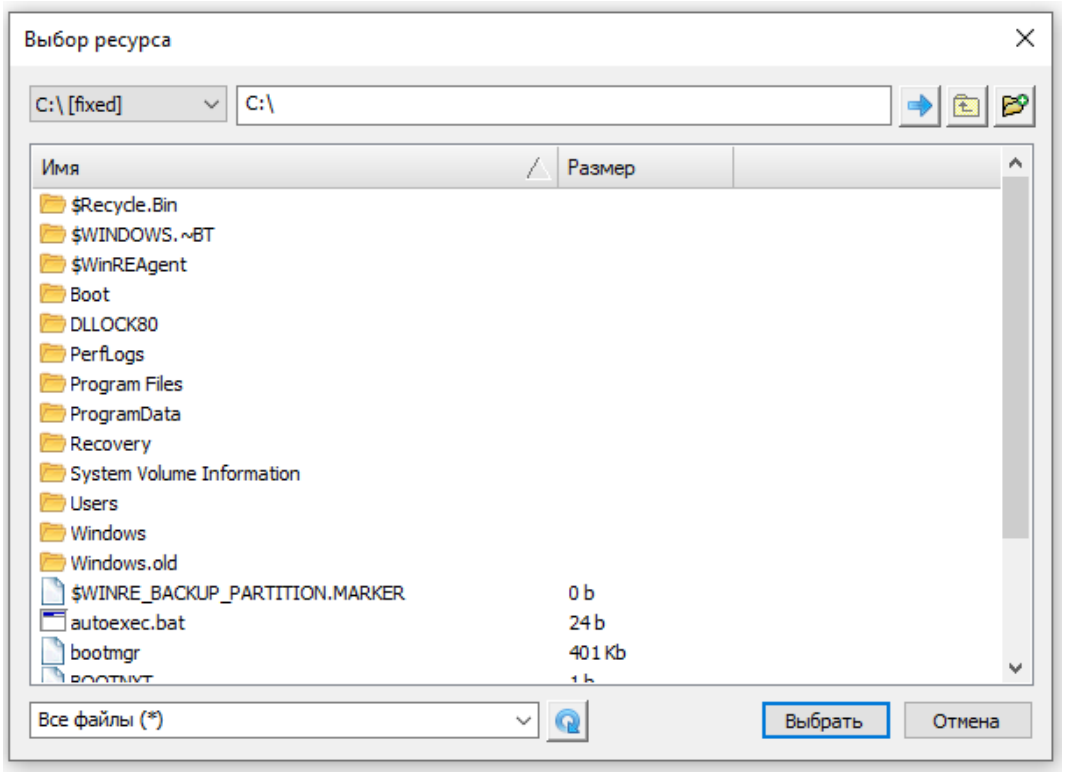


Рис. 142. Выбор ресурса для назначения аудита

5. В дескрипторе объекта открыть закладку «Аудит доступа».
6. Включить аудит (отметить флагом поле «Аудит включен»), и отметить события «Успех» или «Отказ» по выбранным операциям.

Объекты, для которых назначен аудит любым из способов, автоматически появляются в списке объектов выбранного фильтра по типу контроля «Аудит» на вкладке «Контроль ресурсов».

6.4 Журналы

В системе защиты Dallas Lock 8.0 регистрация и запись событий ведется в различных типах журналов. Для удобства выделены 12 основных журналов.

1. Журнал входов.
2. Журнал управления учетными записями.
3. Журнал ресурсов.
4. Журнал печати.
5. Журнал управления политиками.
6. Журнал процессов.
7. Журнал резервного копирования.
8. Журнал пакетов МЭ.
9. Журнал соединений МЭ.
10. Журнал событий ОС.
11. Журнал трафика.
12. Журнал контроля приложений.

Для просмотра содержимого определенного журнала необходимо в оболочке администратора на вкладке основного меню «Журналы» выбрать категорию, соответствующую одному из 12 типов журналов (рис. 143).

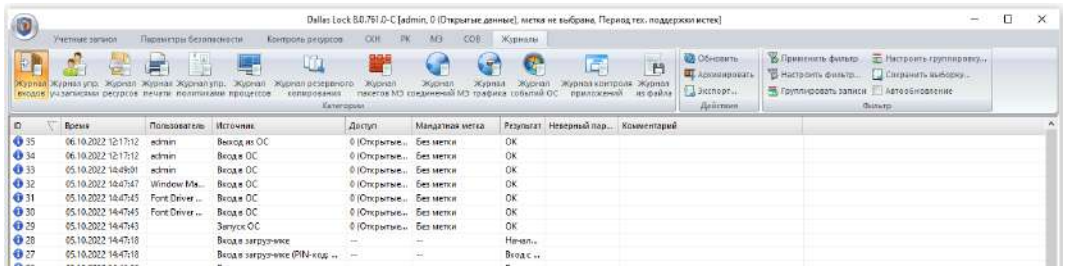


Рис. 143. Вкладка Журналы

В каждом журнале фиксируются дата, время, имя пользователя, операция, результат и прочие параметры. Возможно упорядочивание элементов списков журнала по необходимому значению, для этого нужно кликнуть на кнопку с названием столбца журнала.

Двойной щелчок мыши на любой записи любого журнала открывает окно, содержащее всю информацию, относящуюся к этой записи (рис. 144).

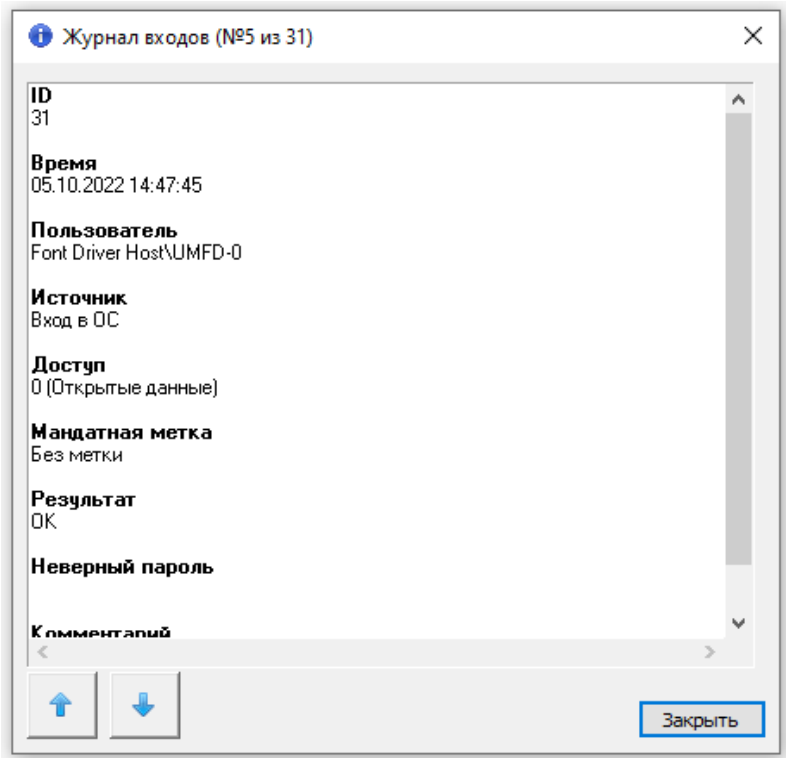


Рис. 144. Отдельная форма записи журнала событий

Нажимая на кнопки «вверх» и «вниз», можно листать журнал, просматривая предыдущие или следующие записи.

Панель кнопок «Действия», общая для всех журналов, позволяет произвести над открытым журналом действия по обновлению журнала (кнопка «Обновить»), по архивации всего журнала (кнопка «Архивировать»), по экспорту всего журнала или отфильтрованных записей в файл (кнопка «Экспорт»), по автоматическому обновлению журнала раз в 5 секунд (кнопка «Автообновление»). Также эти действия возможно выбрать из контекстного меню.

Примечание. С помощью клавиши «Delete» можно очистить любой журнал. Для этого выполнить следующее:

1. Выделить выбранный журнал и нажать клавишу «Delete».
2. Перед очисткой журнала пользователю задается вопрос о необходимости архивирования записей (Рис. 145).

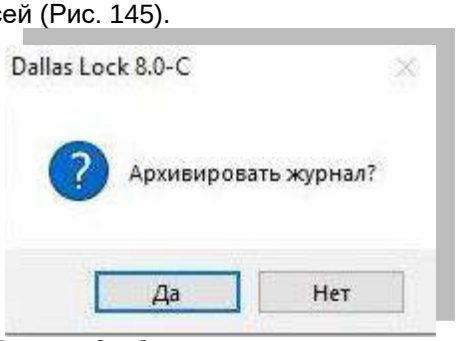


Рис. 145. Сообщение о архивировании журнала

3. При положительном ответе происходит архивирование и очистка журнала, при отрицательном обе операции будут отменены.

После выбора архивации журнала его записи сохраняются в файл в системной папке «C:\DLLOCK80\Logs», в окне журнала записи очищаются, и он начинает вестись заново. В том случае, когда журнал переполняется (максимальный размер — 20000 записей), он архивируется в файл со специальным расширением *.lg8 и помещается в папку «C:\DLLOCK80\Logs». При этом текущий журнал в оболочке администратора очищается и начинает вестись заново. В имени архивного файла с журналом записаны его тип, дата и время создания файла.

Каждый текущий журнал формируется в папке «C:\DLLOCK80\Jrn» и имеет фиксированный максимальный размер — 20000 записей.

Если необходимо удалить журнал окончательно, нужно зайти в папку «C:\DLLOCK80\Logs» и удалить соответствующий файл.

Категория «Журнал из файла» на вкладке «Журналы» позволяет открыть журнал из сохраненного файла, отфильтровать его значения и экспортировать в файл. Это могут быть журналы от Dallas Lock 7.7 или Dallas Lock 8.0 предыдущих сборок.

Журналы в СЗИ Dallas Lock 8.0 имеют следующую структуру:

Журнал входов

В данном журнале фиксируются все входы (или попытки входов с указанием причины отказа) и выходы пользователей ПК, включая как локальные, так и сетевые, в том числе, терминальные входы и события разблокировки, а также события входа при активном модуле загрузчика DL (Включение ПК, вход с PIN-кодом, начало загрузки ОС). Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Пользователь» фиксируется имя пользователя;
- в графе «Источник» фиксируется тип события: загрузка ПК, вход в ОС, выход из ОС;
- в графе «Доступ» указывается мандатный уровень, под которым осуществлен вход (только для Dallas Lock 8.0 редакции «С»);
- в графе «Мандатная метка» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);
- в графе «Результат» фиксируется успех или отказ в доступе и причина отказа;
- в графе «Неверный пароль» фиксируются неверно введенные пароли при попытке загрузки ПК или входе в ОС;
- в графе «Комментарий» отображается дополнительная информация.

Примечание. При сетевом входе в графе «источник» к типу события добавляется имя компьютера, с которого произведен вход, и его IP-адрес.

Журнал управления учетными записями

В данном журнале ведется учет всех действий по созданию, удалению или изменению прав пользователей и события смены пароля учетной записи. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время действий, производимых над правами пользователей;
- в графе «Пользователь» фиксируется имя пользователя, осуществившего вышеперечисленные операции администрирования;
- в графе «Компьютер» фиксируется имя компьютера, с которого производилось администрирование;
- в графе «Имя» фиксируется имя пользователя, изменение прав которого было произведено;
- в графе «Результат» отображается результат выполнения операции («OK» — операция выполнена удачно или «доступ запрещен»);
- в графе «Комментарий» отображается дополнительная информация;
- в графе «Операция» отображается наименование произведенной операции (создать пользователя, удалить пользователя, сменить пароль, изменить параметры и др.).

Журнал ресурсов

Данный журнал позволяет проследить обращения к объектам ФС, реестру и устройствам, для которых назначен аудит, а также события по настройке дескрипторов объектов ФС и устройств. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Пользователь» фиксируется имя пользователя, осуществившего действие;
- в графе «Компьютер» фиксируется имя компьютера, с которого осуществлялся доступ;
- в графе «Объект доступа» фиксируется путь к ресурсу или имя устройства;
- в графе «Результат» фиксируется успех или отказ в доступе и причина отказа;
- в графе «Операция» фиксируются все действия, которые производились с объектом;

- в графе «Доступ» указывается мандатный уровень, под которым осуществлен доступ к ресурсу (только для Dallas Lock 8.0 редакции «С»);
- в графе «Мандатная метка» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);
- в графе «Права» фиксируются права, с которыми был осуществлен доступ к ресурсу ФС и ветке реестра:

Для папок и веток реестра			Для файлов и ключей параметров реестра		
MAX	—	открытие на полный доступ	MAX	—	открытие на полный доступ
D	—	удаление папки	R	—	открытие на чтение
L	—	получить содержимое папки	W	—	открытие на запись
AF	—	добавление файла в папку	A	—	открытие на добавление данных в конец файла
AD	—	добавление подпапки	D	—	открытие с последующим удаление файла.
DF	—	удаление файла из папки	E	—	выполнение файла
RA	—	чтение атрибутов папки	RA	—	чтение атрибутов файла
WA	—	запись атрибутов папки	WA	—	запись атрибутов файла

- в графе «Процесс» фиксируется программа, из которой производилась операция по доступу;
- в графе «Комментарий» отображается дополнительная информация.

Журнал печати

В данный журнал заносятся все события, связанные с распечаткой документов на локальных или удаленных принтерах. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время начала печати;
- в графе «Пользователь» фиксируется имя пользователя, запустившего процесс печати;
- в графе «Принтер» фиксируется имя принтера, на котором производилась печать;
- в графе «Порт» фиксируется название порта, к которому подключено устройство;
- в графе «Документ» фиксируется название документа и программа, из которой производилась печать;
- в графе «Результат» фиксируется успех или отказ в печати;
- в графе «Страниц» фиксируется количество распечатанных страниц документа;
- в графе «Копий» отображается количество копий;
- в графе «Процесс» фиксируется процесс, который запущен программой печати;
- в графе «Доступ» фиксируется уровень мандатного доступа, под которым работает пользователь, производящий печать;
- в графе «Мандатная метка» — указывается назначенный уровень мандатного доступа для документа, отправленного на печать.

Записи в журнал печати заносятся при условии включенного аудита печати (вкладка «Параметры безопасности» → «Аудит»). Процесс печати сопровождается двумя записями: начала и окончания печати.

Журнал управления политиками

Данный журнал дает возможность просмотреть все действия, изменяющие настройку параметров системы защиты и прав пользователей. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Пользователь» фиксируется имя пользователя, производящего изменения;
- в графе «Компьютер» фиксируется имя компьютера;
- в графе «Параметр» фиксируется название процесса по настройке параметров;
- в графе «Комментарий» отображается дополнительная информация;
- в графе «Результат» фиксируется результат редактирования.

Журнал процессов

В данный журнал заносятся события запуска и завершения процессов. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Пользователь» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Процесс» фиксируется путь к файлу процесса и его имя;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «Операция» фиксируется тип события — запуск или завершение;
- в графе «Доступ» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «Мандатная метка» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат;
- в графе «Отправлено» фиксируется количество отправленных байт;
- в графе «Получено» фиксируется количество принятых байт.

Журнал резервного копирования

В данный журнал заносятся события, связанные с резервным копированием. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Операция» отображается наименование произведенной операции;
- в графе «Имя» отображается наименование задания;
- в графе «Пользователь» указывается пользователь, который принудительно запустил задание. Если задание запущено по расписанию — в поле указывается «Служба РК»;
- в графе «Результат» фиксируется успешность операции;
- в графе «Комментарий» отображается дополнительная информация.

Журнал пакетов МЭ

В данный журнал заносятся события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Локальный адрес» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Локальный порт» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Внешний адрес» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Внешнее имя» фиксируется NETBIOS- или DNS-имя внешнего респондента при наличии такой информации в отправленных или принятых данных (принудительный запрос этой информации не производится);
- в графе «Внешний порт» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Направление» фиксируется направление передачи данных (прием или отправка);
- в графе «Протокол» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «Информация» фиксируется вся техническая информация, найденная и проанализированная в отправленном или принятом пакете данных;
- в графе «Пользователь» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Доступ» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «Процесс» фиксируется путь к файлу процесса и его имя;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «Длина» фиксируется отправленного или принятого пакета данных;
- в графе «Правило» фиксируется правило, которое было применено;
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат.

Журнал соединений МЭ

В данный журнал заносятся сведения об истории сетевых соединений, устанавливаемых

процессами (приложениями) в соответствии с заданными правилами. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Локальный адрес» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Локальный порт» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Внешний адрес» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Внешнее имя» фиксируется NETBIOS- или DNS-имя внешнего респондента при наличии такой информации в отправленных или принятых данных (принудительный запрос этой информации не производится);
- в графе «Внешний порт» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «IP версия» фиксируется версия используемого протокола IP;
- в графе «Протокол» фиксируется протокол отправленного или принятого пакета данных;
- в графе «Пользователь» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Доступ» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «Процесс» фиксируется путь к файлу процесса и его имя;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «Событие» фиксируется наименование события соединения;
- в графе «Отправлено» фиксируется количество отправленных байт;
- в графе «Получено» фиксируется количество принятых байт;
- в графе «Правило» фиксируется правило, которое было применено;
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат.

Журнал трафика

В данном журнале фиксируется проходящий сетевой трафик через контролируемые узлы сети. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат;
- в графе «Тип атаки» фиксируется тип атаки события;
- в графе «Адрес источника» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Порт источника» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Внешнее имя» фиксируется имя компьютера, от которого запущена атака;
- в графе «Адрес назначения» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Порт назначения» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «Протокол» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «Пользователь» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Процесс» фиксируется путь к файлу процесса и его имя;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «Комментарий» отображается дополнительная информация;
- в графе «Сообщение» фиксируется описание атаки;
- в графе «ID сигнатуры» фиксируется уникальный идентификатор сигнатуры.

Журнал событий ОС

В данном журнале фиксируются важные события безопасности, генерируемые ОС. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Уровень тревоги» фиксируется уровень важности события;

- в графе «Тип события» фиксируется тип события;
- в графе «Источник события» фиксируется процесс, зарегистрировавший событие в журнале;
- в графе «Код события» фиксируется число, определяющее конкретный тип события;
- в графе «Протокол» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «Пользователь» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Категория» фиксируется категория события;
- в графе «Процесс» фиксируется программа, из которой производилась операция;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «ID сигнатуры» фиксируется уникальный идентификатор сигнатуры;
- в графе «Сигнатура» фиксируется информация о сигнатуре;
- в графе «Текст события» фиксируется описание события;
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат.

Журнал контроля приложений

В данном журнале фиксируются события об активности приложений, их целостности и набора загружаемых ими компонентов. Журнал содержит следующие элементы списков:

- в графе «Время» фиксируется дата и время события;
- в графе «Тип атаки» фиксируется описание атаки;
- в графе «Подробнее» фиксируется сообщение, присвоенное правилу.
- в графе «Процесс» фиксируется путь к файлу процесса и его имя;
- в графе «PID» фиксируется уникальный идентификатор процесса;
- в графе «Пользовател» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «Правило» фиксируется правило, которое было применено;
- в графе «Результат» фиксируется успешный (OK) или неуспешный («Доступ запрещен!») результат;
- в графе «Комментарий» фиксируется дополнительная информация.

6.4.1 Фильтры журналов

Панель кнопок «Фильтр», общая для всех журналов, используется для задания параметров отбора событий, отображаемых в текущем или экспортированном журнале.

Использование фильтров дает возможность отсеять ненужные данные в журнале так, что они становятся невидимы при просмотре. В то же время информация при использовании фильтров из журналов не удаляется.

Чтобы произвести настройки, необходимо нажать кнопку «Настроить фильтр» и выбрать необходимые параметры фильтра в открывшемся окне, нажать «OK» (рис. 146). После настройки необходимо нажать кнопку «Применить фильтр», после чего записи журнала будут отсортированы. Повторное нажатие «Применить фильтр» вернет полное содержание журнала.

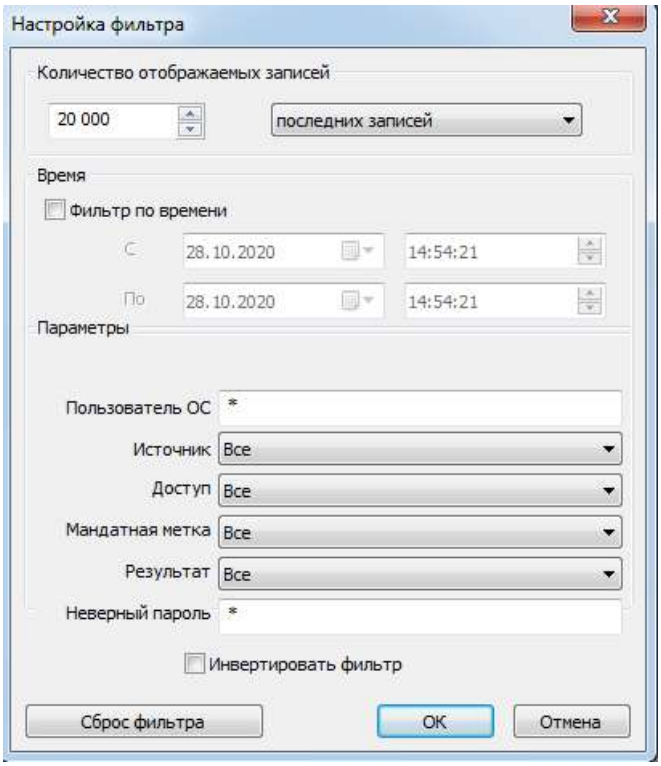


Рис. 146. Окно настройки фильтра журнала входов

Фильтр можно настроить по параметрам и(или) по времени. Для включения временного периода в фильтр необходимо отметить флагом поле «Фильтр по времени».

Каждый фильтр имеет параметры настройки, которые соответствуют основным элементам списков выбранного журнала. Например, журнал входов можно отфильтровать по времени, в которое была осуществлена попытка входа на ПК, по логину пользователя, по результату процесса (удачный/не удачный), по источнику процесса (удаленный вход, терминальный вход, смена пароля и т. д.).

Отфильтрованные записи журнала можно сохранить, воспользовавшись кнопкой «Экспорт», в выбранную папку в выбранном типе файла (TXT, CSV, HTML, XML). Экспортированные журналы служат для того, чтобы администратор мог рассмотреть записи в более удобном виде.

6.4.2 Группировка записей журнала

Для удобства просмотра записей в системе реализована группировка записей.

При включении действия «Группировать записи» полностью совпадающие записи (за исключением времени) группируются в одну запись. Если время самой ранней из них отличается от времени самой поздней, в колонке «Время» параметров журнала указывается диапазон. В этой же колонке в скобках указывается количество сгруппированных записей.

В отдельном окне характеристик такой записи в названии окна указывается, сколько записей объединено, перечисляются моменты времени с пометкой, какие записи выведены в журнал и другие общие параметры.

6.5 Теневое копирование

Функция теневого копирования обеспечивает копирование информации, которую пользователь записывает на сменные или сетевые накопители, в специальную папку на локальном жестком диске для последующего анализа.

Просмотр копий, созданных при теневом копировании, доступен для пользователей, наделенных данными полномочиями: «Аудит: Просмотр журналов» и «Аудит: Просмотр теневых копий файлов» на вкладке «Параметры безопасности» → «Права пользователей».

Режим теневого копирования информации доступен для следующего типа сменных и сетевых накопителей:

- магнитные гибкие диски (FDD);
- оптические диски (CD, DVD);
- USB-Flash накопители и сменные дисковые накопители;
- сетевые диски и накопители;

- карты памяти (SD, MicroSD, MMC).

Чтобы задать теневое копирование, необходимо в дескрипторе объекта (класса объектов) перейти на закладку «Аудит», отметить флагом Включение аудита и поле «Теневое копирование» (Рис. 147).

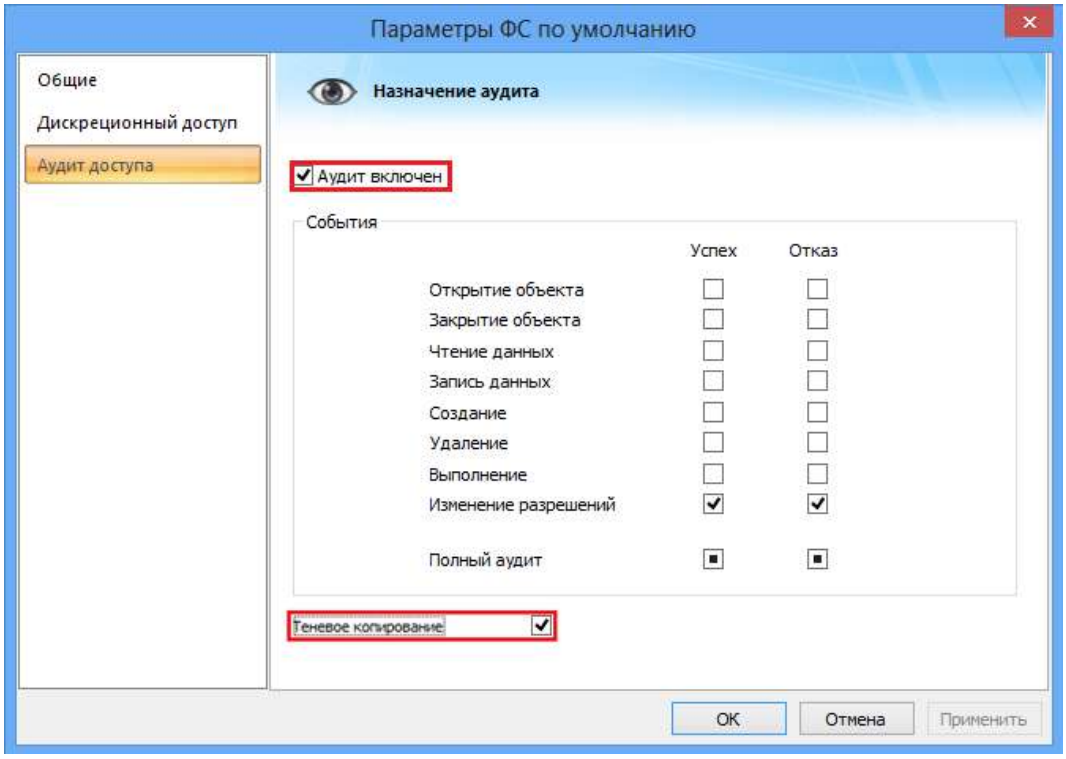


Рис. 147. Установка теневого копирования для директории

Теневое копирование можно задать для классов накопителей и для конкретных экземпляров подключаемых накопителей:

- задать теневое копирование глобально и для определенного класса можно через оболочку администратора, выбрав необходимый параметр на вкладке «Контроль ресурсов» → «Глобальные»;
- задать теневое копирование для отдельно взятого накопителя можно, выбрав его в проводнике Windows, и с помощью пункта контекстного меню «Права доступа 8.0» открыть закладку аудита доступа или через оболочку администратора, добавив объект в список на вкладке «Контроль ресурсов» → «Аудит».

В момент копирования информации на накопитель с включенным режимом теневого копирования копии файлов помещаются в специальную защищенную папку.

Просмотр теневых копий доступен через запись о теневом копировании в журнале ресурсов: в отдельном окне записи размещена кнопка, открывающая системную папку с теневыми копиями файлов (рис. 148).

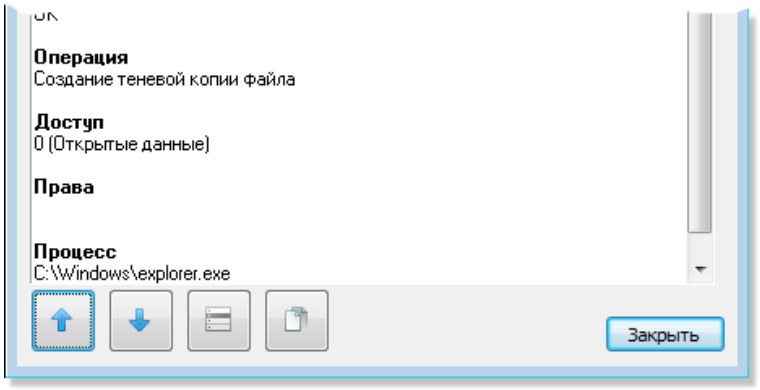


Рис. 148. Возможность просмотра теневой копии

Примечание. Если теневое копирование было выполнено под определенным мандатным уровнем доступа, то просмотреть созданную теневую копию возможно только под таким же уровнем доступа или выше. Так же должны совпадать неиерархические мандатные метки.

7 ПОДСИСТЕМА ПЕЧАТИ

7.1 Разграничение доступа к печати

Для того, чтобы выполнить настройку разрешения или запрета печати с ПК, защищенного Dallas Lock 8.0, необходимо в оболочке администратора открыть вкладку «Параметры безопасности» → «Права пользователей».

С помощью параметров «Печать разрешена» и «Печать запрещена» можно гибко настроить список учетных записей, которым разрешена или запрещена печать с данного компьютера. Добавить разрешенные или запрещенные учетные записи в список значений можно, выбрав параметр и нажав кнопку «Свойства» (рис. 149).

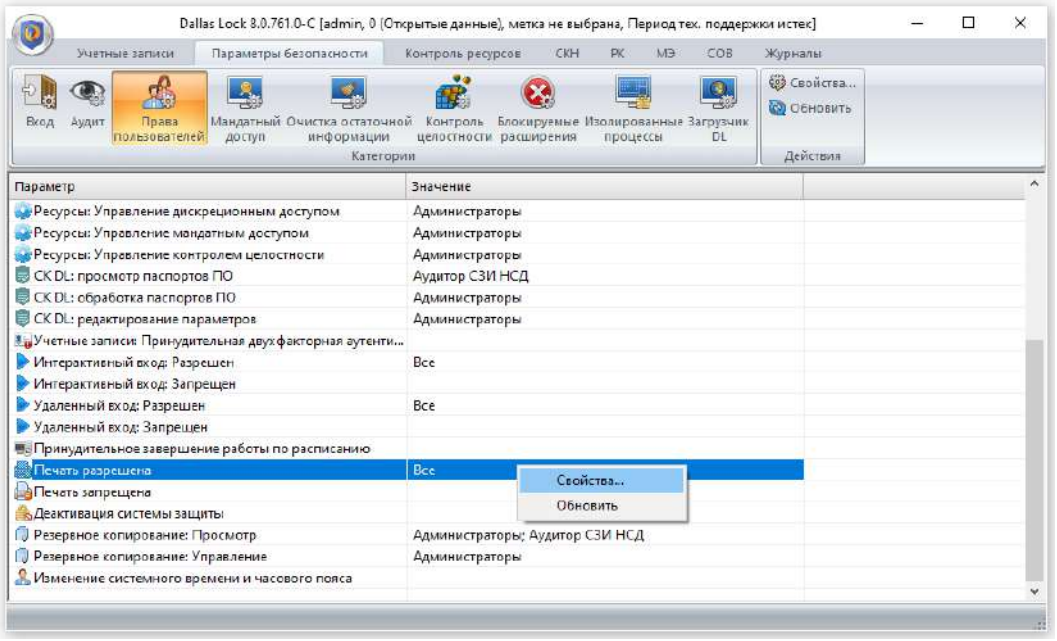


Рис. 149. Права пользователей на доступ к печати

При настройке следует учесть, что установленный параметр запрета имеет более высокий приоритет перед установленным параметром разрешения.

Правило разрешения и запрета следующее:

Условие	Результат
Нет никаких запретов и разрешений	Действие запрещено
Есть запись о разрешении, и нет записи о запрете	Действие разрешено
Есть запись о запрете	Действие запрещено, несмотря на наличие или отсутствие записи о разрешении

В списке субъектов, для которых устанавливается запрет или разрешение, определяется иерархия в порядке возрастания: группа «Все» → индивидуальная группа → учетная запись (доменная учетная запись «по маске») → пользователь.

Таким образом, чтобы субъекту (например, пользователю) действие было разрешено, то он не должен входить в состав субъекта (например, группы), для которого это действие имеет явный запрет.

Пример

Требуется запретить печать определенным доменным пользователям определенного домена, а разрешить всем остальным пользователям только данного домена.

По умолчанию печать разрешена всем пользователям: параметр «Печать разрешена» имеет значение «Все», параметр «Печать запрещена» имеет пустое значение. Чтобы запретить печать определенным доменным пользователям определенного домена, необходимо для параметра «Печать разрешена» установить значение «имя_домена*» (учетная запись по маске), а для параметра «Печать запрещена» установить значение «имя_домена\имя_пользователя» (индивидуальная учетная запись выбранного пользователя).

В итоге всем пользователям печать будет запрещена (так как группы «Все» уже не будет ни в одном

из двух списков), пользователям выбранного домена печать будет разрешена, и индивидуальным выбранным пользователям данного домена печать будет запрещена.

7.1.1 Мандатное разграничение доступа к печати

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

В СЗИ Dallas Lock 8.0 редакции «С» имеется возможность выполнить настройку разграничения печати документов с защищенного ПК для пользователей, работающих под различными уровнями доступа, путем разрешения печати из-под определенных уровней.

Чтобы выбрать уровни доступа, необходимо в оболочке администратора открыть вкладку «Параметры безопасности» → «Аудит» и выбрать параметр «Разрешить печать из-под уровней». Появится окно, в котором необходимо отметить уровни, при работе под которыми для пользователей будет открыт доступ для печати документов с данного ПК (рис. 150).

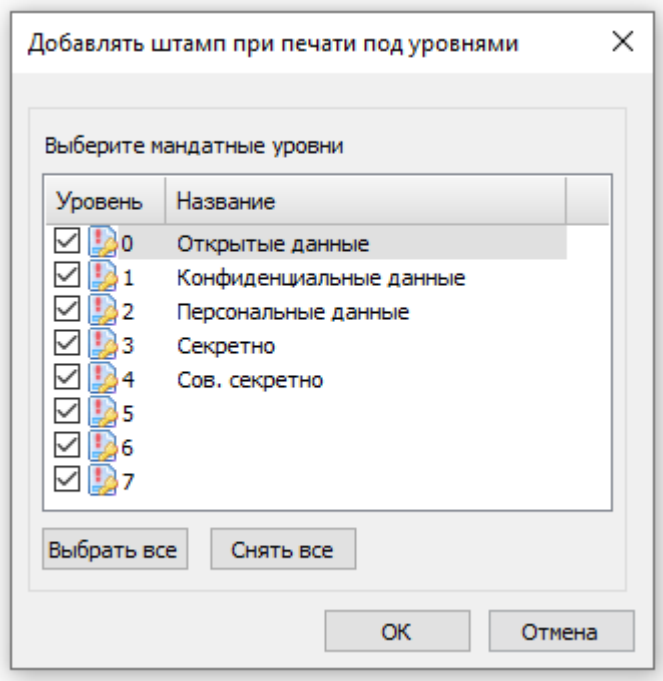


Рис. 150. Выбор мандатных уровней для доступа к печати

Пользователям, которые осуществили авторизацию под уровнем, не отмеченным к доступу печати, при попытке отправить файл на печать будет выдаваться отказ в доступе, процесс печати будет прекращен.

7.1.2 Разграничение доступа к принтерам

Средствами контроля доступа к устройствам в СЗИ можно настроить разграничение доступа определенных пользователей к определенным печатающим устройствам (см. «Контроль устройств»).

В дереве устройств («Контроль ресурсов» → «Устройства») имеется возможность для выбранного значка печатающего устройства открыть дескриптор с параметрами безопасности, в котором возможны настройки доступа:

- Дискреционным принципом. Имеется два права доступа для выбранной учетной записи или группы по отношению к устройству: «Разрешить» и «Запретить».
- Мандатным принципом (только для Dallas Lock 8.0 редакции «С»). Имеется возможность установить уровень доступа и мандатную метку для доступа к устройству только пользователей с таким же уровнем.

Также возможна установка ведения аудита события доступа к выбранному устройству.

7.2 Аудит печати

Помимо разграничения доступа к печати документов в СЗИ имеется возможность вести аудит событий печати, настроить теневое копирование распечатываемых документов и добавление штампов на распечатываемые документы.

7.2.1 Журнал печати

Для того, чтобы протоколировать события печати с защищенного ПК на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.), необходимо включить журнал печати (вкладка «Параметры безопасности» → «Аудит» → «Журнал печати» → значение «Вкл.»).

Примечание. Если включен журнал печати, то подсистемам СЗИ необходимо контролировать права на выполнение печати для любого процесса, выполняющего печать. Для корректного расчета прав пользователя, запустившего процесс, определяется актуальный список групп, в которые данный пользователь входит. Соответственно, если пользователь доменный (AD) и нет связи с соответствующим контроллером домена (т. е. расчет актуального набора прав технически невозможен), то возможность печати для таких пользователей будет заблокирована СЗИ.

Примечание. Печать пробной страницы является служебной информацией и не подлежит контролю и регистрации.

Если дополнительно включен параметр «Создавать теневые копии распечатываемых документов» (см. ниже), то в журнале печати для записи процесса распечатки документа доступна функция просмотра копии документа, созданной в системной папке (рис. 151).

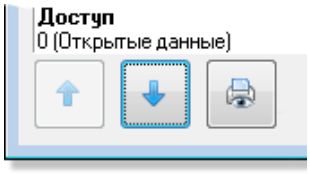


Рис. 151. Просмотр копии распечатываемого документа

Примечание. Для корректной работы функции аудита печати необходимо сперва закрыть все открытые файлы, потом включить журнал печати. В противном случае для открытых ранее файлов события печати регистрироваться не будут.

7.2.2 Теневые копии распечатываемых документов

Для того, чтобы включить создание теневых копий, необходимо открыть вкладку «Параметры безопасности» → «Аудит», выбрать параметр «Создавать теневые копии распечатываемых документов» и установить значение «Да».

Включение данного параметра позволяет сохранять копии распечатываемых документов в отдельной папке по пути: «C:\DLLOCK80\Logs\PrintCopy». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства. Просмотреть созданную таким образом копию документа можно, кликнув мышкой соответствующую запись в журнале печати, и в окне свойств записи нажав кнопку просмотра.

Внимание! При просмотре теневой копии некоторые программы просмотра в процессе своей работы создают временные файлы в папках, не отмеченных, как разделяемые. Это может привести к соответствующим ограничениям при просмотре теневых копий в конфиденциальных сеансах доступа, так как нельзя создавать временные файлы в директориях с другой мандатной меткой или более низким уровнем доступа.

Для решения данной проблемы можно воспользоваться следующими вариантами:

1. Произвести настойку СЗИ таким образом, чтобы создание временных файлов выполнялось в разделяемых папках (см. «Механизм разделяемых папок»).
2. Использовать программы просмотра, не создающие временные файлы, например, Paint.

С помощью параметра «Аудит: Просмотр теневых копий распечатанных документов» на вкладке «Права пользователей» устанавливается доступ к данной папке, и, соответственно к возможности просмотра теневых копий.

Примечание. При включенном параметре «Создавать теневые копии распечатываемых документов» вывод на печать файлов формата PDF будет осуществляться в виде пустых файлов. Это является особенностью защиты от копирования самого формата и не является ошибкой.

Примечание. При включенном параметре «Создавать теневые копии распечатываемых документов» вывод на печать документов может происходить с задержкой, так как на печать отправляется именно созданная теневая копия (размер 1-страничного файла составляет ≈180 Мбайт).

7.2.3 Добавление штампа на распечатываемые документы

Система защиты Dallas Lock 8.0 позволяет на всех распечатываемых документах добавлять штамп независимо от программы, из которой производим печать.

Внимание! Следует учесть, что при условии включенного аудита печати (вкладка «Параметры безопасности» → «Аудит») в случае использования приложений Microsoft Edge, Internet Explorer 11, Microsoft.Photos при попытке печати штампа выполняется запрет печати, и выводится соответствующее предупреждение.

Примечание. Для СЗИ Dallas Lock 8.0 редакции «С» имеется возможность разграничения нанесения штампа на распечатываемые документы при печати под определенными уровнями доступа. Для того, чтобы выбрать уровни доступа, необходимо в оболочке администратора открыть вкладку «Параметры безопасности» → «Аудит» и выбрать параметр «Добавлять штамп при печати под уровнями». Появится окно, в котором необходимо отметить уровни.

Для настройки печати штампа на документах необходимо на вкладке основного меню «Параметры безопасности» открыть категорию «Аудит» и в списке параметров выбрать пункт «Печатать/редактировать штамп» (рис. 152).

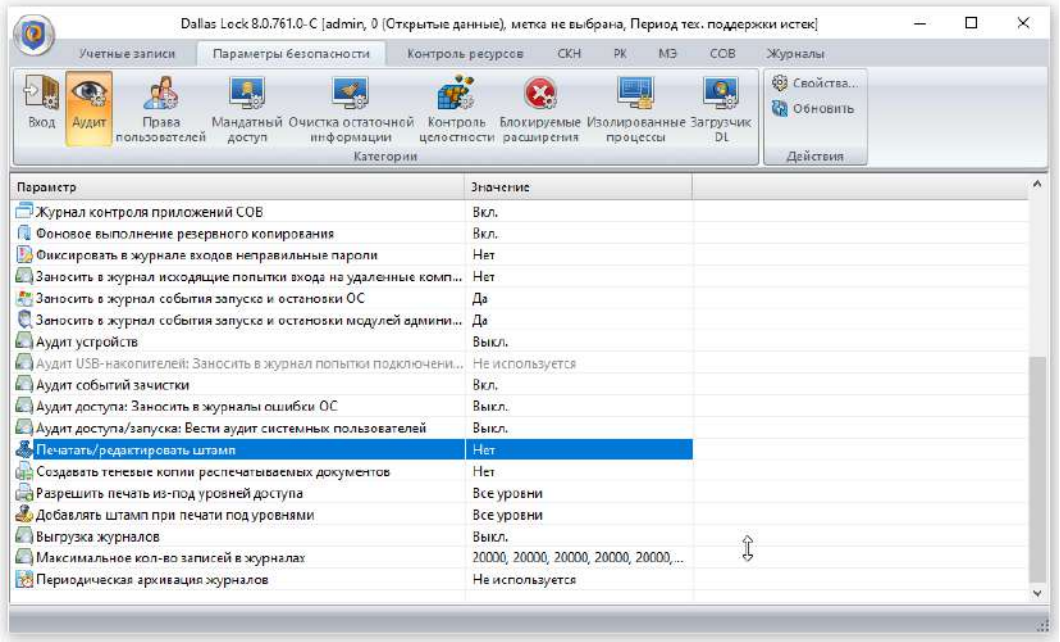


Рис. 152. Выбор настройки печати штампа на документах

Откроется диалоговое окно включения и редактирования штампа на распечатываемые документы (рис. 153).

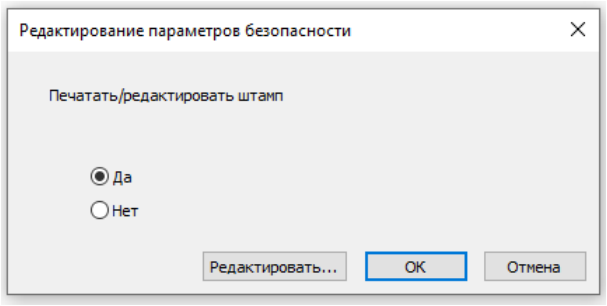


Рис. 153. Диалоговое окно включения и редактирования штампа

Для того, чтобы включить печать штампа, необходимо в диалоговом окне нажать кнопку «ОК».

Для того, чтобы отредактировать штамп, необходимо нажать в диалоговом окне кнопку «Редактировать».

Откроется окно «Редактор штампа» (рис. 154).

Рис. 154. Редактор штампа

Штампы в Dallas Lock 8.0 могут быть двух типов:

- **Штамп по ГОСТ** — не редактируемый предопределенный вид штампа;
- **Штамп на обратной стороне** — пользователь может произвольно редактировать внешний вид штампа и его местоположение на листе.

При выборе печати штампа по ГОСТ на печатные документы будет наноситься штамп в соответствии с правилами учета секретных документов, при этом дополнительная настройка штампа не возможна: вид штампа предопределен.

При включенной печати штампа по ГОСТ выбрать число распечатываемых копий средствами ОС становится невозможным, но это меняется при появлении на экране формы параметров печати Dallas Lock 8.0 распечатываемого документа.

В данном окне пользователю необходимо ввести:

- учетный номер документа (обязательное поле);
- код носителя (обязательное поле);
- общее количество экземпляров (по умолчанию — 1);
- номер текущего экземпляра (при выборе количества экземпляров более 1 определяется или автоматически и последовательно, или вручную);
- в поле «Использование» можно ввести комментарии для каждого распечатываемого экземпляра.

Штамп по ГОСТ на распечатанном документе имеет следующий формат: на первом листе документа в верхнем правом уголке добавляется уровень доступа и (или) мандатная метка и номер экземпляра, в нижнем левом уголке добавляется учетный номер. На последующих листках документа в нижнем левом уголке добавляется учетный номер.

В процессе распечатки документа на экране появляется сообщение: «После того, как все страницы документа будут распечатаны, вставьте последнюю страницу в лоток подачи бумаги обратной стороной и нажмите кнопку «ОК». Пользователю необходимо выполнить указанное действие.

В результате на обратной стороне последней страницы документа появится метка, содержащая учетный номер документа, код носителя, количество экземпляров, использование экземпляров, время распечатки и имя пользователя, который произвел распечатку. При этом имя пользователя берется из имени учетной записи пользователя.

Внимание! Следует учесть, что при выборе типа печати штампа «по ГОСТ», печать каждого экземпляра осуществляется только после вызова функции печати данного файла. То есть за одно обращение к принтеру можно напечатать только одну копию документа. Если требуется N копий, то необходимо отправить документ на печать N раз.

При выборе печати штампа на обратной стороне становятся доступными для выбора другие поля окна настройки. Становится возможным отредактировать внешний вид и содержимое штампа (для редактирования доступны штампы на лицевой и обратной стороне документа). Доступны

следующие настройки:

- **Настройки текста**. Здесь выбирается шрифт, размер, цвет шрифта и выравнивание текста в блоке штампа.
- **Позиция и размер элемента**. Здесь задается поворот штампа, ширина и высота штампа, а также координаты расположения штампа по осям X и Y.
- **Единицы измерения**. Указываются единицы измерения (%, пиксели, миллиметры).
- **Атрибуты** (отобразить текстовые значения). Вместо тегов в угловых скобках возможно задать текстовые значения.

В качестве имени пользователя для произвольного штампа можно использовать не имя учетной записи пользователя, а его описание, для чего выставить флаг в соответствующем поле.

Сам штамп представляет собой текст, который, после нажатия кнопки  вводится в отведенном для набора поле (рис. 156).

В штамп можно вставить служебную информацию. Для этого необходимо дважды щелкнуть левой кнопкой мыши в поле ввода. В появившемся окне выбрать, какая именно информация должна быть напечатана (рис. 155).

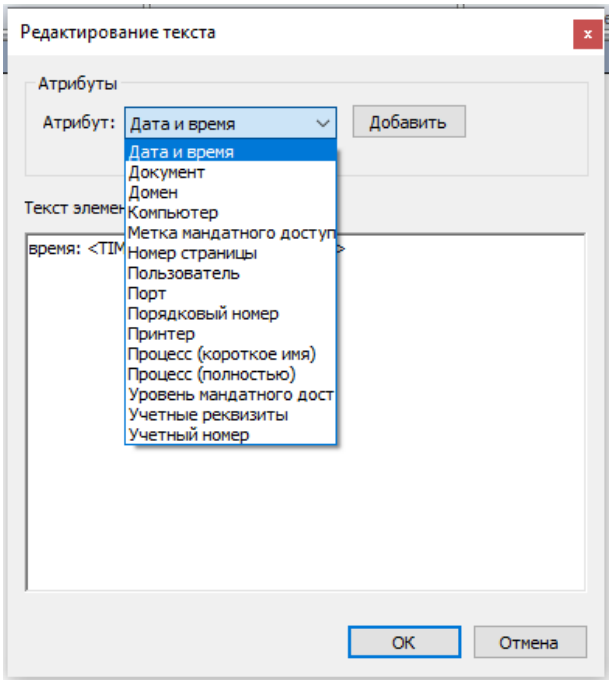


Рис. 155. Выбор данных для текста штампа из контекстного меню

В поле ввода в угловых скобках отображается выбранная для печати информация в виде тегов.

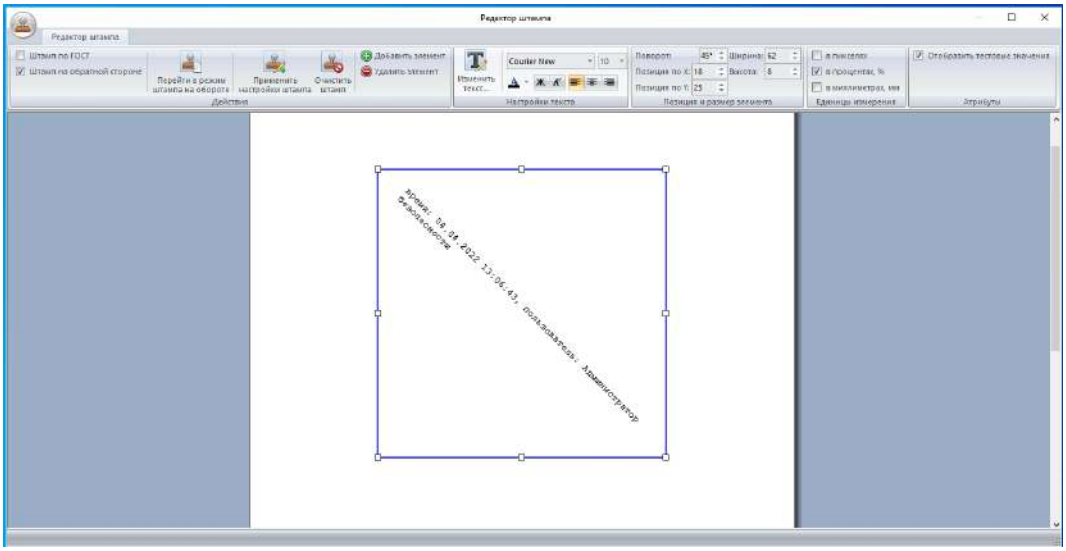


Рис. 156. Теги текста штампа в окне настройки

Если в штампе есть учетный номер документа (тег <REGISTRY NUMBER>), то перед распечаткой документа на экране появится окно, в котором пользователь должен ввести учетные реквизиты и

нажать кнопку «ОК». Вставка тега <SERIAL NUMBER> потребует ввести при печати порядковый номер документа в появившуюся форму.

При использовании произвольного типа штампа, на всех распечатываемых страницах, независимо от номера, будет добавляться одинаковый штамп.

Примечание. Данное маркирование документов — это некий аналог «механического» штампа. Поэтому он добавляет штампы независимо от содержимого документов. В некоторых случаях, штамп может добавляться прямо поверх текста документа.

Что понимать под уровнем доступа документа, выводимого на печать?

Уровень доступа документа — это свойство объекта ФС, в частности файла. Но соответствия между конкретным файлом и распечатываемым документом может и не быть.

Например, запускается MS Word, в нем набирается какой-то текст и отправляется на печать. Как называется файл, который распечатывается? Никак. Файла нет, так как текст существует только в оперативной памяти компьютера, и когда закроется приложение MS Word, исчезнет и текст.

Другой пример. В MS Word открыт файл «C:\document1.docx», имеющий уровень доступа 0, далее, с помощью буфера обмена, ему добавлен в конец текст из файла «C:\document2.docx» имеющий уровень доступа 1. Исходный документ отправлен на печать. Как называется файл, который распечатывается, какой уровень доступа он имеет? Аналогично первому случаю — файла с таким содержимым нет, уровня доступа, соответственно, тоже нет.

Таким образом, под уровнем доступа распечатываемого документа понимается **текущий уровень доступа пользователя,** который распечатывает данный документ. И по этой же причине в журнале печати нет поля «имя файла».

Маркирование документов под мандатными метками производится аналогичным образом.

8 ОЧИСТКА ОСТАТОЧНОЙ ИНФОРМАЦИИ

Большинство ОС при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории ФС. Так сделано для ускорения работы системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть до тех пор, пока ОС заново не использует это пространство для хранения новых данных. Данная остаточная информация может легко привести к непреднамеренному распространению конфиденциальной и секретной информации.

СЗИ Dallas Lock 8.0 включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Данная подсистема позволяет выполнять следующее:

- Затирать всю остаточную информацию при освобождении областей на дисках, т.е. при удалении файлов или при перемещении файлов, или при уменьшении размеров файлов. Затирание производится записью, маскирующей последовательности поверх освобождаемого пространства.
- Затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).
- Принудительно зачищать конкретную папку/файл, выбрав соответствующий пункт в контекстном меню данного файла.
- Проверять корректное завершение процесса очистки информации.
- Предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого без перезагрузки, что гарантирует освобождение используемых областей оперативной памяти, с помощью параметра «Запрет смены пользователя без перезагрузки».

8.1 Регистрация действий по очистке остаточной информации

Для того, чтобы фиксировать события зачистки остаточной информации (успешные и неуспешные), необходимо включить (значение «Вкл.») отвечающий за это параметр аудита: «Параметры безопасности» → «Аудит» → параметр «Аудит событий зачистки».

При включенном данном параметре события очистки остаточной информации (см. ниже), будут заноситься в журнал ресурсов, который также должен быть включен («Параметры безопасности» → «Аудит» → параметр «Журнал ресурсов», значение «Вкл.»).

8.2 Параметры очистки остаточной информации

Для настройки процесса очистки остаточной информации в соответствии с требованиями, необходимо в оболочке администратора во вкладке основного меню «Параметры безопасности» выбрать категорию «Очистка остаточной информации» (

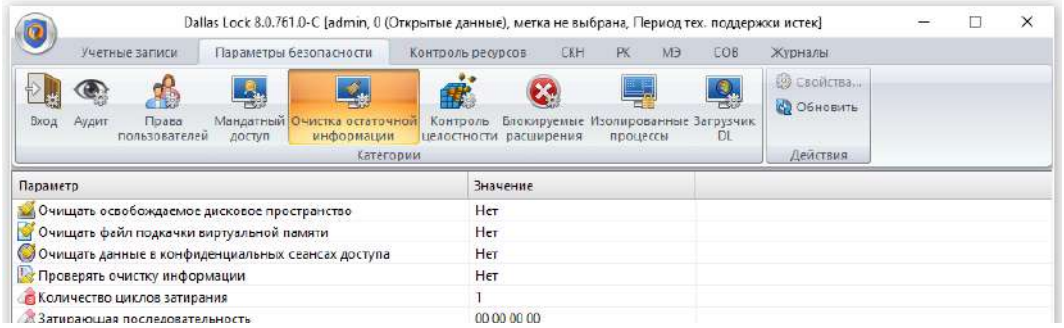


рис. 157).

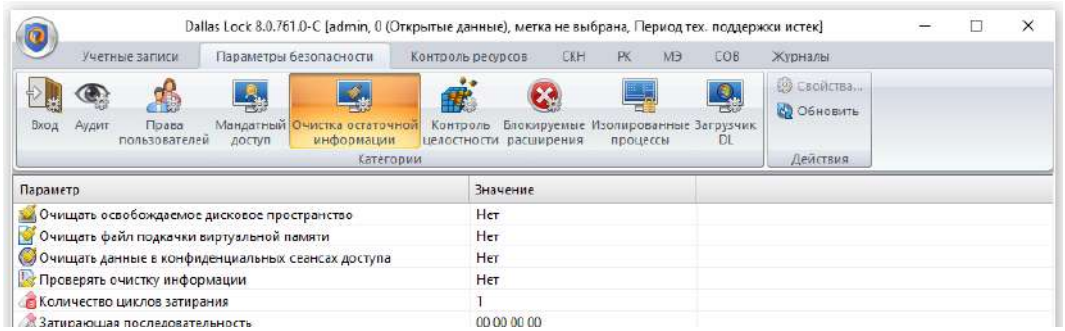


Рис. 157. Параметры очистки остаточной информации

Появится список параметров очистки остаточной информации. Изменить необходимый параметр можно, выделив его и нажав на панели действий кнопку «Свойства».

8.2.1 Проверка очистки информации

Если параметр «Проверять очистку информации» включен, то после проведения очистки объектов ФС, дополнительно выполняется проверка того, что очистка действительно осуществлена. В том случае, если проверка выявила, что очистка не осуществлена или завершена с ошибкой, то в журнал ресурсов заносится соответствующее событие.

Проверка осуществляется при очистке остаточной информации, выполняемой по команде администратора, в автоматическом режиме, и при зачистке накопителя целиком (функция «Зачистка диска»).

8.2.2 Очистка освобождаемого дискового пространства

Включение параметра «Очищать освобождаемое дисковое пространство» (значение «вкл.») позволяет автоматически затирать всю остаточную информацию при освобождении областей на дисках, то есть при удалении файлов или при уменьшении размеров файлов. Затирание производится записью маскирующей последовательности поверх освобождаемого пространства заданным количеством циклов затирания (см. ниже). Включение данного параметра может заметно снизить скорость выполнения файловых операций, особенно при количестве циклов затирания больше единицы.

8.2.3 Очистка файла подкачки виртуальной памяти

Включение параметра «Очищать файл подкачки виртуальной памяти» (значение «вкл.») позволяет автоматически затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).

8.2.4 Очистка данных в конфиденциальных сеансах доступа

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Включение параметра «Очищать данные в конфиденциальных сеансах доступа» (значение «вкл.») позволяет осуществлять автоматическую зачистку освобождаемого дискового пространства только при удалении/перемещении/уменьшении размера объектов ФС при работе под мандатной меткой или уровнем доступа больше нуля. Данная политика функционирует при условии включенной политики «Очищать освобождаемое дисковое пространство».

8.2.5 Количество циклов затирания, затирающая последовательность

Затирание производится записью маскирующей последовательности поверх освобождаемого пространства. Чем большее число циклов затирания выбрано, тем надежнее происходит удаление информации. При этом следует учесть, что чем больше циклов затирания будет выбрано, тем больше времени эта процедура будет занимать.

В СЗИ Dallas Lock 8.0 с помощью параметра «Количество циклов затирания» можно выбрать от одного до четырех циклов затирания.

Другим параметром «Затирающая последовательность» определяется метод затирания остаточной информации, путем установки числовых байтовых значений (от 0 до F) для каждого из четырех циклов затирания. Если эти значения не установлены или установлены не для каждого цикла, то по умолчанию для затирающей последовательности циклов используется последовательность, установленная в Dallas Lock.

Установленное количество циклов затирания и методы затирания используются при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме, и при зачистке накопителя (функция «Зачистка диска»).

8.3 Удаление файлов и зачистка остаточной информации по команде

При необходимости удалить какие-либо данные без возможности их восстановления нужно воспользоваться контекстным меню данного объекта ФС и выбрать пункт «DL8.0: Удалить и зачистить» (рис. 158).

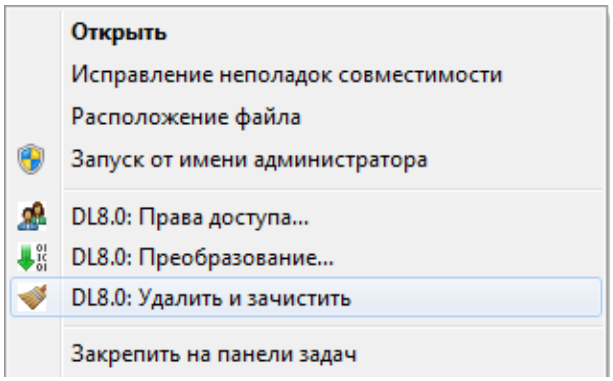


Рис. 158. Контекстное меню

Аналогичным образом реализуется удаление и зачистка файлов и папок, перемещенных в корзину (рис. 159).

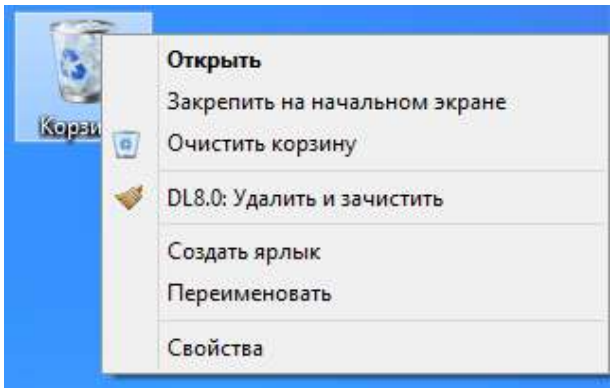


Рис. 159. Контекстное меню зачистки корзины

Появится окно с требованием подтвердить операцию (рис. 160).

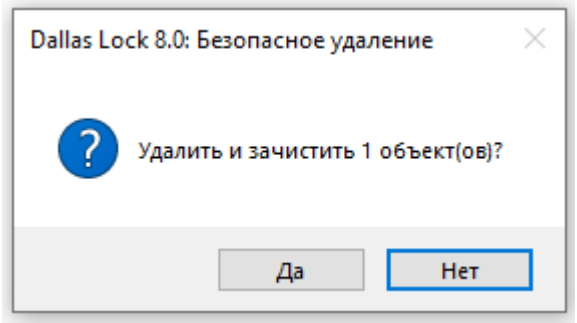


Рис. 160. Подтверждение удаления файла

Внимание! Для того, чтобы выполнить зачистку логического диска, пользователь, от которого выполняется операция, должен иметь следующие права:

1. Низкоуровневая запись и чтение для данного диска.
2. Просмотр и редактирование политик.

При активации удаления происходит зачистка данного объекта путем перезаписи файла. Количество циклов затирания определяется соответствующей политикой (см. «Количество циклов затирания, затирающая последовательность»). После перезаписи восстановить хоть сколько-нибудь значимый фрагмент файла становится практически невозможно. После успешного удаления объектов система выведет соответствующее подтверждение (рис. 161).

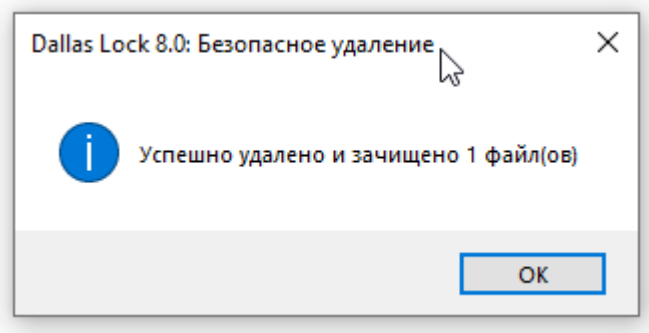


Рис. 161. Сообщение системы об успешном удалении

Примечание. При нескольких одновременно выделенных объектах происходит их одновременное удаление и зачистку как группы. При этом появится окно подтверждения удаления с количеством зачищаемых объектов.

Примечание. При автоматической зачистке файла, не содержащего информацию, запись в журнал не заносится.

8.4 Запрет смены пользователя без перезагрузки

В соответствии с требованиями политик безопасности организации возможно Включение запрета смены пользователя компьютером без его перезагрузки.

Чтобы установить данный запрет, необходимо включить параметр входа «Вход: запрет смены пользователя без перезагрузки» («Параметры безопасности» → «Вход»). Параметр может принимать значение «Включен» или «Выключен». Включение данной политики («Вкл.») не позволит осуществить смену пользователя без перезагрузки компьютера (рис. 162).

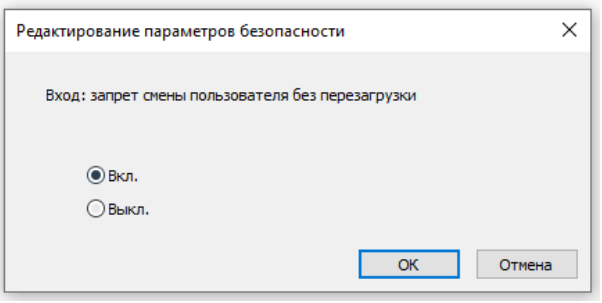


Рис. 162. Редактирование параметров безопасности

Если установлено значение «Включен», то при выборе пункта «Завершение сеанса» в окне «Завершение работы Windows», компьютер автоматически уйдет на перезагрузку (рис. 163).

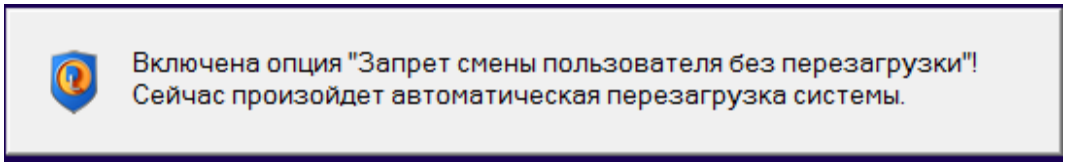


Рис. 163. Сообщение системы при автоматической перезагрузке

Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПК, оставшуюся там после завершения сеанса работы другого пользователя.

8.5 Зачистка диска

Система защиты Dallas Lock 8.0 позволяет полностью зачищать остаточные данные всего диска или его разделов. Для этого служит функция «Зачистка диска». Данная функция может применяться к разделам фиксированных и съемных жестких дисков и к USB-Flash накопителям. Системный раздел с установленной ОС для данной операции будет недоступен.

Примечание. Функциональная возможность зачистки фиксированного диска требует наличия доступа к зачищаемому диску. В частности, если стороннее ПО (например, антивирусы или иные средства защиты информации) блокируют доступ к какому-либо файлу или папке на фиксированном диске, функция зачистки данного диска СЗИ Dallas Lock 8.0 может оказаться заблокированной.

Зачистка диска может быть полезна при снятии носителей с учета и необходимости полного удаления данных без возможности их восстановления по остаточной информации.

Примечание. Полная зачистка диска выполняет в том числе зачистку boot-сектора. В связи с этим после проведения данной операции зачищенный диск подлежит форматированию.

Для вызова данной функции необходимо в оболочке администратора нажать кнопку основного меню и в списке дополнительных функций выбрать пункт «Зачистка диска» (рис. 164).

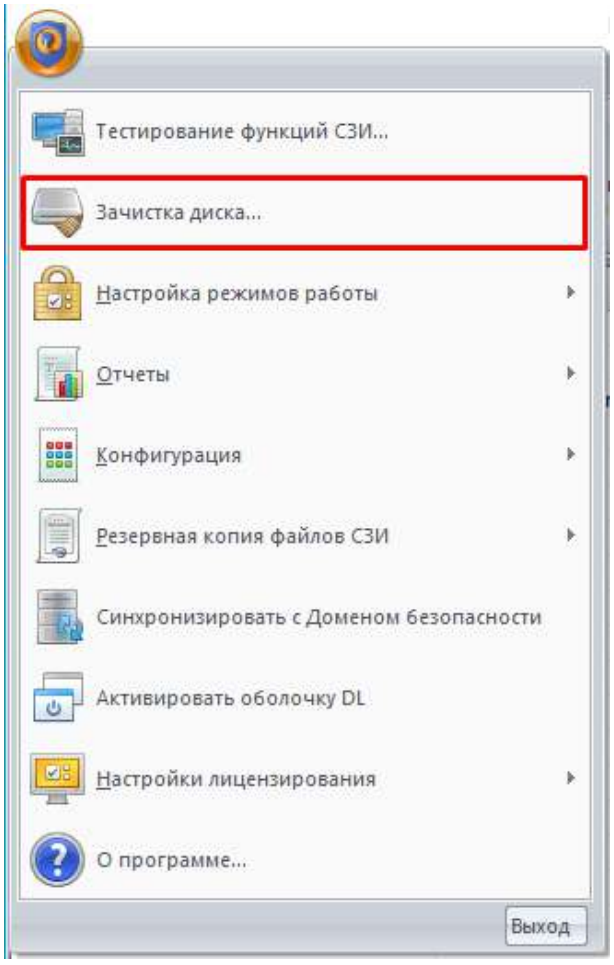


Рис. 164. Выбор функции «Зачистка диска»

Появится окно, в котором необходимо выбрать жесткие диск из списка обнаруженных в системе и нажать «Зачистить».

Внимание! Для того, чтобы выполнить зачистку логического диска, пользователь, от которого выполняется операция, должен иметь следующие права:

1. Низкоуровневая запись и чтение для данного диска.
2. Просмотр и редактирование политик.

Запустится процесс зачистки остаточных данных жесткого диска. Процесс будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса на экран будет выведено сообщение об успешном окончании операции.

9 ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ

Система защиты информации Dallas Lock 8.0 включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность программно-аппаратной среды компьютера, целостность объектов ФС и реестра, а также восстанавливать файлы и ветки реестра в случае обнаружения нарушенной целостности.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Процедура контроля целостности осуществляется следующим образом: после назначения дескриптора целостности при следующей проверке проверяется, было ли уже вычислено эталонное значение контрольной суммы параметра. Если оно еще не было вычислено, оно вычисляется и сохраняется. Если же оно уже было вычислено, то оно сравнивается с вычисляемым текущим значением контрольной суммы контролируемого параметра. Если хотя бы для одного из проверяемых параметров текущее значение параметра не совпало с эталонным значением, результат проверки считается отрицательным, а целостность контролируемых объектов — нарушенной.

Примечание. Для программно-аппаратного контроля целостности СЗИ использует подсистему WMI. Если стороннее ПО блокирует или встраивается в работу этой подсистемы, могут наблюдаться проблемы выполнения расчета программно-аппаратной целостности и, соответственно, проблемы авторизации пользователей. В частности, если требуется контролировать программно-аппаратную целостность системы, следует избегать установки Microsoft SQL сервера в конфигурации, при которой он будет запускаться от имени пользователя. Данный вариант приводит к взаимоблокировке подсистемы WMI и SQL-сервера. Это, в свою очередь, может сопутствовать проблемам авторизации пользователей в ОС.

В ряде подобных случаев для разрешения сценариев блокировки сессий на этапе авторизации может помочь использование функциональной возможности сессий-исключений. Достаточно понимать, что для сессий-исключений обращение к подсистеме WMI в рамках встроенных механизмов СЗИ не производится.

У каждой учетной записи пользователя есть свойство, отвечающее за то, что делать при выявлении нарушения целостности — либо блокировать загрузку (при условии, что в свойствах учетной записи включен параметр «Запретить работу при нарушении целостности»), либо выдавать предупреждение и продолжать загрузку.

Проверка целостности по умолчанию осуществляется при загрузке компьютера, при доступе к объекту и при проверке по команде администратора. Дополнительно можно задать проверку целостности по расписанию и по времени.

Примечание. Для расчета контрольных сумм по содержимому объектов используются алгоритмы: ГОСТ Р 34.11-94 (расчет хэш-функций), CRC32, MD5. Алгоритм выбирается администратором при назначении контроля целостности.

Для изменения значений параметров контроля целостности и для изменения списка контролируемых объектов: ФС, программно-аппаратной среды и веток реестра (добавление, удаление, редактирование), пользователь должен обладать правом «Параметры безопасности: управление». В то же время для просмотра только значений установленных параметров и дескрипторов целостности пользователь должен обладать правом «Параметры безопасности: просмотр».

Примечание. СЗИ для возможности восстановления веток реестра при нарушении контроля целостности требуется доступ к соответствующим веткам от имени системного пользователя. Если доступ системному пользователю будет ограничен, функциональная возможность восстановления веток не будет работать корректно.

9.1 Настройка параметров контроля целостности

Для настройки контроля целостности необходимо в оболочке администратора на вкладке «Параметры безопасности» выделить категорию «Контроль целостности». В окне автоматически откроются параметры контроля целостности (рис. 165).

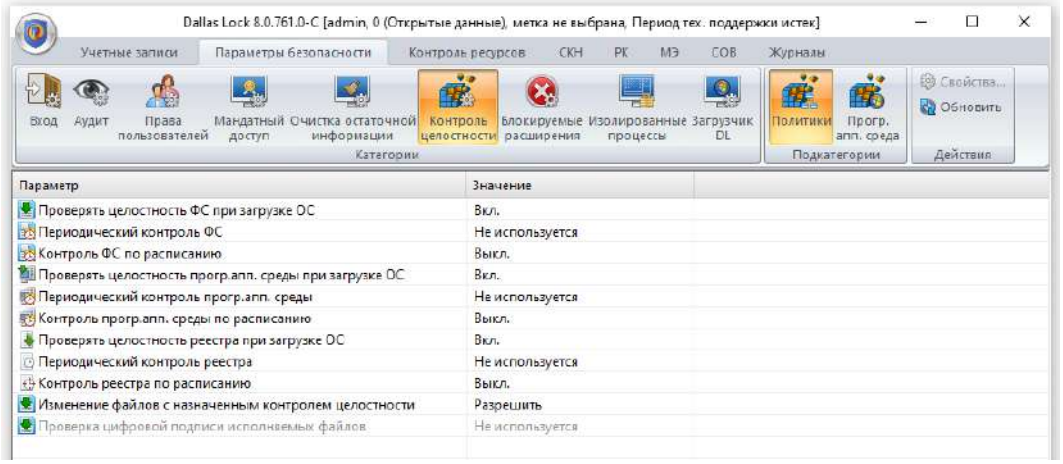


Рис. 165. Закладка Контроль целостности в оболочке администратора

С помощью данных параметров необходимо настроить периодичность проверки целостности отдельно для объектов ФС, отдельно для объектов программно-аппаратной среды и отдельно для реестра. По умолчанию проверка целостности установлена только при загрузке ОС.

Параметры проверки целостности при загрузке ОС могут быть установлены в значении «включен» или «выключен».

Параметры периодического контроля позволяют производить проверку целостности через указанный промежуток времени: от 1 минуты до 5 часов. Для отключения периода необходимо выбрать значение «Не используется».

Редактирование значений параметров контроля по расписанию позволяет настроить проверку целостности по гибкому расписанию (рис. 166).

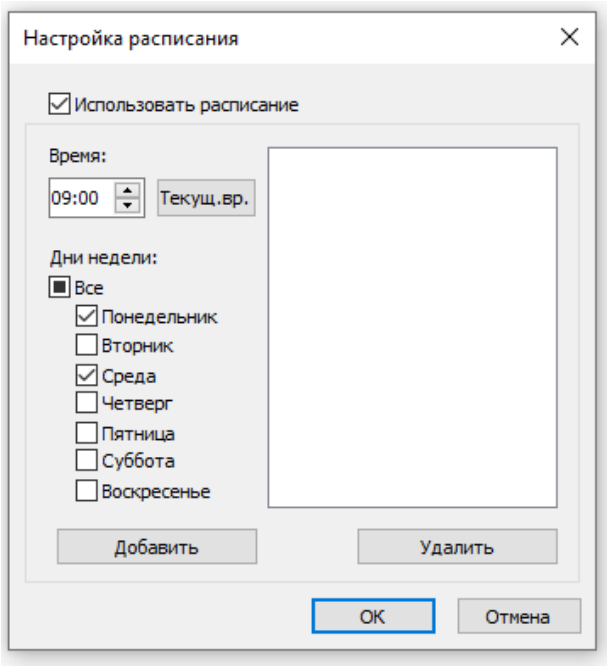


Рис. 166. Настройка расписания контроля целостности

В окне настройки расписания необходимо включить контроль (поставить флаг в поле «Контроль по расписанию включен») и составить расписание.

Примечание. В случае обнаружения события нарушения целостности ФС в процессе периодического контроля ФС или контроля ФС по расписанию, действия СЗИ зависят от значения свойства текущего пользователя «**Запретить работу при нарушении целостности**». В случае, если это свойство включено, сеанс работы пользователя автоматически завершится. Если же это свойство выключено, то пользователю будет выведено предупреждение о нарушении целостности. Имена объектов ФС, целостность которых была нарушена, администратор системы защиты сможет посмотреть в журнале доступа к ресурсам. Если рабочая станция входит в ДБ, то при событии нарушения целостности на СБ будет отправляться соответствующее событие сигнализации (см. «Сигнализация об НСД»).

Каждое события нарушенной целостности сопровождается всплывающим сообщением на панели задач и записью в журнале ресурсов, при этом в графах «Результат», «Операция» и «Процесс» отображается значение параметра контроля целостности. При проверке целостности при загрузке ОС записи о нарушенной целостности попадают и в журнал входов. Следует учесть, что после включения проверки целостности при загрузке ОС одновременно и для объектов ФС, и для объектов программно-аппаратной среды и для реестра (все включено по умолчанию), при проверке целостности при загрузке ОС в журнал входов попадает запись о первом событии.

9.2 Контроль целостности объектов ФС и веток реестра

Моменты, когда осуществляется проверка целостности объектов ФС (файлов и папок) и веток реестра, определяются соответствующими политиками контроля целостности.

Также проверка целостности осуществляется по команде администратора (действие «Проверить» в оболочке администратора) и при доступе к объекту.

Назначить контроль целостности для файла можно двумя разными способами: используя оболочку администратора СЗИ или вызвав контекстное меню файла щелчком по его значку. Объекты ФС, на которые назначен контроль целостности любым из способов, автоматически появляются в списке объектов в окнах категорий «ФС» и «Реестр» при выбранном фильтре по типу контроля «Контроль целостности» на вкладке «Контроль ресурсов».

При выборе категории «Все» на вкладке «Контроль ресурсов» также появляется список, содержащий параметры всех объектов: глобальных, локальных или сетевых, на которые назначены какие-либо права дискреционного доступа, аудит, а также контроль целостности.

9.2.1 Установка целостности

Для того, чтобы установить целостность для конкретного объекта ФС или ветки реестра, необходимо выполнить следующее:

1. Открыть дескриптор безопасности объекта, используя оболочку администратора Dallas Lock 8.0 (перейти на вкладку «Контроль ресурсов», выбрать тип ресурса «ФС» или «Реестр» и нажать кнопку «Добавить (ФС)» или «Добавить (Реестр)») соответственно, или через контекстное меню объекта (пункт «Права доступа» для объекта ФС) (рис. 167).

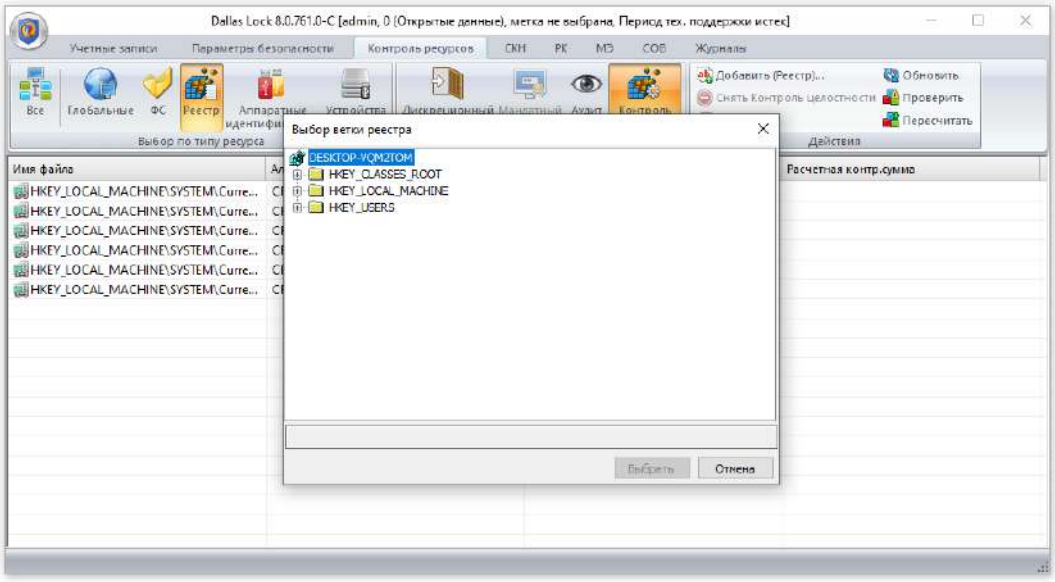


Рис. 167. Вызов дескриптора безопасности

2. В отобразившемся окне дескриптора безопасности объекта необходимо открыть закладку «Контроль целостности» (рис. 168).
3. Необходимо отметить флагом поле «Контроль целостности включен», выбрать алгоритм расчета контрольной суммы (CRC32, Хэш ГОСТ Р 34.11-94, Хэш MD5) и нажать «Пересчитать».
4. При необходимости нужно отметить следующие параметры для следующих объектов:
   - **Для файлов —** «Проверять контроль целостности при доступе» и «Восстанавливать в случае нарушения целостности». При попытке доступа к файлу, у которого нарушена целостность, но отмечено поле «Проверять контроль целостности при доступе», ПК пользователя заблокируется (при условии, что в свойствах учетной записи включен параметр «Запретить работу при нарушении целостности»). Правило распространяется и для веток реестра.
   - **Для папок** — «Проверять целостность при доступе» и «Включая вложенные папки». Если поле «Включая вложенные папки» не отмечено, то контроль целостности будет распространяться только на содержимое корневой папки. Изменение содержимого вложенных папок к нарушению целостности не приведет. Если данное поле отмечено, то помимо корневой папки, на которую назначен контроль целостности, он будет распространяться и на содержимое внутренних (вложенных) папок. Правило распространяется и для веток реестра.
   - **Для веток реестра** — «Включая вложенные ветки» и «Восстанавливать в случае нарушения целостности».
5. Нажать «Применить» и «ОК».

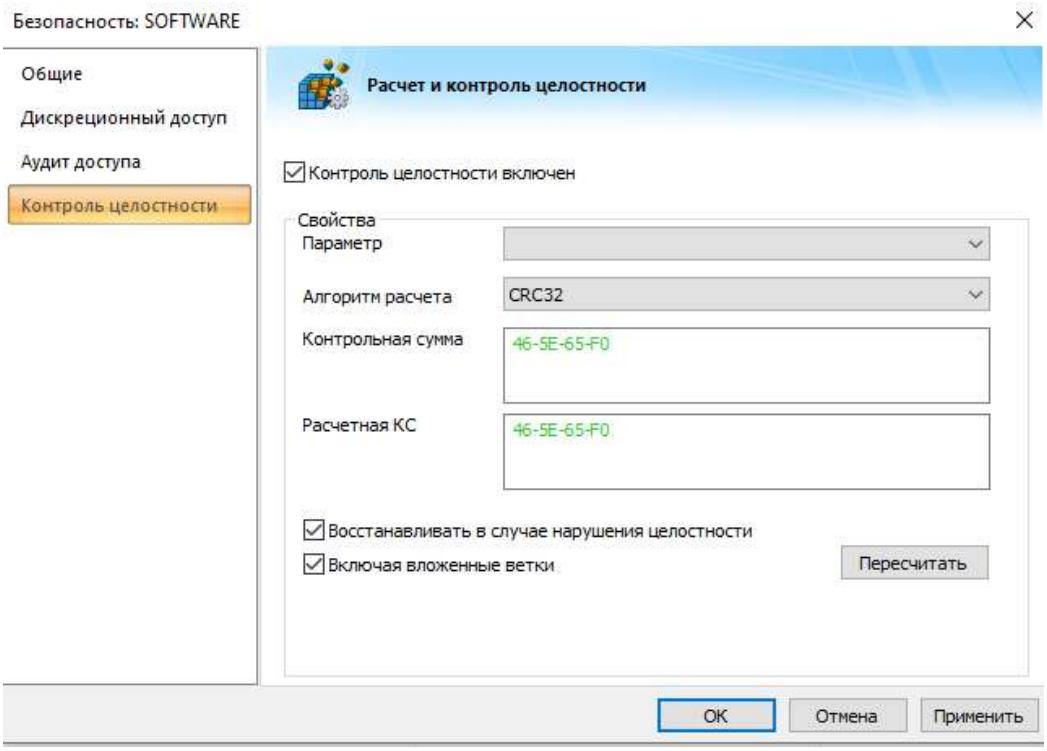


Рис. 168. Контроль целостности ресурса ФС

На вкладке «Параметры безопасности» в категории «Контроль целостности» необходимо установить значение параметра «Изменение файлов с назначенным контролем целостности» (рис. 169). Параметр может принимать одно из значений:

- «Разрешить» — при нарушении целостности СЗИ не блокирует доступ к объекту, для которого назначен контроль целостности;
- «Запретить» — при нарушении целостности СЗИ блокирует доступ к объекту, для которого назначен контроль целостности.

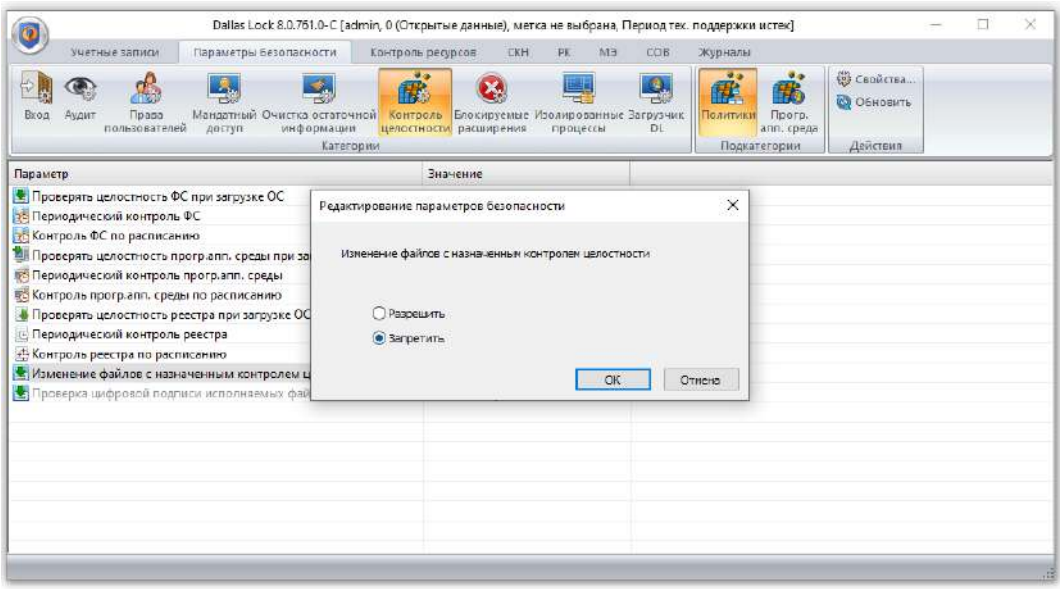


Рис. 169. Изменение файлов с назначенным контролем целостности

Для проверки цифровой подписи для исполняемых файлов перейти на вкладку «Параметры безопасности» в категории «Контроль целостности» и установить необходимое значение параметра «Проверка цифровой подписи исполняемых файлов» (Рис. 170). Параметр может принимать значение «Вкл» или «Выкл». При «Вкл» необходимо указать расширения исполняемых файлов для проверки цифровой подписи.

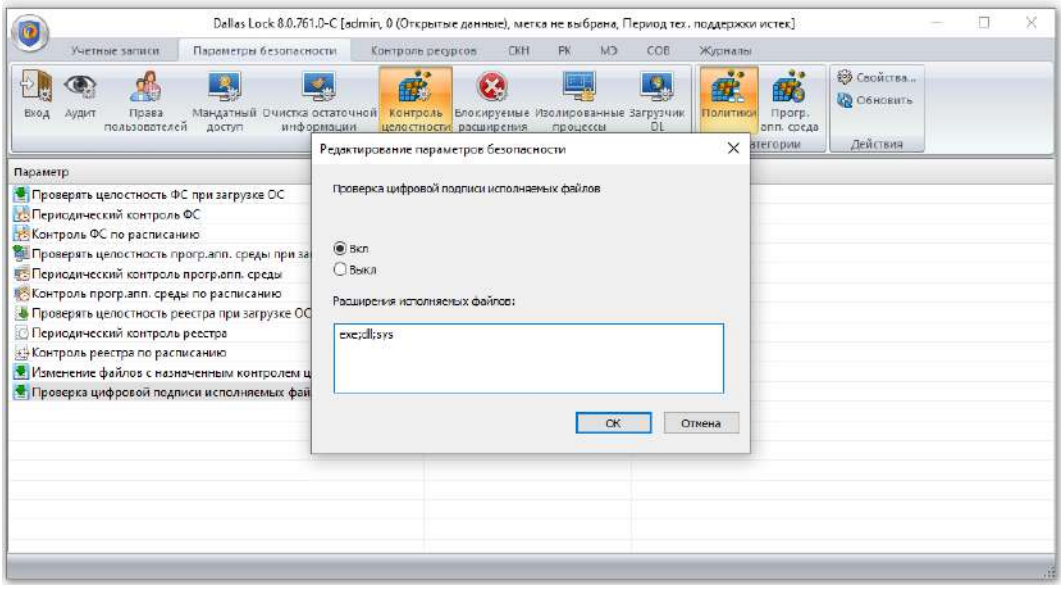


Рис. 170. Настройка проверки цифровой подписи исполняемых файлов

Примечание. Если для объекта задан контроль целостности, то система защиты уже не позволит его удалить, изменить или переименовать. Попытки будут блокироваться. Такой объект будет доступен только для чтения и исполнения. Полный доступ к объекту, для которого установлен контроль целостности, имеет только суперадминистратор.

9.2.2 Проверка целостности

Если некоторый объект ФС или реестра, на который назначена целостность, будет изменен или поврежден, то при проверке (периодичность события проверки определяется установленными параметрами), контрольная сумма нарушится и ее запись в окне дескриптора безопасности будет выделена красным цветом (рис. 171).

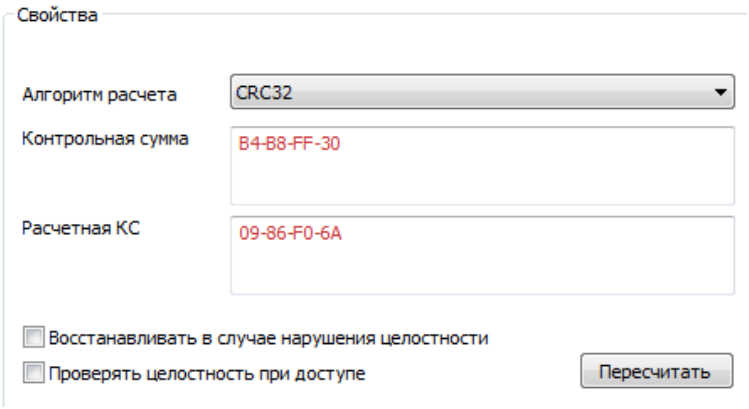


Рис. 171. Нарушение целостности файла

При нажатии на кнопку «Пересчитать» в окне дескриптора или на панели действий в оболочке администратора происходит пересчет контрольной суммы. Пересчет новой контрольной суммы позволяет снова установить целостность файла и проводить ее дальнейшее отслеживание.

События нарушения контроля целостности фиксируются в журнале ресурсов. При проверке целостности по команде администратора (действие «Проверить» в оболочке администратора) в списке объектов категории «Контроль целостности» значок объекта, у которого нарушена целостности будет выделен красным (рис. 172).

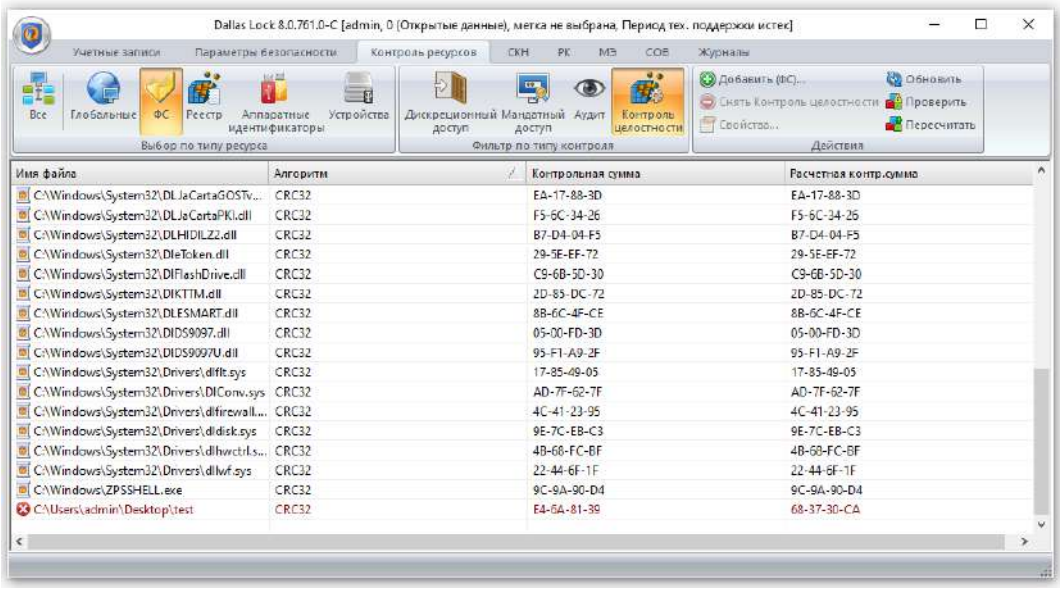


Рис. 172. Список контролируемых объектов

Значения контрольных сумм для контролируемых объектов в оболочке администратора появляются после команд проверки и пересчета контрольных сумм.

9.2.3 Восстановление файла или ветки реестра в случае нарушения целостности

Если для объекта (файла или ветки реестра) установлена целостность и отмечено свойство «Восстанавливать в случае нарушения целостности», то в случае несанкционированного изменения объекта в результате проверки целостности он будет восстановлен до исходного состояния, для которого рассчитана контрольная сумма. Восстанавливается содержимое объекта и его атрибуты.

В списке объектов на вкладке «Контроль ресурсов» → «Контроль целостности» восстановленный объект будет выделен особым значком . Контрольные суммы восстановленного файла будут не измененными.

В журнал ресурсов будут занесены две записи о событиях: о нарушении целостности и о восстановлении объекта. Пользователю отобразиться предупреждение.

9.3 Контроль целостности программно-аппаратной среды

С помощью политик контроля целостности на вкладке «Параметры безопасности» устанавливается периодичность и расписание контроля целостности для объектов программно-аппаратной среды.

Чтобы выбрать категории объектов программно-аппаратной среды, для которых требуется установить контроль целостности, необходимо открыть соответствующую категорию на вкладке «Параметры безопасности» → «Контроль целостности» (рис. 173).

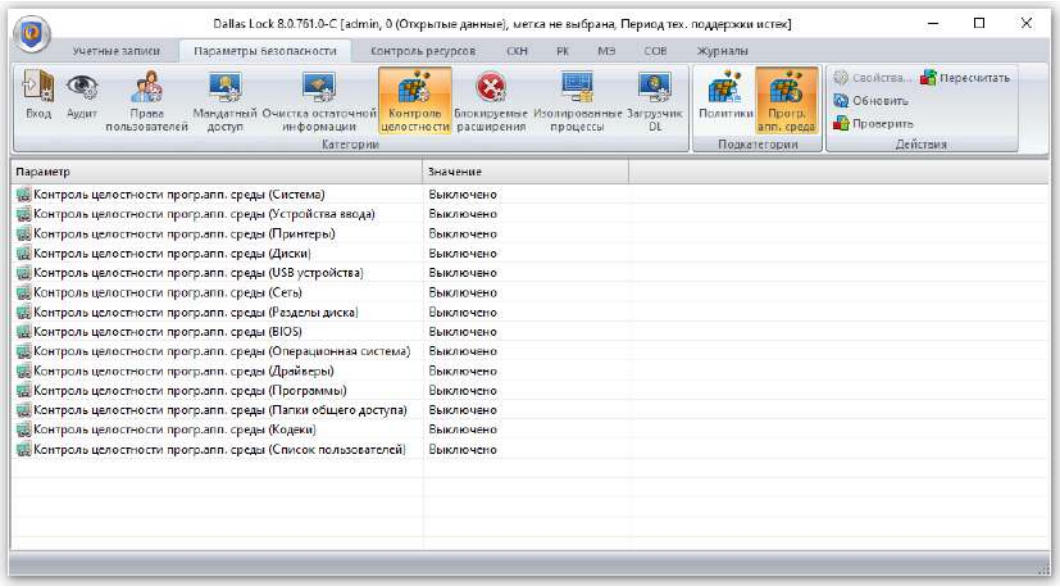


Рис. 173. Параметры программно-аппаратной среды

Для установки целостности параметров программно-аппаратной среды необходимо выделить параметр и нажать кнопку «Свойства». В окне редактирования параметров выбрать алгоритм, который будет использоваться при подсчете контрольных сумм, либо отключить контроль целостности данного параметра (рис. 174).

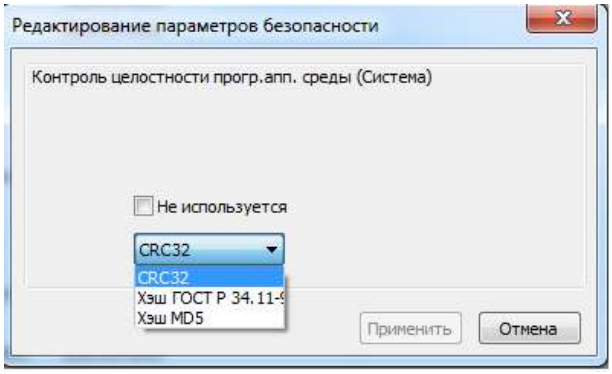


Рис. 174. Редактирование параметров безопасности

После нажатия кнопки «ОК» будет рассчитано значение контрольных сумм по алгоритму.

Для проверки значений целостности параметров следует нажать кнопку «Проверить». Система сверит установленные значения контрольных сумм параметров с текущими. В окне оболочки администратора у каждого параметра в списке появится значок, соответствующий значению целостности:

- — целостность не нарушена;
- — целостность нарушена;
- — целостность не установлена.

Чтобы установить новые значения целостности (пересчитать контрольные суммы параметров) следует нажать «Пересчитать», система пересчитает значения контрольных сумм для параметров, у параметров появятся соответствующие значки.

Моменты, когда осуществляется контроль целостности программно-аппаратной среды, также, как и для объектов ФС, определяется политиками целостности: «Проверять целостность программно-аппаратной среды при загрузке ОС», «Периодический контроль программно-аппаратной среды», «Контроль программно-аппаратной среды по расписанию». Также

контроль целостности осуществляется по команде администратора (в оболочке администратора кнопка «Проверить»).

Примечание. Расчет целостности программно-аппаратной среды по объективным причинам может занимать время. В связи с этим при включении контроля на какой-либо сегмент программно-аппаратной среды расчет эталонной контрольной суммы не производится. Он будет автоматически выполнен в момент первой проверки целостности. Таким образом, время на выполнение этой операции не отнимается у администратора без необходимости. Соответственно, если по каким-либо причинам есть потребность рассчитать эталонное состояние именно на текущий момент, следует сразу после назначения выполнить проверку целостности программно-аппаратной среды.

СЗИ Dallas Lock 8.0 контролирует следующие объекты программно-аппаратной среды:

Параметр	Что контролируется
Система	Контролируются порты, мониторы, шины, звуковые устройства и другие системные устройства
Устройства ввода	Контролируются подключенные устройства ввода на данном ПК: клавиатуры, мыши
Принтеры	Контролируется список всех установленных на ПК принтеров, факсов, МФУ и др. печатающих устройств
Диски	Контролируются контроллеры гибких дисков, дисководы и дисковые устройства
USB-устройства	Контролируются изменения в USB-контроллере, подключения и отключения USB-портов
Сеть	Контролируются сетевые подключения и сетевые карты
Разделы диска	Контролируются изменения разделов жесткого диска, форматирование диска, подключение новых дисков
BIOS	Контролируются изменения параметров BIOS
Операционная система	Контролируются изменения свойств ОС данного ПК: изменение имени, IP-адреса и пр.
Драйверы	Контролируется установка и удаление драйверов
Программы	Контролируется установка или удаление программ на данном ПК
Папки общего доступа	Контролируется создание или удаление папок общего доступа на данном ПК
Кодеки	Контролируется установка или удаление кодеков на ПК
Список пользователей	Контролируется список пользоват елей, созданных в локальной ОС

10 КОНТРОЛЬ УСТРОЙСТВ

Основной задачей функции контроля доступа к устройствам в СЗИ Dallas Lock 8.0 является возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Разграничение доступа и ведение аудита возможно, как для классов устройств, так и для конкретных экземпляров. К классу устройств на конкретном ПК может быть одновременно отнесено одно, несколько или ни одного устройств.

Чтобы произвести настройки доступа для контроля устройств, необходимо в оболочке администратора на вкладке основного меню «Контроль ресурсов» выбрать тип ресурса «Устройства» (рис. 175).

В основном окне отобразится дерево устройств, которое состоит из двух уровней иерархии: классов и индивидуальных устройств, которые входят в определенный класс. Если в класс входит несколько устройств, они отображаются последовательно.

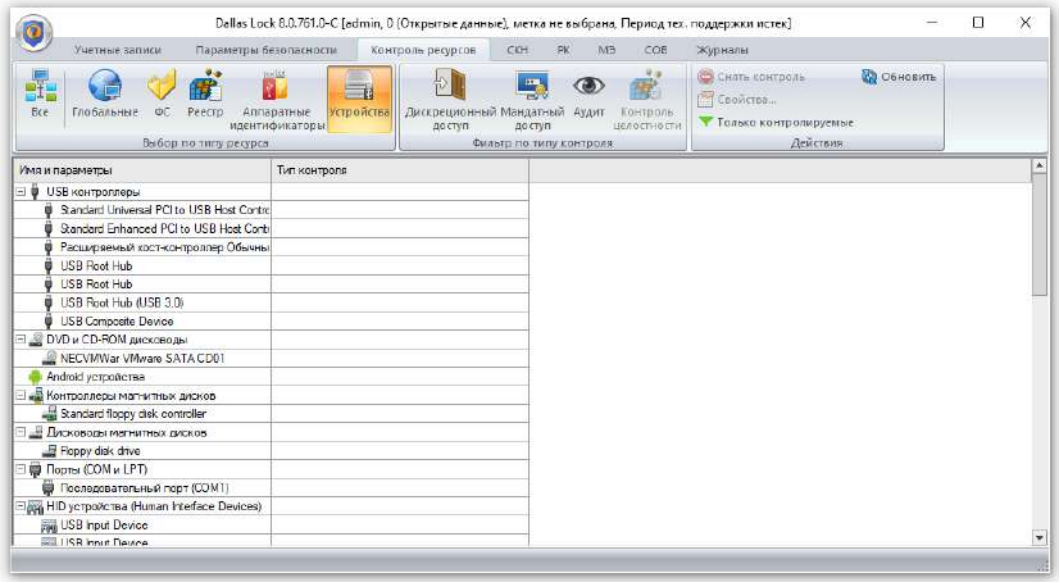


Рис. 175. Дерево классов и видов устройств

Список классов в Dallas Lock 8.0 фиксирован и одинаков для всех защищенных ПК. Список устройств на каждом ПК свой индивидуальный, он берется из локальной ОС.

Также возможно блокировать перенаправляемые по RDP протоколу (Remote Desktop Protocol) устройства.

Примечание. После назначения дискреционного доступа на «Перенаправленные по RDP устройства» администратору необходимо перезагрузить компьютер, чтобы назначенные права стали активными.

Примечание. Часть устройств ПК относится к системным, без которых работа компьютера невозможна (процессор, оперативная память, видеоадаптеры, мосты системной платы и т. д.). Разграничивать доступ к таким устройствам не имеет смысла, так как запрет доступа к ним приведет к тому, что пользователь не сможет загрузить систему. Поэтому Dallas Lock 8.0 такие устройства не контролирует.

Примечание. При настройке работы с USB-устройствами их можно подключать как напрямую через USB-порт, так и через интерфейсные модули типа Anywhere USB.

10.1 Полномочия на управление контролем устройств

Для того, чтобы иметь возможность управлять доступом к устройствам, пользователь должен иметь в СЗИ Dallas Lock 8.0 соответствующие права.

Для управления (назначения) дискреционным доступом к устройству учетная запись пользователя должна присутствовать в списке параметра «Ресурсы: Управление дискреционным доступом»

(«Параметры безопасности» → «Права пользователей»).

Для управления (назначения) мандатным доступом к устройству учетная запись пользователя должна присутствовать в списке параметра «Ресурсы: Управление мандатным доступом» («Параметры безопасности» → «Права пользователей»).

Если пользователю необходимо установить право только на просмотр уже установленных настроек доступа к устройствам, то его учетная запись должна присутствовать в списке параметра «Параметры безопасности: Просмотр».

Пользователь, установивший СЗИ, суперадминистратор, обладает данными правами по умолчанию. В то же время, пользователь, учетная запись которого присутствует в списке «Параметры безопасности: Управление» может назначать других пользователей для управления доступом к устройствам.

Подробнее о предоставлении полномочий см. «Полномочия пользователей на администрирование системы защиты».

10.2 Разграничение доступа к устройствам

Внимание! При настройке разграничения доступа к устройствам необходимо учесть следующие особенности:

1. В разных версиях ОС Windows в диспетчере устройств одно и то же физическое устройство может идентифицироваться по-разному. Это следует учитывать при определении прав доступа к устройству/классу устройств, особенно при централизованной настройке средствами СБ.

   Сотовые телефоны в зависимости от комплектации самого устройства могут определяться как беспроводное устройство, как USB-Flash накопитель, как набор портов, или даже как несколько устройств одновременно. В категорию «Беспроводные устройства» могут попадать устройства беспроводного доступа, такие как современные сотовые телефоны-модемы, в тоже время беспроводные адаптеры Wi-Fi обычно попадают в категорию «Сетевые адаптеры». Это связано с особенностью реализации самих устройств и их драйверов, и может быть установлено наверняка опытным путем.

2. Иногда некоторые устройства после их выключения могут потребовать перезагрузку компьютера для последующего включения. Это особенность конкретных устройств, которая будет проявляться и без Dallas Lock 8.0 (если, например, вручную запретить устройство через диспетчер устройств). Важно помнить об этом, особенно при назначении мандатных уровней для доступа к устройствам — устройство может не включиться после входа пользователя под «разрешенным» уровнем, и для включения устройства будет требоваться перезагрузка ОС.

3. При разграничении доступа к устройствам, отличным от COM/LPT-портов, запрет доступа действует на всех пользователей и устройство полностью отключается в случае его запрета. Отключенное устройство будет недоступно, в том числе, для учетной записи пользователя, выполнившего установку СЗИ, суперадминистратора.
4. Не рекомендуется глобально запрещать все USB-контроллеры, лучше выполнять блокировку на уровне конкретных контроллеров и устройств.
5. Запрещая использование некоторых устройств, например, USB-устройств ввода, можно лишиться возможности работать устройствами типа «мышь» и «клавиатура» и, соответственно, возможности отменить данную настройку на локально установленной СЗИ (тем не менее, по сети можно будет выполнить отмену такой настройки).
6. Важно помнить, особенно при настройке терминального сервера, что при назначении мандатного доступа к устройствам, устройства (кроме COM/LPT-портов) запрещаются, если в ОС зарегистрирована хотя бы одна сессия, которая является запрещенной для устройства. Например, если сетевой адаптер запрещен для работы в режиме «открытые данные», то пока на компьютере присутствует хотя бы одна сессия с открытыми данными, сетевой адаптер будет выключен. Вычисление эффективного состояния всех устройств в зависимости от настроек мандатного доступа и зарегистрированных в ОС сессий осуществляется в момент входа новой сессии и в момент завершения любой из сессий.

Для настройки прав доступа к классам устройств или устройствам необходимо выбрать соответствующий элемент в дереве устройств и нажать на кнопку «Свойства» на панели действий

(или выбрать данное действие в контекстном меню объекта).

Откроется окно редактирования дескриптора устройства, которое состоит из закладок: «Дискреционный доступ», «Мандатный доступ» и «Аудит доступа». В зависимости от политик безопасности необходимо выполнить установку прав доступа. Значки устройств и классов в дереве объектов, для которых назначены какие-либо права, будут выделены определенным образом.

В дереве устройств помимо элементов, отображающих устройства данного ПК присутствуют дополнительные классы устройств. Это — классы сменных накопителей и преобразованных сменных накопители (только для Dallas Lock 8.0 с модулем СКН). Настройки доступа и аудита для объектов данных классов устанавливаются по общим правилам, а также соответствуют глобальным одноименным дескрипторам в списке вкладки «Контроль ресурсов» → «Глобальные» (см. «Доступ к преобразованным накопителям», «Дискреционный доступ для глобальных параметров» и «Аудит для глобальных параметров»).

10.2.1 Дискреционный доступ к устройствам

Дискреционный принцип разграничения доступа к устройствам состоит из двух возможностей: доступ всех пользователей к данному устройству разрешен и доступ запрещен (рис. 176). Для некоторых классов устройств разграничение дискреционного доступа на уровне пользователей не доступно, т.е. возможности выбора учетных записей нет, кроме записи «Все».

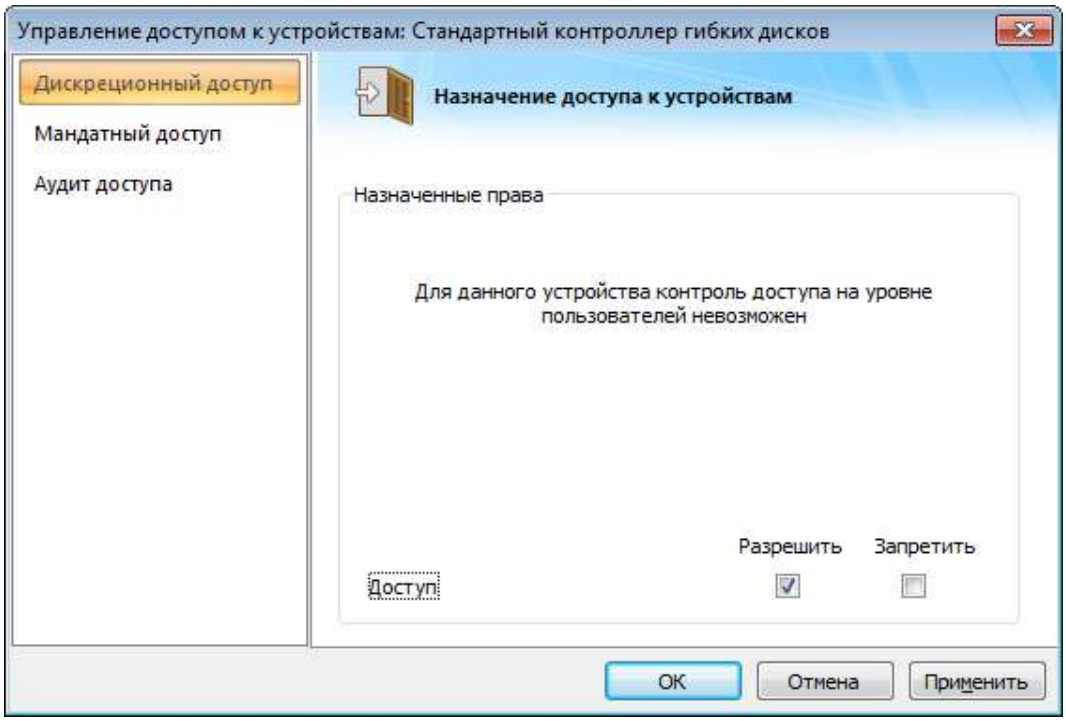


Рис. 176. Дескриптор дискреционного доступа к устройству

Принцип определения прав доступа пользователей к устройствам аналогичен Механизму определения прав доступа пользователя к ресурсам файловой системы:

1. Права, заданные для класса устройств, имеют более низкий приоритет, чем права, заданные для конкретного экземпляра.
2. Права, заданные для группы пользователей, имеют более низкий приоритет, чем права, заданные для пользователя (если доступно разграничение на уровне пользователей).
3. Если доступ к устройству не назначен ни классу, которому принадлежит устройство, ни самому устройству, то доступ разрешен.

10.2.2 Мандатный доступ к устройствам

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Подробнее о принципе мандатного разграничения доступа см. «Мандатный доступ». Установка мандатного доступа на устройство происходит путем определения уровней доступа и мандатных меток в дескрипторе объекта, для работы под которыми устройство должно быть доступно.

Для того, чтобы установить мандатный доступ на устройство, необходимо в окне дескриптора

доступа объекта на закладке «Мандатный доступ» поставить флаг в поле «Мандатный доступ включен», отметить мандатные уровни и добавить мандатные метки (рис. 177).

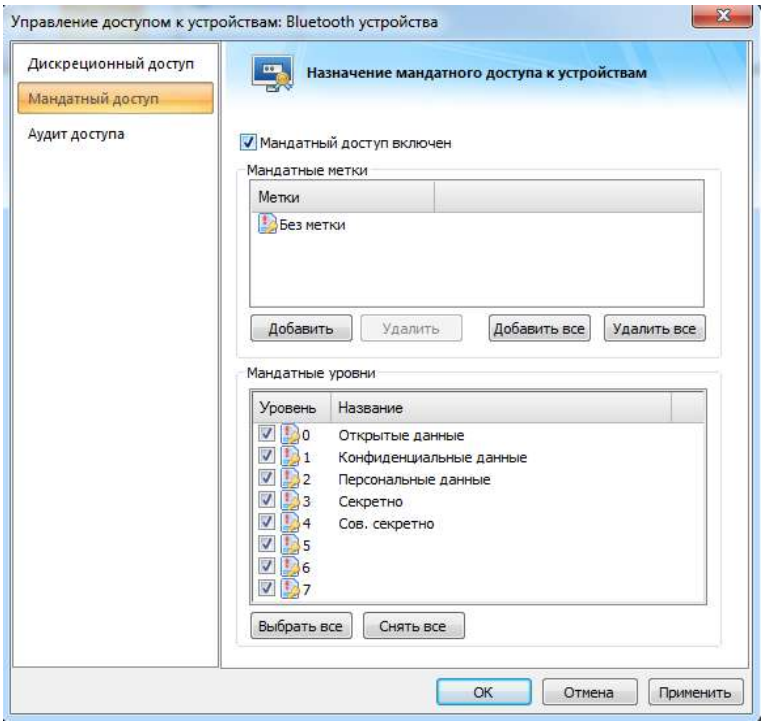


Рис. 177. Управление доступом к устройствам

Мандатный доступ можно назначить как для класса устройств, так и для отдельного экземпляра, при этом действует следующий принцип определения мандатного доступа:

- Если для устройства заданы некоторые мандатные уровни и мандатные метки, то доступ осуществляется в соответствии с ними.
- Если для устройства не заданы мандатные уровни и мандатные метки, то используются значения мандатного доступа класса устройств.
- Если и для класса устройств не назначены мандатные уровни и мандатные метки, то работать с устройством можно под всеми уровнями и метками.
- Сложения значений не происходит. Значения уровней устройства, если они заданы, «перекрывают» значения уровней класса. Например, если для класса значения состоят из уровней 0,1,2, а для устройства значения состоят из уровней 2,3, то действуют значения 2,3.

Примечание. Мандатный доступ можно назначить к классам устройств, контролирующимся через контроль устройств (кроме сменных накопителей, преобразованных накопителей и перенаправляемые по RDP устройства).

10.3 Аудит доступа к устройствам

Для назначения аудита событий доступа к устройствам в первую очередь необходимо включить два глобальных параметра безопасности «Аудит устройств» и «Журнал ресурсов» на вкладке основного меню «Параметры безопасности» → «Аудит» (значение «Вкл.»).

В окне редактирования дескриптора выбранного устройства необходимо выбрать закладку «Аудит доступа». Далее включить аудит устройства: поставить флаг в поле «Аудит включен» и выбрать из двух событий аудита: аудит успешных подключений устройства («Успех») или аудит неуспешных подключений («Отказ»).

Если для конкретного устройства не установлен аудит событий, то события аудита будут соответствовать значениям для класса, которому принадлежит данное устройство; если у класса устройств тоже не будут выбраны значения аудита, то аудит вестись не будет.

Аудит событий доступа к устройствам, а также аудит событий по настройке доступа ведется в журнале ресурсов (см. «Журналы»).

11 УДАЛЕННЫЙ ДОСТУП И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ

Если ЗАРМ входит в состав ЛВС, то информация, хранящаяся на этом компьютере, защищена от НСД по сети.

Возможны следующие ситуации:

1. Пользователь обращается к незащищенному Dallas Lock 8.0 компьютеру с компьютера, который защищен Dallas Lock 8.0.
2. Пользователь обращается к защищенному Dallas Lock 8.0 компьютеру с компьютера, на котором эта система не установлена (с незащищенного компьютера).
3. На компьютерах, с которого обращаются и к которому обращаются, установлена система защиты Dallas Lock 8.0.

Удаленный доступ защищенных компьютеров осуществляется независимо от редакций системы защиты Dallas Lock 8.0 «К» или «С».

11.1 Удаленный доступ к незащищенному компьютеру с защищенного

Данный случай ничем не отличается от случая, когда доступ осуществляется с незащищенного СЗИ компьютера на незащищенный компьютер.

11.2 Удаленный доступ к защищенному компьютеру с незащищенного

По умолчанию в системе Dallas Lock 8.0 на ЗАРМ предусмотрена зарегистрированная учетная запись пользователя *anonymous*.

Для того, чтобы был возможен доступ к защищенному СЗИ компьютеру по сети с незащищенного компьютера, учетная запись пользователя anonymous должна быть включена. Также нужно проследить, чтобы пользователю anonymous не был запрещен удаленный доступ. Все остальные права пользователя *anonymous* администратор определяет согласно проводимой политике безопасности.

Таким образом, со всех компьютеров, включенных в ЛВС, но не защищенных СЗИ Dallas Lock 8.0, можно будет обратиться к ЗАРМ и получить доступ к его ресурсам в рамках прав, установленных для учетной записи anonymous.

При попытке обратиться к ЗАРМ на экране может возникнуть сообщение об ошибке (рис. 178).

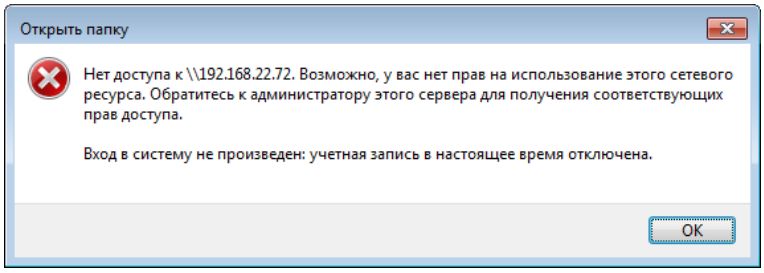


Рис. 178. Ошибка подключения к удаленному компьютеру

В этом случае следует внимательно проверить права, предоставленные учетной записи *anonymous*, в частности, право на удаленный доступ. Нужно внимательно просмотреть журнал входов, так как в нем можно увидеть причину отказа.

11.3 Удаленный доступ к защищенному компьютеру с защищенного

Для удаленного входа необходимо, чтобы у учетной записи, под которой входит пользователь, параметрами безопасности было предусмотрено соответствующее право: вкладка «Параметры безопасности» → категория «Права пользователей» → параметр «Удаленный вход: Разрешен».

При удаленном входе с ЗАРМ на ЗАРМ, пользователь осуществляет вход под учетной записью с таким же именем, под которым он работает. Если на удаленном компьютере нет учетной записью с таким же именем, у пользователя есть возможность войти под учетной записью *anonymous*, которая предусмотрена в системе защиты по умолчанию.

Примечание. Следует учитывать, что, если на ЗАРМ «Клиент» выполняется вход под пользователем «*user1*» и данный пользователь выполняет подключение сетевого диска через подключение к удаленной ЗАРМ «Сервер» под пользователем «*user2*», СЗИ на ЗАРМ «Сервер» будет фиксировать подключение именно пользователя «*user1*». Это обосновано тем, что работать с подключенным сетевым диском будет именно пользователь «*user1*».

В случае неудачного соединения, доступ к удаленному компьютеру осуществлен не будет, и система выдаст предупреждение.

На разных защищенных компьютерах в ЛВС одна учетная запись может быть зарегистрирована с разными правами. Когда происходит удаленный вход, права проверяются в соответствии с правами учетной записи удаленного компьютера.

Еще одним необходимым условием удаленного входа является следующее: если в свойствах учетной записи удаленного компьютера включен параметр «Запретить работу при нарушении целостности», то на удаленном компьютере целостность не должна быть нарушена.

Так же следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

11.4 Ключи защиты сетевого взаимодействия

Каждый защищенный СЗИ Dallas Lock 8.0 компьютер имеет ключ защиты сетевого взаимодействия. Данный параметр предназначен для усиления защиты сетевого взаимодействия между СБ и клиентом, а также между клиентом и модулем удаленного администрирования «Сетевой администратор» (см. «Сетевое администрирование»). Указанные виды сетевого взаимодействия возможны только при условии совпадения ключей защиты сетевого взаимодействия.

На всех защищенных компьютерах в ЛВС после установки СЗИ с файлом конфигурации по умолчанию зарегистрирован ключ защиты сетевого взаимодействия с пустым значением. Однако в системе реализована возможность изменения указанного ключа на компьютере. Для этого в оболочке администратора на вкладке «Параметры безопасности» в категории политик безопасности «Вход» необходимо выбрать и открыть параметр «Сеть: Ключ защиты сетевого взаимодействия» и заполнить требуемые поля (рис. 179).

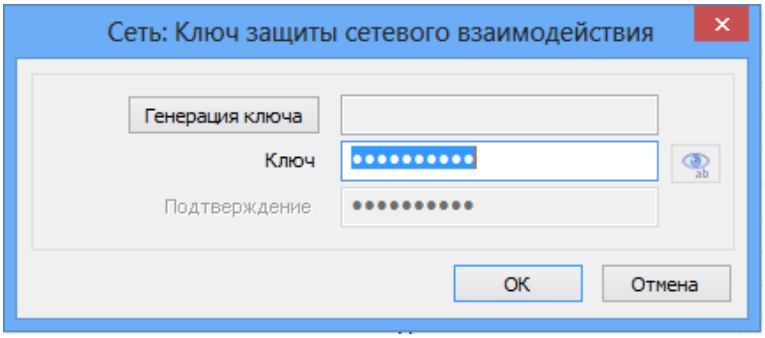


Рис. 179. Окно ввода нового ключа защиты сетевого взаимодействия

Рекомендуется вводить и изменять настройки ключей защиты сетевого взаимодействия только опытным специалистам, и только в тех случаях, когда это действительно необходимо. Так как неосторожная смена ключа доступа у одного ПК, может привести к тому, что удаленный доступ на него будет невозможен.

Для создания ключа защиты сетевого взаимодействия, отвечающего всем требованиям параметров безопасности, установленных системой защиты Dallas Lock 8.0, можно воспользоваться помощью генератора паролей системы защиты. Для этого следует нажать поле с надписью: «Генерация ключа». Система автоматически создаст уникальный ключ, значение которого необходимо ввести в поля «Ключ» и «Подтверждение».

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение в этом случае не потребуется и заблокируется.

Примечание. Политики сложности паролей распространяются и на установку значений для ключа защиты сетевого взаимодействия. Поэтому, чтобы была возможность задать пустое значение ключа защиты сетевого взаимодействия, необходимо, чтобы параметр «Пароли: минимальная длина» имел значение «Не используется».

11.5 Сетевое администрирование

Система защиты Dallas Lock 8.0 позволяет осуществлять сетевое (удаленное) администрирование параметров безопасности других компьютеров, на которых установлена система защиты. С помощью сетевого администрирования возможны те же действия, что и при локальном администрировании: создание, удаление, редактирование пользователей и групп; редактирование политик безопасности; просмотр, назначение, редактирование параметров доступа, контроля целостности, аудита объектов ФС; просмотр журналов и прочее.

Визуально процесс сетевого администрирования практически не отличается от процесса локального администрирования, так как запускается та же самая оболочка администратора, которая подключается не к локальному драйверу защиты, а к удаленному.

После установки системы защиты на компьютере в меню «Пуск» в группе программ Dallas Lock 8.0 появляется значок модуля удаленного администрирования «Сетевой администратор» (рис. 180).

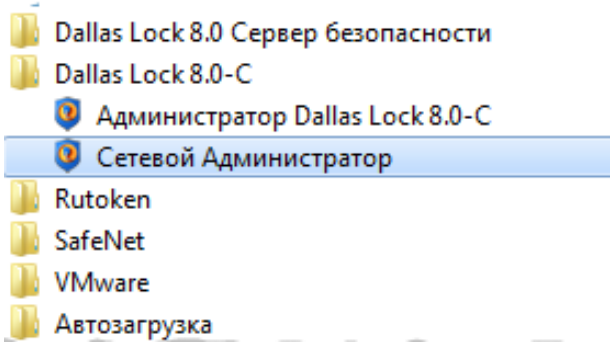


Рис. 180. Вызов удаленного администрирования СЗИ

Для осуществления сетевого администрирования на компьютерах, входящих в ЛВС, необходимо соблюдение следующих условий:

- На всех компьютерах, для которых предполагается сетевое администрирование, должна быть установлена СЗИ Dallas Lock 8.0.
- Для межсетевого взаимодействия на целевых компьютерах, защищенных Dallas Lock 8.0, должен быть открыт TCP/IP порт 17490.
- На всех компьютерах, для которых предполагается сетевое администрирование, должны быть установлены одинаковые ключи защиты сетевого взаимодействия (см. «Ключи защиты сетевого взаимодействия»).

Примечание. По умолчанию в системе защиты ключ защиты сетевого взаимодействия пустой, и если ни на одном из компьютеров он не изменялся, то специально для осуществления сетевого взаимодействия его вводить не следует.

- Пользователь, осуществляющий сетевое администрирование (удаленный администратор), должен быть зарегистрирован на всех компьютерах К1, К2, К3…Кn.
- Администратор должен обладать правом удаленного доступа на целевых компьютерах: вкладка «Параметры безопасности» → категория «Права пользователей» → параметр «Вход в ОС: удаленный» (в параметрах локально установленной СЗИ).
- На компьютерах К2, К3…Кn сетевому администратору должны быть предоставлены соответствующие полномочия на администрирование.
- Сетевое администрирование защищенных компьютеров осуществляется, независимо от редакций установленной системы защиты Dallas Lock 8.0 «К» или «С».

При соблюдении этих условий с компьютера К1 можно осуществлять сетевое администрирование компьютеров К2, К3…Кn. Для этого необходимо запустить модуль «Сетевой администратор» и в появившемся окне ввести имя удаленного компьютера и авторизационные данные учетной записи пользователя (рис. 181). Если администрирование удаленного ПК осуществляется под учетной записью текущего пользователя, то авторизационные данные можно не вводить, но отметить флагом поле «Использовать текущего пользователя».

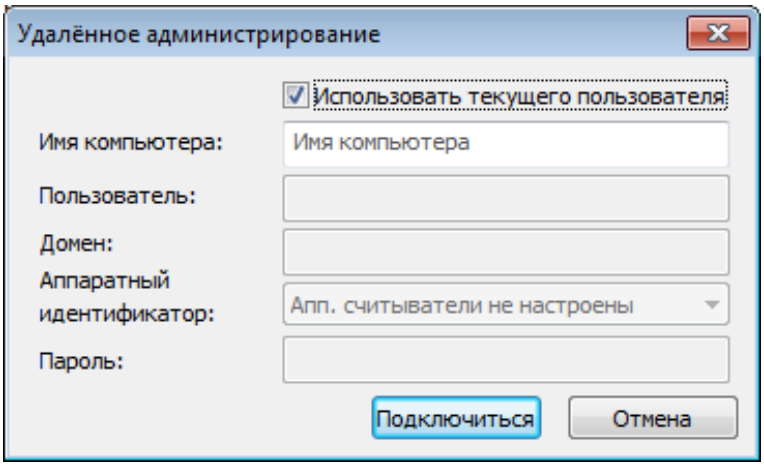


Рис. 181. Доступ к удаленному администрированию

Если имя и данные пользователя введены верно и все вышеперечисленные условия соблюдены, то на экране развернется оболочка администратора Dallas Lock 8.0 с параметрами удаленного компьютера, и пользователь получит возможность осуществлять администрирование в рамках, предоставленных ему на том компьютере полномочий.

В случае неудачного соединения, доступ к удаленному компьютеру осуществлен не будет, и появится предупреждение. В этом случае следует внимательно проверить выполнение условий осуществления удаленного администрирования.

В окне отображения текущих сессий на клиенте в оболочки администратора можно наблюдать появление новой записи о текущей сессии под учетной записью суперадминистратора с удаленного компьютера, (рис. 182).

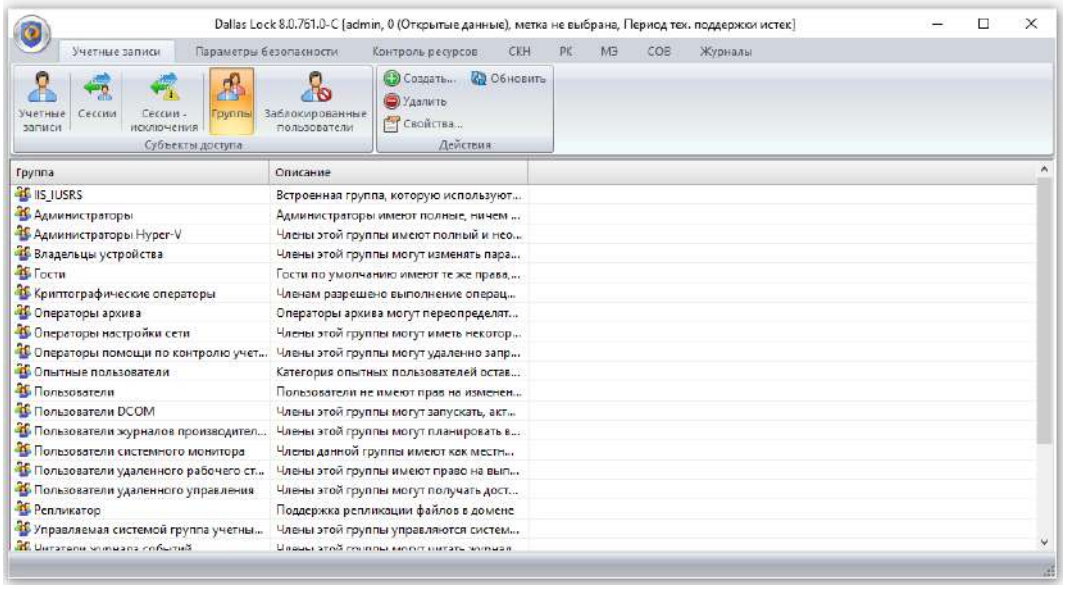


Рис. 182. Сессии пользователей при удаленном администрировании

В списке меню дополнительных функций оболочки администратора при удаленном администрировании компьютера появится функция принудительной перезагрузки удаленного компьютера (рис. 183).

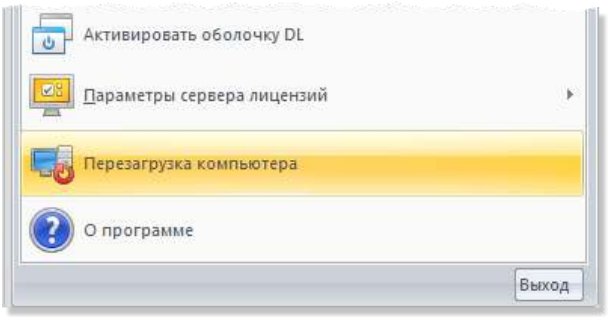


Рис. 183. Кнопка перезагрузки при удаленном администрировании

Однако функции «Тестирование функционала СЗИ» и «Зачистка диска» станут недоступны.

12 ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ

12.1 Прозрачное преобразование дисков

Данный механизм доступен только для Dallas Lock 8.0 редакции «С»

В состав системы защиты Dallas Lock 8.0-С входит механизм прозрачного преобразования жесткого диска уровня загрузочной записи. Прозрачное преобразование позволяет осуществить преобразование информации, хранящейся на локальных, а также съемных жестких дисках.

При попытке работы с преобразованным жестким диском в обход системы защиты Dallas Lock 8.0, например, при извлечении жесткого диска из одного ПК и подключении его к другому, данные будут защищены.

Прозрачное преобразование становится доступным после включения модуля загрузчика DL. При включении загрузчика DL выбирается алгоритм преобразования жесткого диска. Выбор алгоритма преобразования зависит от политик информационной безопасности, принятых в организации. Подсистема позволяет настраивать и размер преобразуемой части жесткого диска.

Примечание. Выполнять преобразование диска (полное или частичное), можно только убедившись, что сам модуль загрузчика DL корректно загружает ПК по PIN-коду.

Примечание. После инициации процесса преобразования необходимо дождаться его завершения. Отслеживать статус возможно через оболочку администратора.

Примечание. Система защиты Dallas Lock 8.0-С не поддерживает использование функции прозрачного преобразования системной области на виртуальных машинах VMWare и Hyper-V с UEFI и дисками GPT.

Для преобразования дисков необходимо:

1. Включить модуль загрузчика DL (см. «Загрузчик DL»).
2. Перейти на вкладку «Список зон» («Параметры безопасности» → «Загрузчик DL» → «Список зон») и нажать действие «Добавить зону»[11] (рис. 184).

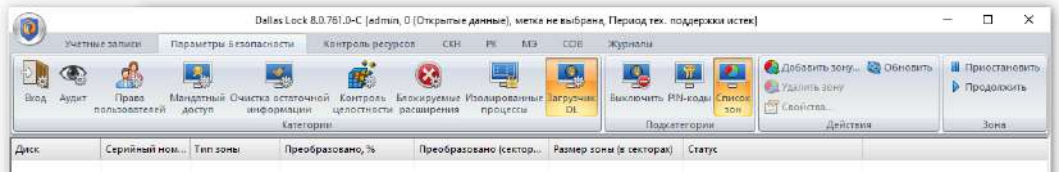


Рис. 184. Добавление зоны прозрачного преобразования диска

Откроется окно создания зоны жесткого диска для прозрачного преобразования (рис. 185).

[11] Вызов данной функции также возможен из контекстного меню.

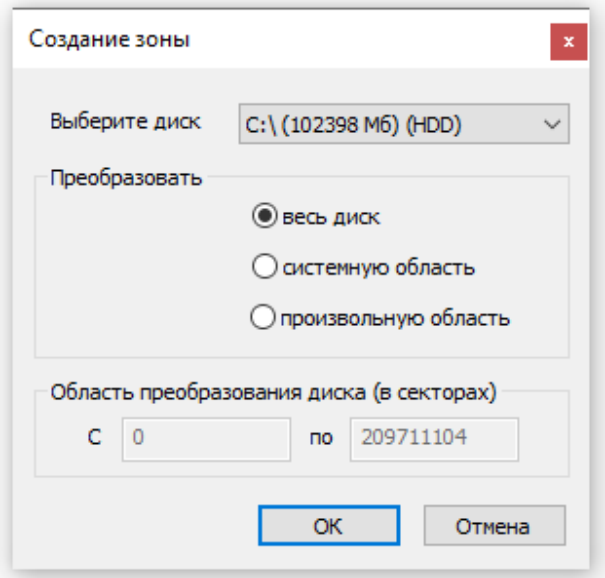


Рис. 185. Параметры создания зоны преобразования

3. В данном окне необходимо выбрать диск. Указать область выбранного диска, которую необходимо преобразовать:
   - весь диск;
   - системную область диска;
   - произвольную область (с указанием размера).
4. Нажать кнопку «OK» и подтвердить операцию. После чего сразу начнется процесс преобразования выбранной зоны жесткого диска.

В окне хода выполнения процесса преобразования его можно приостановить и продолжить, выбрав запись о процессе в списке основного окна и нажав кнопку на панели действий.

После преобразования на данной вкладке оболочки администратора в списке процессов появится запись о параметрах данного процесса преобразования.

Далее работа с данными жесткого диска, имеющего преобразованные области, на защищенном Dallas Lock 8.0 компьютере никак не будет отличаться от работы с непреобразованными областями.

Чтобы удалить зону преобразования, т.е. произвести восстановление жесткого диска или его части, необходимо выделить его в списке и нажать кнопку «Удалить зону» на панели действий, далее подтвердить операцию. Запустится процесс обратного преобразования, который также можно приостановить и возобновить позже.

Примечание. Выбор действия «Аварийное восстановление» клавишей F2 при входе в загрузчике необходимо для обратного преобразования дисков до этапа загрузки ОС и доступно только с PIN-кодом администратора. Восстановление диска на данном этапе является необходимым для восстановления работоспособности компьютера при сбое системы защиты (см. «Восстановление компьютера при сбое системы защиты»).

12.2 Преобразование данных в файл-контейнер

Имеющиеся на защищенном ПК файлы или папки могут быть преобразованы в файл-контейнер с помощью системы защиты Dallas Lock 8.0 с использованием ключевой информации (пароля и (или) аппаратного идентификатора). Преобразованные файлы или папки могут быть обратно преобразованы в исходные данные, при условии верного ввода ключевой информации.

Таким образом, содержимое файлов-контейнеров становится недоступным на ПК, не защищенном СЗИ Dallas Lock 8.0, и также недоступным на ПК, защищенном СЗИ Dallas Lock 8.0, но в случае введения неверной ключевой информации при обратном преобразовании.

Преобразованные данные хранятся в файле-контейнере, который может быть безопасно передан по незащищенным сетевым каналам, электронной почте или с помощью сменного накопителя.

Для восстановления этих данных необходим пароль и аппаратный идентификатор, используемый при преобразовании.

Следует отметить, что права на использование данной функции конкретному пользователю для конкретного файла определяются параметрами безопасности, установленными администратором безопасности. Если у пользователя данные права отсутствуют (установлен флаг «Запретить» в поле «Запись» в дескрипторе объекта для пользователя или группы), то попытка преобразования и

зачистки исходных данных будет неуспешной, и появится предупреждающее сообщение.

12.2.1 Преобразование объектов ФС

Чтобы преобразовать объект ФС, необходимо выбрать в контекстном меню соответствующего файла или папки пункт «DL80: Преобразование» (рис. 186).

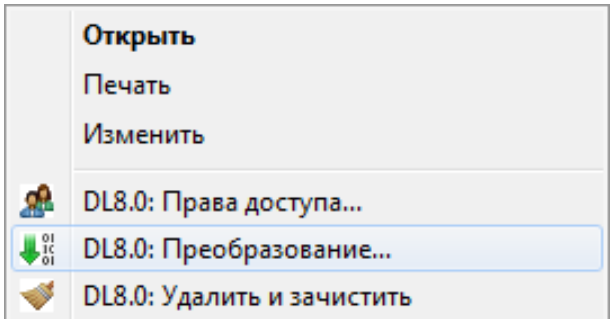


Рис. 186. Контекстное меню

На экране появится окно модуля преобразования объекта ФС, в котором необходимо указать данные и параметры. Окно модуля преобразования объекта ФС содержит следующие поля для заполнения:

Наименование поля	Описание
Результат преобразования	Имя и путь к будущему файлу-контейнеру (по умолчанию, оно формируется из имени преобразовываемого объекта с добавлением специального расширения, в текущей папке). Имя будущего файла и путь к нему можно прописать вручную. Выбор другой папки можно осуществить с помощью кнопки «Обзор…»
Алгоритм преобразования	Операции по настройке алгоритма преобразования. По умолчанию используется встроенный в Dallas Lock 8.0 алгоритм.
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей (см. «Настройка параметров входа»). Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные
Аппаратная идентификация	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка. Если аппаратный идентификатор не указывать, преобразование происходит только по паролю
Уровень доступа	Поле является информационным. При преобразовании объекта (только для Dallas Lock 8.0 редакции «С») ему присваивается мандатный уровень и мандатная метка текущего уровня доступа пользователя. При обратном преобразовании в этом же поле — уровень доступа, который назначен при прямом преобразовании. Для объектов, в СЗИ редакции «К» документы имеют уровень доступа «0»
Зачистить исходные файлы	Выбор операции по зачистке исходных данных после получения преобразованного файла-контейнера
Комментарий	Комментарий к файлу-контейнеру (он не преобразуется, является необязательным и доступен без пароля)

После заполнения всех необходимых параметров необходимо нажать «Преобразование».

Примечание. Преобразование может производиться без задания пароля, если будет использован аппаратный идентификатор. Значение пароля, который используется при преобразовании, должно соответствовать установленным политикам сложности паролей.

Процесс преобразования будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса будут выведены следующие сообщения: «Исходный файл удален!» (если операция по зачистке исходных файлов была включена) и сообщение об успешном преобразовании. Файл–контейнер с расширением *.dlcf появится в указанной папке (рис. 187).

Рис. 187. Ярлык преобразованного файла

Возможно одновременное преобразование сразу нескольких файлов. Для этого их нужно одновременно выделить (с помощью Ctrl) и, щелкнув правой кнопкой мыши, выбрать в контекстном меню пункт «DL8.0: Преобразование». Будущий файл-контейнер будет содержать все выбранные файлы. При этом имя и путь к будущему файлу-контейнеру будет по умолчанию состоять из имени первого из выбранных файлов. Преобразование завершится сообщениями системы с указанием количества файлов.

Примечание. При преобразовании и последующем обратном преобразовании папки, содержащей не только файлы, но и вложенные папки происходит следующее: если исходная папка содержит пустую подпапку (без файлов), то при преобразовании она удаляется. Соответственно и обратно — преобразованная структура вложенных папок будет отличаться от исходной.

12.2.2 Обратное преобразование объектов ФС

В окне модуля преобразования объекта всегда присутствует кнопка, которая может переключить окно в режим обратного преобразования. Выбрать и открыть файл-контейнер в данном окне можно с помощью кнопки проводника  или двойным нажатием значка преобразованного объекта.

Появится окно, подобное тому, что и при преобразовании, в котором нужно ввести параметры восстановления: папку для восстановления и пароль, а также выбрать предъявленный аппаратный идентификатор.

Отмеченное флагом поле «Зачистить исходные файлы» активирует операцию по удалению исходного файла-контейнера.

В этом же окне будет выведен комментарий к файлу-контейнеру, общее количество файлов и папок, содержащихся в нем, их общий размер, который определила СЗИ. Уровень доступа объекта будет тем, который присвоен объекту при преобразовании (только для Dallas Lock 8.0 редакции «С»).

После ввода параметров восстановления и нажатия кнопки «Обратное преобразование» будет произведено восстановление информации. По окончании появится сообщение о подтверждении удаления исходного файла-контейнера и сообщение об удачном завершении процесса (рис. 188).

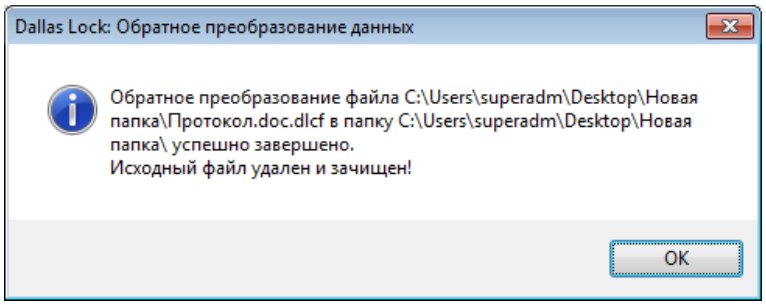


Рис. 188. Подтверждение успешного обратного преобразования файла

Преобразованные файлы-контейнеры, созданные в других версиях Dallas Lock, также можно обратно преобразовать в исходные данные, так как формат совместим. При этом необходимо учесть следующее:

Условие	Результат
Преобразованный архив в Dallas Lock 8.0 редакции «С»	может быть обратно преобразован в Dallas Lock 8.0 редакции «С», а также в Dallas Lock 8.0 редакции «К» — но при условии у архива уровня доступа равным нулю («открытые данные») и без мандатной метки

Условие	Результат
Преобразованный архив в Dallas Lock 8.0 редакции «К»	может быть обратно преобразован в Dallas Lock 8.0 редакций «К» и «С»
Преобразованный архив в Dallas Lock 7.7	может быть обратно преобразован в Dallas Lock 8.0 редакций «К» и «С»

12.3 Преобразованные файл-диски

Для безопасности хранения и обработки информации в Dallas Lock 8.0 реализован механизм создания таких контейнеров информации, при работе с размещенными на которых объектами ФС параллельно работе и не заметно для пользователя выполняется преобразование информации. Данные контейнеры называются преобразованные файл-диски.

Особенностью данного механизма является то, что данные файл-диски могут подключаться (монтироваться и демонтироваться) в ОС Windows как логические диски и иметь свою букву диска и определенный объем. В то же время информация на таком диске будет преобразованной и подключение диска для работы с ним пользователем может быть произведено только на ПК, защищенном Dallas Lock 8.0, и только с указанием ключевой информации.

12.3.1 Создание преобразованного файл-диска

Создавать преобразованные файл-диски могут пользователи, обладающие следующим правом: разрешающее право «Изменение содержимого» для глобального дескриптора «Параметры преобразованных файл-дисков по умолчанию».

Для того, чтобы создать преобразованный файл-диск, необходимо в меню значка блокировки ПК на панели задач выбрать пункт меню «Создать преобразованный файл-диск» (рис. 189).

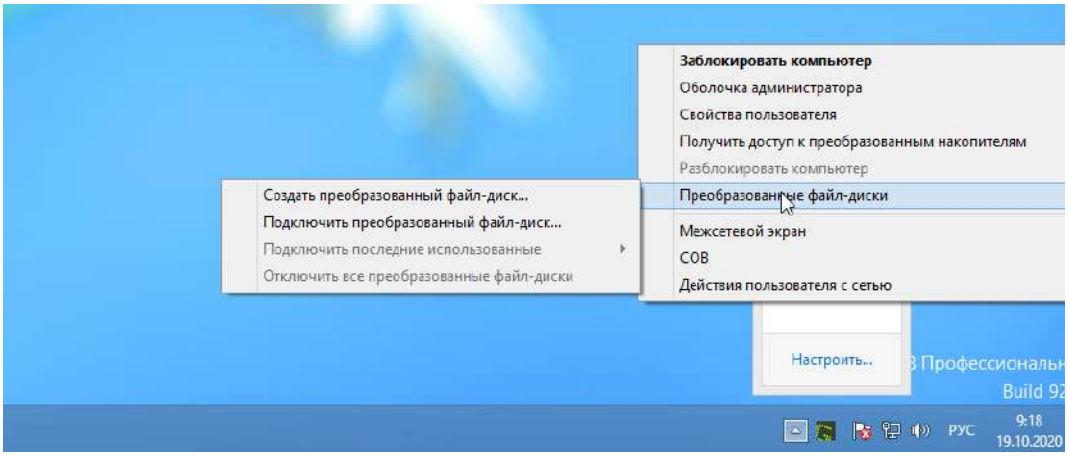


Рис. 189. Выбор пункта меню для создания преобразованного файл-диска

На экране появится окно свойств создаваемого файл-диска, в котором необходимо указать следующие параметры преобразования:

Наименование поля	Описание
Файл-диск	Путь, по которому будет сохранен создаваемый файл-диск и его имя
Название	Описание для создаваемого файл-диска (не обязательное поле)
Размер файл-диска	Необходимо указать оптимальный объем создаваемого файл-диска в МБ (учитывая наличие необходимого места на физическом диске ПК)
Буква диска	Необходимо определить букву логического диска для монтирования в ОС (букву диска можно выбрать и во время подключения файл-диска)
Подключить после создания	Отмеченное поле позволяет автоматически монтировать данный созданный файл-диск в качестве логического дичка в ОС и осуществлять на нем работу текущему пользователю

Наименование поля	Описание
Алгоритм преобразования	Операции по выбору и настройке алгоритма преобразования, которым будет преобразовываться информация при работе в данном файл-диске. По умолчанию используется встроенный в Dallas Lock 8.0 алгоритм преобразования
Аппаратный идентификатор	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка (также необходимо предварительно зарегистрировать в СЗИ считыватели). Если аппаратный идентификатор не указывать, то преобразование будет происходить только по паролю
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей (см. «Настройка параметров входа»). Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные

После заполнения всех необходимых параметров необходимо нажать «Создать».

После успешного создания пользователю будет выведено сообщение о том, что создан преобразованный файл-диск и, если было отмечено подключение, подключен как логический диск с указанной буквой диска.

Созданный таким образом файл будет иметь расширение *.dlpfd и иметь определенный значок (рис. 190).

Рис. 190. Значок созданного преобразованного файл-диска

После создания изменить название, размер, алгоритм преобразования и свойства для объекта файл-диск уже невозможно.

12.3.2 Работа на преобразованном файл-диске

Для работы с преобразованным файл-диском необходимо подключить такой диск в ОС и зайти на логический диск, появившийся в проводнике Windows.

Если у пользователя есть разрешение на работу с преобразованными файл-дисками, то ему будет доступен пункт «Преобразованные файл-диски» в меню значка блокировки ПК на панели задач. Для подключения файл-диска необходимо выбрать данный пункт меню или просто дважды кликнув кнопкой мыши на значке самого файл-диска. Включение также доступно из контекстного меню значка самого файл-диска.

В появившемся диалоговом окне при подключении файл-диска необходимо заполнить ключевую информацию:

- выбрать путь к файл-диску;
- указать букву, под которой он будет монтирован как логический диск в ОС;
- предъявить аппаратный идентификатор, если он был назначен;
- ввести пароль.

После нажатия кнопки «Подключить», если введенные данные были корректны, файл-диск подключиться и отобразиться в проводнике как логический диск с присвоенной ему буквой диска.

Пользователь может работать с таким диском в штатном режиме, но в то же время вся информация на нем является преобразованной, преобразование же выполняется по установленному алгоритму в процессе самой работы. Пользователь может размещать, создавать, изменять файлы на преобразованном файл-диске, копировать их с него. Для пользователя подключенный файл-диск в своей работе ничем не отличается от любого другого диска.

В меню «Преобразованные файл-диски» значка блокировки на панели задач также имеется пункт, позволяющий подключить последние использованные файл-диски — в выпадающем списке отображается список из 10 последних файл-дисков.

Чтобы отключить конкретный преобразованный файл-диск или все подключенные на данном ПК необходимо выбрать соответствующие пункты в меню «Преобразованные файл-диски». Отключение также происходит после выключения или перезагрузки ПК.

Преобразованный файл-диск может быть перемещен на другой защищенный ПК. В этом случае такой диск должен успешно подключаться в ОС, при условии ввода корректной ключевой информации и установке используемого встроенного алгоритма преобразования. В то же время, дескриптор (права доступа и аудит), назначенный на преобразованный файл-диск, при его перемещении не сохранится.

12.3.3 Доступ к преобразованным файл-дискам

Кроме того, с помощью параметров безопасности можно определить, какие пользователи могут работать с преобразованными файл-дисками и с какими правами, а какие нет. Для этого используется настройка глобальных дескрипторов: «Параметры ФС по умолчанию», «Параметры преобразованных файл-дисков по умолчанию» и настройка дескриптора объекта.

Настройка доступа и ведения аудита событий осуществляются в соответствии с описанием в разделах «Дискреционный доступ для глобальных объектов» и «Аудит для глобальных объектов».

Если дескриптор «Параметры преобразованных файл-дисков по умолчанию» не настроен, то настройки такого дескриптора будут наследоваться от глобального дескриптора «Параметры по умолчанию».

При настройке прав доступа необходимо учесть следующее:

- Для создания файл-дисков и работы с ним необходимо, чтобы пользователь имел разрешающее право «Изменение содержимого».
- Для просмотра содержимого преобразованных файл-дисков необходимо, чтобы пользователь имел разрешающее право «Обзор папки».
- Для запуска приложения необходимо, чтобы пользователь имел разрешающее право «Выполнение вложенных объектов».

На расположенные в преобразованном файл-диске объекты ФС (файлы, папки) назначить дескриптор безопасности нельзя.

Операции по работе с преобразованными файл-дисками и настройкой прав доступа на управление преобразованными файл-дисками фиксируются в журналах информационной безопасности СЗИ «Dallas Lock» 8.0.

13 СИСТЕМА КОНТРОЛЯ НАКОПИТЕЛЕЙ

В СЗИ Dallas Lock 8.0 в формате двух отдельных модулей реализована СКН, которые предназначены для контроля подключения съемных машинных носителей информации и контроля отчуждения (переноса) информации на информации со съемных машинных носителей информации.

Модуль СКН уровня контроля подключения съемных машинных носителей информации в составе СЗИ НСД Dallas Lock 8.0 позволяет разграничивать доступ пользователей информационной системы к сменным накопителям — осуществляет контроль подключения накопителей. Обеспечивает контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации.

Модуль СКН уровня отчуждения (переноса) информации в составе СЗИ НСД Dallas Lock 8.0 — совместное решение компаний «Конфидент» и «Актив-софт», сертифицированное ФСТЭК России на соответствие требованиям к СКН[12].

Модуль СКН уровня отчуждения позволяет легитимно переносить конфиденциальную информацию на идентификаторы Рутокен ЭЦП 2.0 Flash со встроенной энергонезависимой памятью. Данные идентификаторы могут быть использованы и для аутентификации пользователя в информационной системе. В основе подхода лежит «прозрачное» для пользователя преобразование информации при ее чтении и записи на Рутокен ЭЦП 2.0 Flash. Ключи преобразования недоступны пользователю информационной системы, что закрывает проблему со внутренним нарушителем. Доступ к информации возможен только на определенных АРМ, разрешенных администратором информационной безопасности. Все прочие сменные накопители не могут быть использованы. Дополнительно на каждый накопитель возможно установить пароль пользователя.

Сервер безопасности Dallas Lock и Единый центр управления Dallas Lock в рамках ДБ позволяют централизованно управлять ключами преобразования и разграничивать доступ пользователей к накопителям. Если в организации несколько администраторов ИБ, то существует отдельная роль по централизованному управлению накопителями для разграничения доступа привилегированных пользователей к настройкам системы защиты.

13.1 Права доступа к сменным накопителям

Чтобы назначить права доступа к конкретному накопителю, необходимо подключить этот накопитель к соответствующему порту ПК (если это USB-Flash накопитель) или вставить его в привод CD-ROM (в случае компакт-диска). Далее необходимо найти объект, соответствующий накопителю, с помощью проводника Windows Explorer и в контекстном меню объекта выбрать пункт «DL8.0: Права доступа» или выбрать объект в дереве устройств на вкладке «Контроль устройств». Дальнейшая настройка прав доступа ничем не отличается от настройки доступа к объектам ФС (см. «Разграничение доступа к объектам ФС»).

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность назначения мандатных уровней на сменный накопитель для отдельных пользователей или групп пользователей.

При этом в список контролируемых объектов эти накопители занесутся без буквы диска, а в специальном формате, в который входит тип накопителя и его уникальный номер. («Flash(XXXXXXXXXXX):\», «FDD(XXXXXXX):\», «CD(XXXXXXX):\»).

Для USB-Flash накопителей номер высчитывается как 32-битный хэш от пути к параметрам накопителя в реестре. Для дискеты или компакт-диска — это серийный номер тома. Поэтому, если при следующем подключении ОС назначит ему другую букву диска, права все равно будут контролироваться.

В окне категории «Сменные накопители» («СКН» → «Сменные накопители») контроля ресурсов формируется список всех установленных дескрипторов на сменные накопители, в том числе права доступа (дискреционный и мандатный доступ), назначенный аудит и установленный контроль целостности (рис. 191).

[12] Методические документы «Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты ИТ.СКН.Н4.ПЗ» (ФСТЭК России, 2014), «Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации второго класса защиты ИТ.СКН.Н2.ПЗ» (ФСТЭК России, 2014).

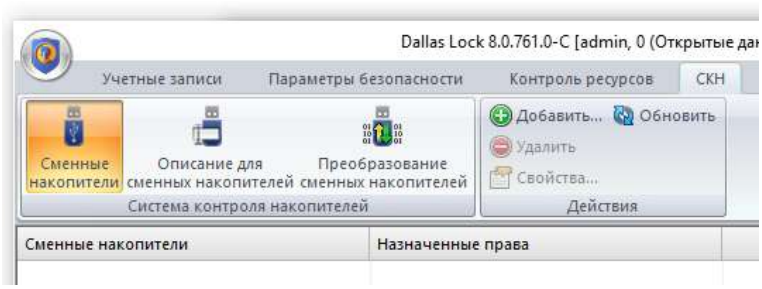


Рис. 191. Окно дескрипторов сменных накопителей

Действие «Добавить…», доступное в категории «Сменные накопители», позволит открыть проводник для выбора ресурса именно на сменных накопителях, установленных в ОС.

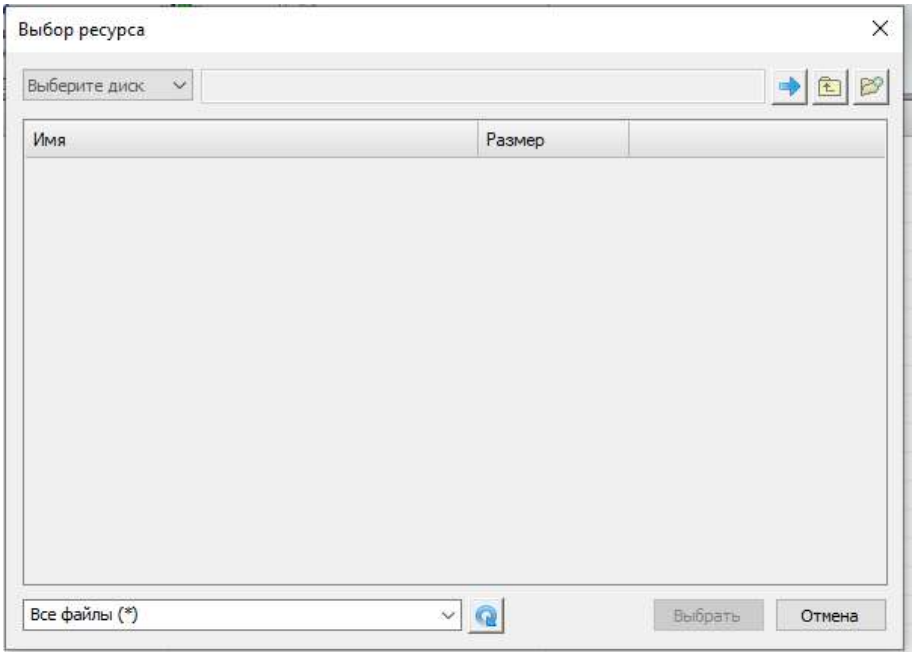


Рис. 192. Добавление сменного накопителя

После выбора необходиммого накопителя появится окно «Безопасность» для настройки доступа к накопителю.

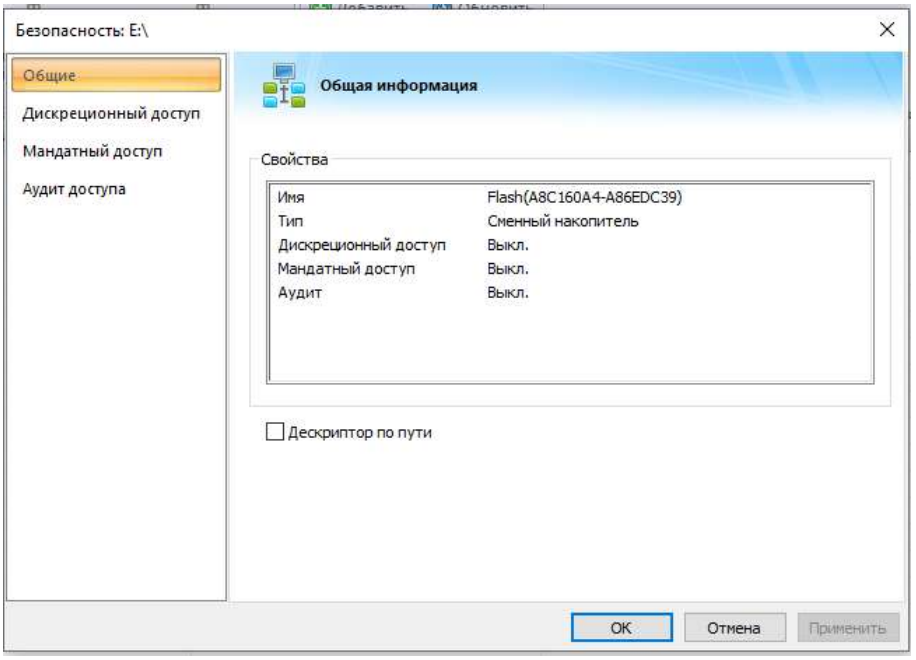


Рис. 193. Настройка безопасности для сменного накопителя

Существует возможность разграничить глобальный доступ к сменным накопителям или преобразованным сменным накопителям. Список глобальных параметров расположен на вкладке «Контроль ресурсов» → «Глобальные».

Если определенному пользователю в глобальном параметре «Параметры открытых сменных дисков по умолчанию» запретить все действия, то этот пользователь не сможет работать ни с одним открытым сменным накопителем. Если в глобальном параметре «Параметры открытых сменных накопителей по умолчанию» запретить все действия для группы «Все», в этом случае с открытыми сменными накопителями не сможет работать ни один из пользователей (за исключением пользователя, установившего СЗИ, суперадминистратора).

Если же после этого необходимо разрешить пользователю работу с преобразованными сменными накопителями, нужно в глобальных параметрах «Параметры преобразованных сменных накопителей по умолчанию» разрешить пользователю все операции. В результате этот пользователь не сможет работать с открытыми сменными накопителями, но будет иметь полный доступ к преобразованным сменным накопителям.

13.2 Описание для сменных накопителей

Для упрощения контроля большого количества сменных накопителей в СЗИ Dallas Lock 8.0 имеется возможность задавать свое описание для отдельно взятого сменного накопителя. Описание сменного накопителя позволяет заменить установленным названием серийный номер для работы с накопителем в СЗИ.

Для того, чтобы назначить описание для сменного накопителя, необходимо предъявить накопитель на ПК, в оболочке администратора на вкладке «СКН» выделить категорию «Описание для сменных накопителей» и нажать «Добавить» на панели действий.

В появившемся окне выбрать накопитель из выпадающего списка и ввести описание для накопителя (рис. 194). В выпадающем списке будут отображаться только те накопители, для которых описание еще не назначено. Чтобы изменить уже установленное описание, необходимо выделить объект в списке основного окна и нажать «Свойства», либо вызвать окно редактирования описания двойным кликом мыши по объекту.

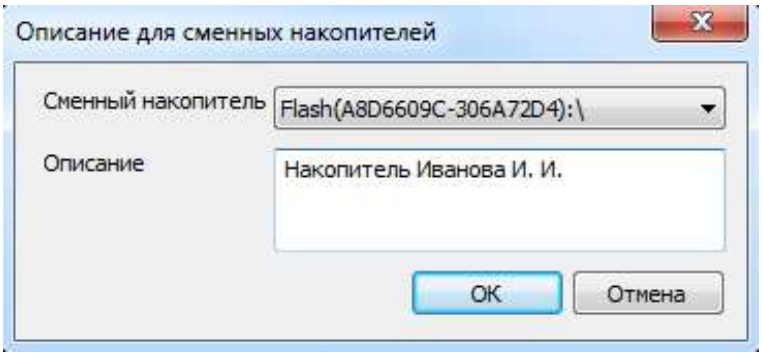


Рис. 194. Окно описания сменных накопителей

После этого при назначении прав доступа, контроля целостности или аудита для объектов ФС на данном накопителе в оболочке администратора в списках с дескрипторами накопитель будет отображаться под установленным описанием (рис. 195).

При просмотре устройств на вкладке «Контроль устройств» текст наименования добавленного сменного накопителя изменится на его описание.

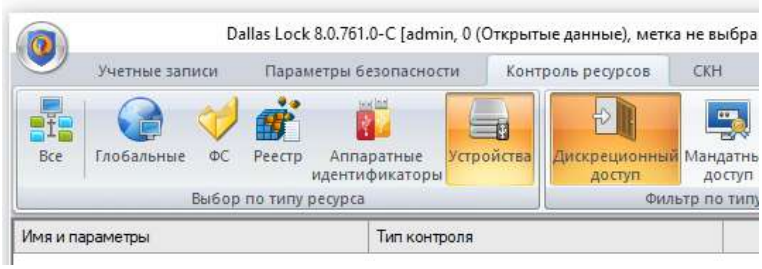


Рис. 195. Отображение сменных накопителей

13.3 Преобразование сменных накопителей

В системе защиты Dallas Lock 8.0 реализована возможность преобразования сменных накопителей. Преобразование сменных накопителей может быть использовано, например, при передаче секретных документов между автономными рабочими станциями.

Данная функция представляет собой создание с помощью ключа преобразования такого накопителя, с информацией на котором работа возможна строго на рабочих станциях, защищенных Dallas Lock 8.0, при условии наличия и совпадения ключа преобразования.

Понятие «преобразование сменных накопителей» подразумевает, что данный накопитель при подключении его к ПК будет отмечен в СЗИ таким образом, что вся информация на нем при ее обработке (создании и изменении файлов) будет автоматически преобразована.

Примечание. Преобразование сменных накопителей доступно только для тех устройств, которые распознаются ОС как сменный/съемный (removable) (USB-Flash накопители, карты памяти, Floppy-диски и прочие). Жесткие диски, подключаемые через устройство Mobile Rack или USB-порт, физически являются сменными, но логически для ОС являются фиксированными. На такие диски данная функция не распространяется.

В отличие от функции прозрачного преобразования фиксированных дисков (см. «Прозрачное преобразование дисков»), в которой возможен выбор областей и размера преобразовываемой области диска, преобразование сменных накопителей происходит только полностью.

Преобразование сменных накопителей осуществляется через оболочку администратора: вкладка «СКН» → категория «Преобразование сменных накопителей» (рис. 196).

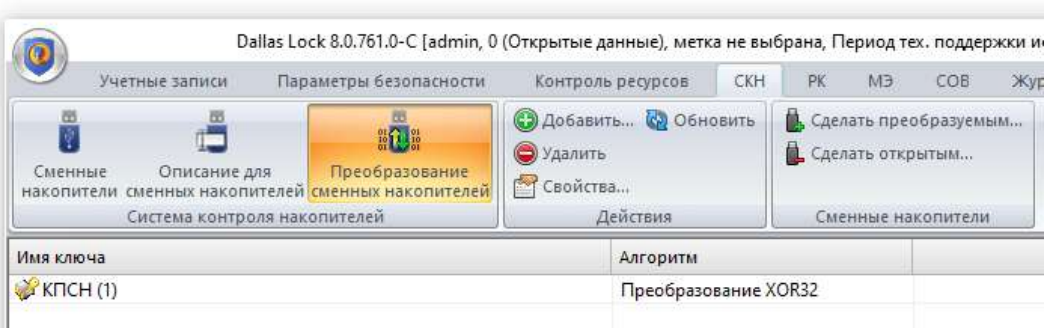


Рис. 196. Преобразование сменных накопителей

Создавать ключи преобразования, выполнять преобразование сменных накопителей могут только пользователи с правом «Параметры безопасности: Управление» (см. «Полномочия на управление параметрами безопасности»).

13.3.1 Создание ключей преобразования

Для создания преобразованных сменных накопителей необходимо наличие ключа преобразования. Чтобы создать ключ преобразования, необходимо нажать «Добавить» на панели действий. Появится окно ввода параметров ключа преобразования:

Наименование поля	Описание
Имя ключа	Имя ключа предлагается по умолчанию «КПСН» — ключ преобразования сменных накопителей. Его можно изменить. Имя ключа должно быть уникальным, создание двух ключей с одинаковыми именами невозможно
Ключ отключен	Определяет активность ключа преобразования
Доступ к накопителю по паролю	Определяет необходимость предоставления пароля для доступа к накопителю. Функциональная возможность доступна в случае приобретения лицензии на модуль «Средство контроля съемных машинных носителей информации»
Алгоритм	Алгоритм преобразования
Идентификатор	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка (предварительно зарегистрировав в СЗИ считыватели идентификатора, как и для любого другого действия с идентификаторами, см. «Настройка считывателей аппаратных идентификаторов»). Если аппаратный идентификатор не указывать, то преобразование происходит только по паролю
Пароль ключа и подтверждение	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей (см. «Настройка параметров входа»). Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные

После заполнения полей необходимо нажать «ОК». Созданный ключ преобразования появится в списке.

С помощью кнопок на панели «Действия с ключами преобразования» можно удалить, изменить параметры выбранного ключа и обновить весь список.

Операции по управлению списком ключей преобразования сменных накопителей фиксируются в журнале управления политиками.

13.3.2 Процесс преобразования накопителя

Внимание! В процессе преобразования накопителя вся информация, расположенная на нем, будет утрачена, так как накопитель будет отформатирован.

Для преобразования сменного накопителя необходимо:

1. Вставить накопитель в разъем.
2. Выбрать на панели действий со сменными накопителями «Сделать преобразуемым». Откроется окно параметров для преобразования (рис. 197).

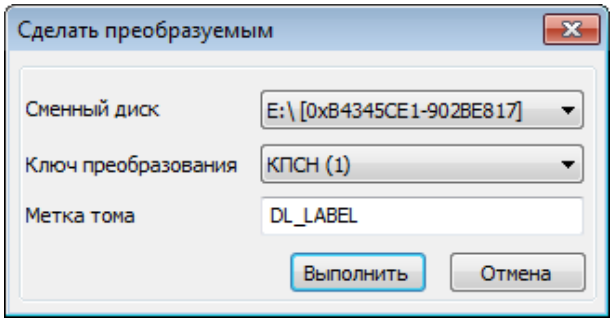


Рис. 197. Параметры для преобразования информации на выбранном диске

3. В появившемся окне параметров преобразования:
   - выбрать букву диска **сменного накопителя**, определенную ОС (если буква не определена, нужно перезапустить окно);
   - выбрать **ключ преобразования** из списка созданных;
   - ввести **метку тома** — произвольное имя будущего преобразованного накопителя.
4. Нажать «Выполнить». Далее запускается процесс форматирования диска, по окончании которого появится сообщение об успешности включения режима преобразования для диска E (рис. 198).

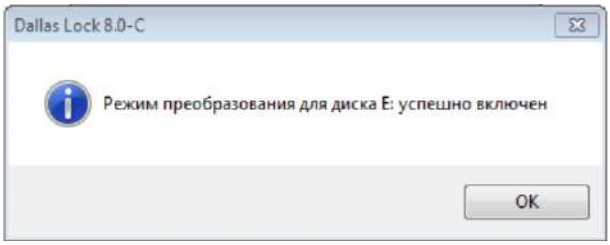


Рис. 198. Сообщение об успешном преобразовании накопителя

Операции по преобразованию сменных накопителей фиксируются в журнале управления политиками.

Внимание! Преобразование уже использованного в качестве аппаратного идентификатора для ключа преобразования USB-Flash накопителя не допускается.

13.3.3 Доступ к преобразованным накопителям

После того, как сменный накопитель преобразован, работать с ним можно только на тех компьютерах, которые защищены Dallas Lock 8.0, и на которых установлен ключ преобразования, аналогичный тому, которым преобразование было выполнено (должен совпадать пароль ключа, предъявленный идентификатор и алгоритм преобразования). При невыполнении этих условий

доступ к накопителю будет заблокирован, и появится сообщение о том, что работа с данным накопителем возможна только после его форматирования в ОС (рис. 199).

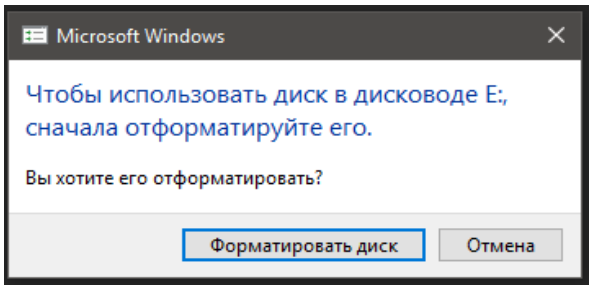


Рис. 199. Блокировка съемного носителя

Для настройки доступа к съемному накопителю по паролю, нужно поставить флаг в соответствующем поле при создании ключей преобразования.

Чтобы получить доступ к преобразованному сменному накопителю с установленным паролем, необходимо подключить данный накопитель к компьютеру. После подключения на экране появляется всплывающее уведомление (рис. 200) и окно для ввода пароля ключа преобразования (рис. 201).

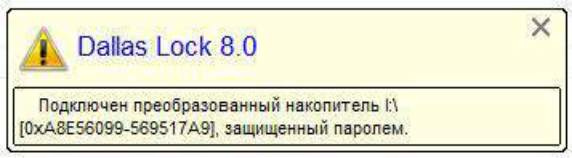


Рис. 200. Получение доступа к преобразованным съемным носителям

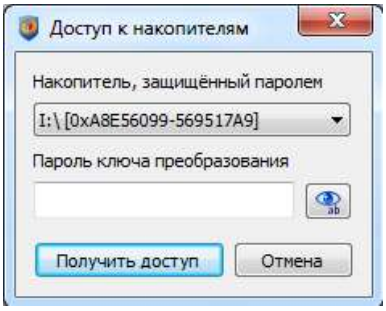


Рис. 201. Пароль ключа преобразования для доступа к преобразованным съемным накопителям

Для открытия окна «Доступ к накопителям» нужно нажать правой кнопкой мыши на панели задач на значок  и из появившегося списка выбрать пункт «Получить доступ к преобразованным накопителям» (рис. 202).

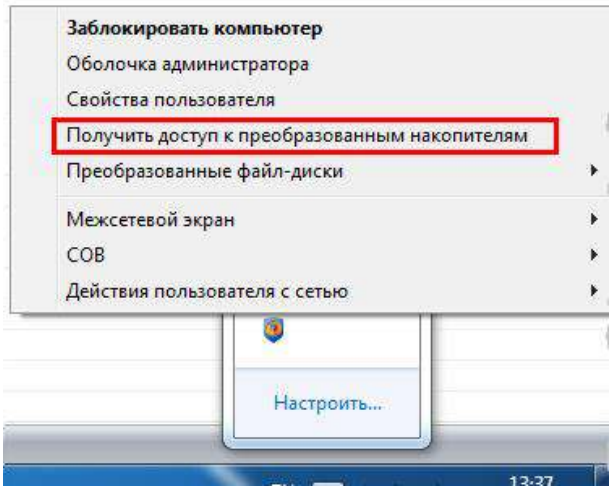


Рис. 202. Получение доступа к преобразованным съемным носителям

В результате на экране должно отобразиться окно, в котором можно выбрать накопитель, к которому необходимо получить доступ, и ввести пароль ключа преобразования для него (рис. 203).

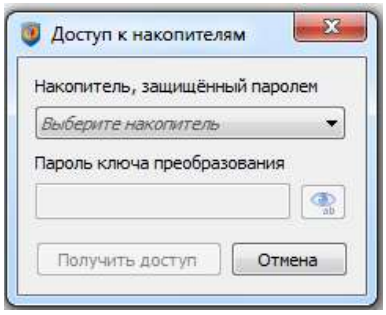


Рис. 203. Получение доступа к преобразованным съемным носителям

При попытке открытия преобразованного съемного накопителя из проводника, возникает сообщение об отказе доступа (рис. 204).

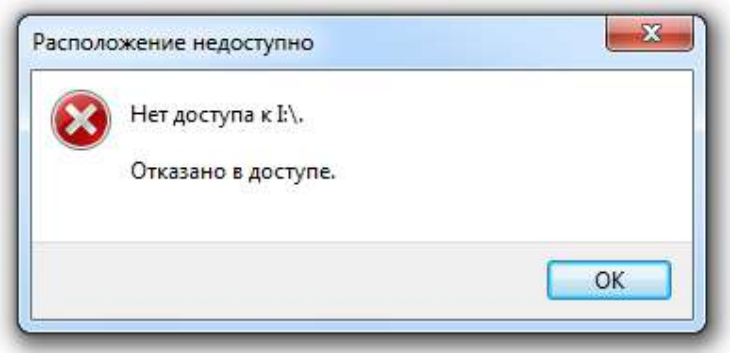


Рис. 204. Отказ доступа

При вводе неверного пароля на экране появляется сообщение об ошибке (рис. 205).

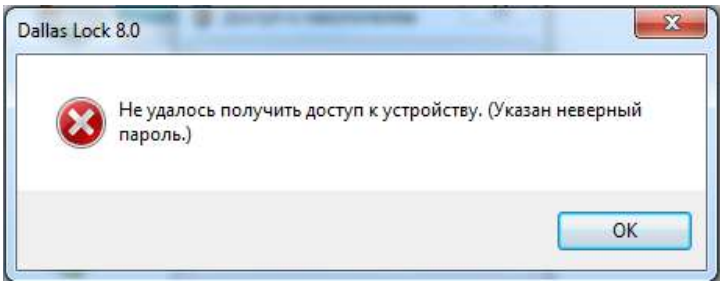


Рис. 205. Попытка доступа к устройству с неверным паролем

При превышении допустимого количества неуспешных попыток аутентификации доступ к защищаемому устройству для данного пользователя блокируется. На экране появляется соответствующее сообщение (рис. 206), в «Журнале входов» регистрируются соответствующие события.

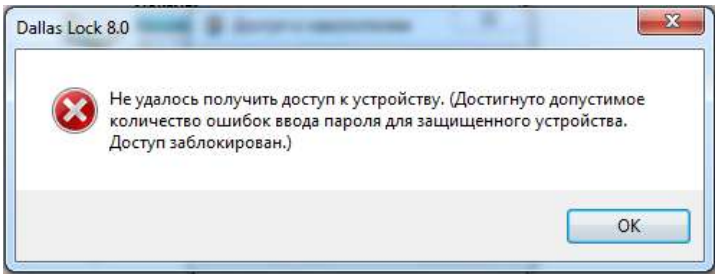


Рис. 206. Блокировка доступа к устройству

Внимание! Восстановление информации после блокировки доступа к преобразованному сменному накопителю осуществляется администратором СЗИ.

Количество попыток ввода пароля для получения доступа к преобразованному накопителю попадает под действие парольной политики СЗИ. Управление политикой осуществляется путем изменения параметра «Вход: максимальное количество ошибок ввода пароля» категории «Вход» вкладки «Параметры безопасности».

Для снятия блокировки доступа к защищенным накопителям для пользователя, администратору необходимо выполнить следующую последовательность действий: открыть в панели администрирования «Учетные записи» → вкладка «Заблокированные пользователи» → выделить соответствующее поле в таблице → на панели «Действия» нажать кнопку «Разблокировать» (рис. 207).

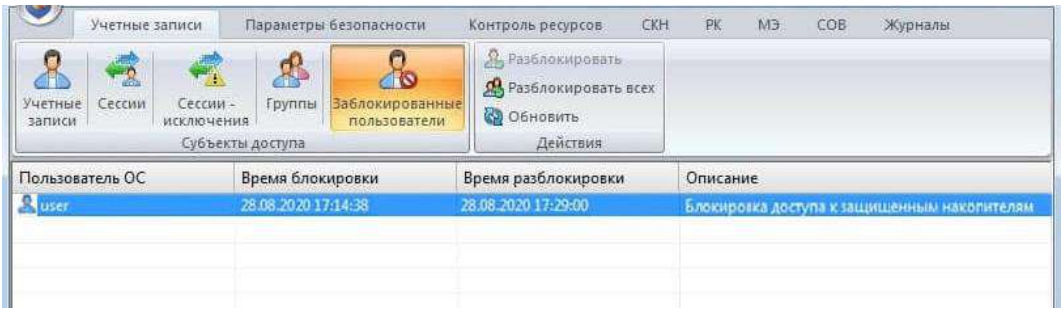


Рис. 207. Разблокировка доступа к защищенному устройству

При указании верного пароля для устройства пользователю предоставляется доступ. На экране появляется соответствующее сообщение (рис. 208).

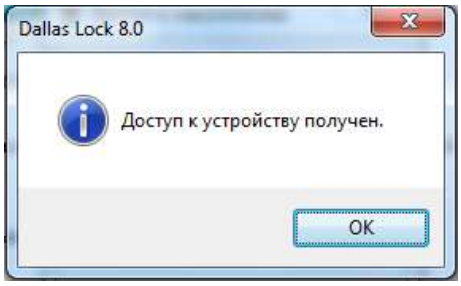


Рис. 208. Доступ к устройству

Кроме того, с помощью параметров безопасности можно определить, какие пользователи могут работать с преобразованными накопителями и с какими правами, а какие нет. Для этого используется настройка глобальных дескрипторов и настройка дескриптора данного накопителя.

Настройку глобальных дескрипторов дискреционного доступа и аудита для преобразованных сменных накопителей можно выполнить в оболочке администратора на вкладке «Контроль ресурсов» → «Глобальные». В списке имеются следующие параметры для настройки преобразованных накопителей:

- Параметры преобразованных сменных накопителей по умолчанию.
- Параметры преобразованных FDD-дисков по умолчанию.
- Параметры преобразованных USB-Flash накопителей по умолчанию.
- Параметры преобразованных файл-дисков по умолчанию.

Настройка доступа и ведения аудита событий осуществляются в соответствии с описанием в разделах «Дискреционный доступ для глобальных объектов» и «Аудит для глобальных объектов».

Настроить параметры доступа и аудита для индивидуального устройства можно через окно дескриптора, вызвав его из контекстного меню объекта в проводнике Windows. Объекты, для которых назначен дескриптор любым из способов, автоматически появляются в списке объектов выбранной категории «Дискреционный доступ» и «Аудит» на вкладке «Контроль ресурсов».

Также можно настроить доступ к преобразованному накопителю на вкладке «Контроль ресурсов» → «Устройства», выбрав класс устройств или само устройство в дереве объектов (см. «Разграничение доступа к устройствам»).

В окне свойств доступа устройства или класса устройств также можно назначить теневое копирование информации с преобразованного накопителя (см. «Теневое копирование»).

Создавать преобразованные файл-диски могут пользователи, обладающие следующим правом: разрешающее право «Изменение содержимого» для глобального дескриптора «Параметры преобразованных файл-дисков по умолчанию».

13.3.4 Обратное преобразование

Процесс обратного преобразования представляет собой форматирование выбранного сменного накопителя и затирание всей остаточной информации. После этого накопитель будет доступен для работы на любом ПК без ограничений и требований форматирования.

Чтобы запустить данный процесс, необходимо выбрать действие «Сделать открытым». В

появившемся окне параметров выбрать букву диска накопителя из списка и ввести в поле «Метка тома» наименование, которое будет у носителя после форматирования.

14 РЕЗЕРВНОЕ КОПИРОВАНИЕ

14.1 Назначение и общие принципы работы

Модуль резервного копирования позволяет восстанавливать безвозвратно модифицированные или удаленные файлы и каталоги (с поддержкой вложенных файлов). Управление резервным копированием может осуществляться как централизованно, с помощью КСБ, так и локально с помощью оболочки администратора.

Данный модуль доступен при наличии лицензии, в состав которой включен модуль «Резервное копирование».

В ходе настройки механизмов резервного копирования создаются задания на резервное копирование, которые определяют периодичность создания резервных копий объектов ФС, их количество, длительность и место хранения. Созданные задания на резервное копирование выполняются в фоновом режиме.

Примечание. Одновременно может выполняться не более 5 заданий (без возможности редактирования), запуск 6-го возможен только принудительно администратором.

Резервные копии объектов ФС создаются в виде zip-архивов, наименования которых автоматически задается по следующей схеме: «*Имя клиента*_*Имя задания*_ДД.ММ.ГГГГ_ЧЧ.ММ.СС».

14.2 Эксплуатация

Полномочия на управление резервным копированием устанавливаются в разделе «Права пользователей» на вкладке «Параметры безопасности» следующими параметрами:

- «Резервное копирование: Просмотр»;
- «Резервное копирование: Управление».

В случае, если резервные копии хранятся на сетевом хранилище, учетной записи пользователя, которая будет использоваться для запуска заданий по резервному копированию, должен быть обеспечен доступ к этому хранилищу.

Управление заданиями на резервное копирование осуществляется в оболочке администратора на вкладке «РК». Управление заданиями с СБ описано в соответствующем разделе (см. «Доменные настройки РК»).

Примечание. Функции создания, копирования, удаления, активации и деактивации заданий недоступны в случае, если клиентский компьютер введен в домен безопасности.

Примечание. Для осуществления резервного копирования должнен быть открыт TCP/IP порт 17903.

Для создания нового задания на резервное копирование необходимо:

1. Нажать кнопку «Создать» в панели действий категории «Задания» либо в контекстном меню, вызываемом щелчком правой кнопки мыши в рабочей области (рис. 209).

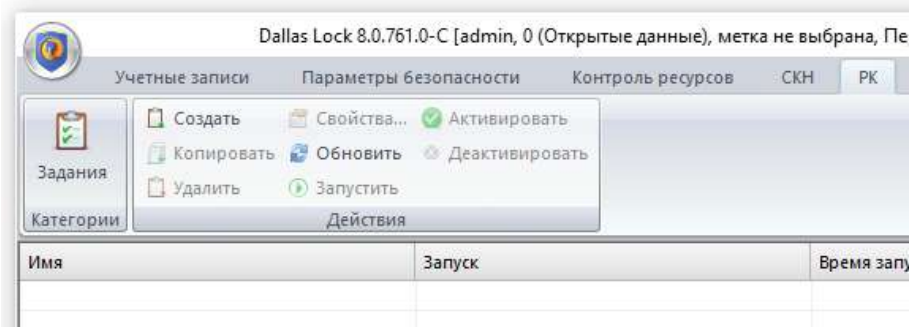


Рис. 209. Создание задания на резервное копирование

2. В появившемся окне мастера создания заданий на вкладке «Параметры» задать параметры

резервного копирования (рис. 210).

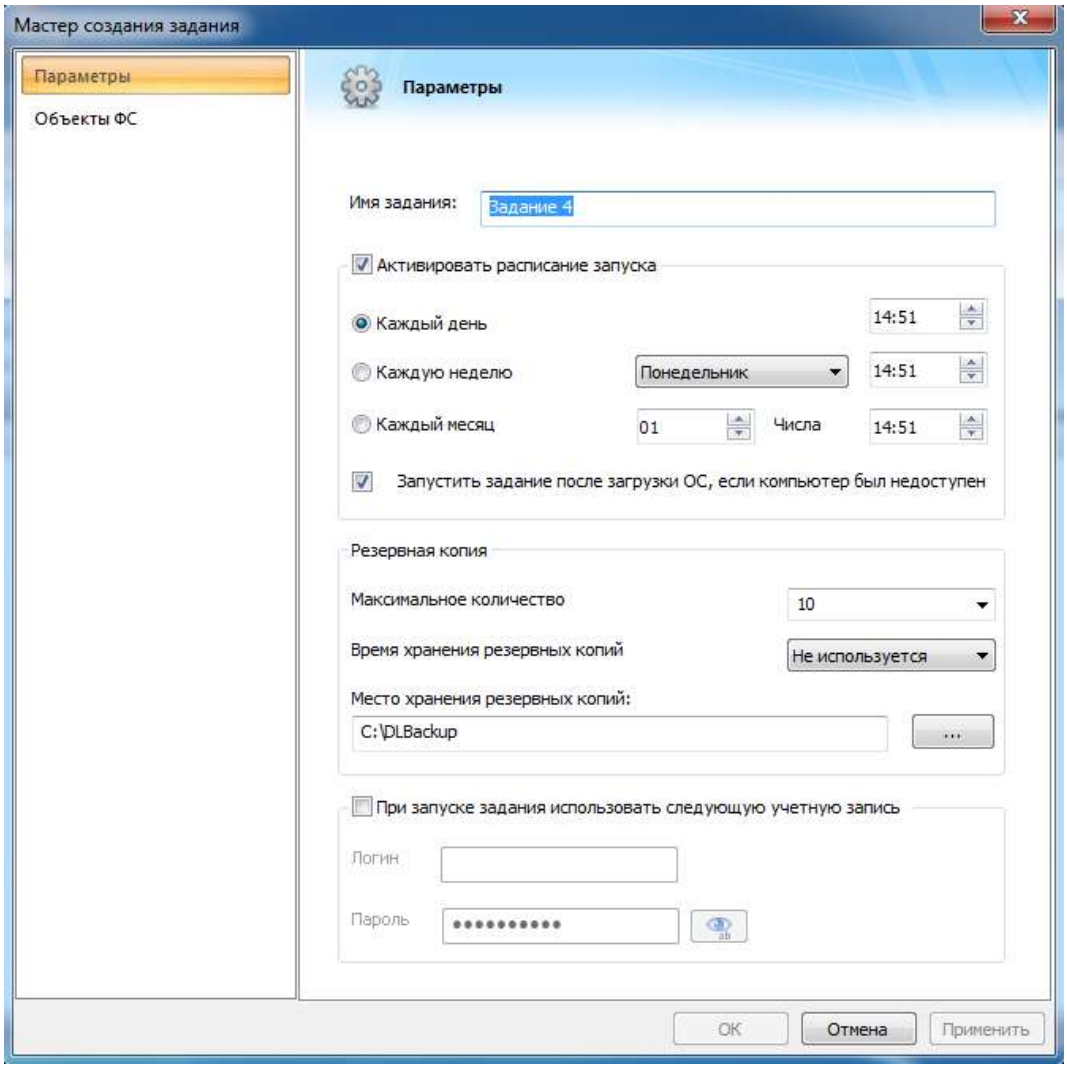


Рис. 210. Мастер создания задания на резервное копирование

В поле «Имя задания» вводится наименование, которое будет отображаться в списке заданий.

Для настройки периодичности резервного копирования необходимо установить флаг в поле «Активировать расписание запуска». Далее необходимо выбрать периодичность и указать время проведения резервного копирования в соответствующем поле (вручную с клавиатуры, либо используя стрелочки).

При необходимости установить флаг в поле «Запустить задание после загрузки ОС, если компьютер будет недоступен».

Настройка параметров резервной копии:

- «Максимальное количество» — значение данного параметра определяет максимальное количество сохраняемых резервных копий объекта ФС. При превышении заданного значения происходит удаление старых копий и создаются новые.
- «Время хранения резервных копий» — данный параметр устанавливает максимальный срок хранения копий. По истечению заданного времени с момента создания копии, данная копия удаляется.
- «Место хранения резервной копии» — данный параметр предоставляет возможность выбора директории, которая послужит хранилищем для создаваемой резервной копии. По умолчанию задан путь «C:\DLBackup».

Задания по резервному копированию по умолчанию выполняются из-под системной учетной записи. Чтобы это изменить, необходимо установить флаг в поле «При запуске задания использовать следующую учетную запись» и ввести данные учетной записи, из-под которой необходимо выполнять задания.

Внимание! Учетная запись пользователя должна быть зарегистрирована на клиенте, на котором будет выполняться данное задание. В противном случае произойдет ошибка архивирования.

Внимание! Для учетной записи, которая используется для запуска заданий, должен быть обеспечен доступ к сетевому хранилищу.

После нажатия кнопок «Применить» или «Ок» будет выполнена проверка используемой учетной записи и возможность доступа к указанному месту хранения резервных копий. Если после проверки указанная учетная запись не имеет доступа к указанному месту хранения, будет выведено предупреждение: «Учетная запись не имеет доступа к указанному месту хранения резервных копий. В случае отсутствия доступа резервная копия не будет сохранена. Вы хотите продолжить?»

3. Перейти на вкладку «Объекты ФС» и добавить объекты ФС, для которых необходимо создавать резервные копии, указав к ним путь в окне выбора ресурса (рис. 211).

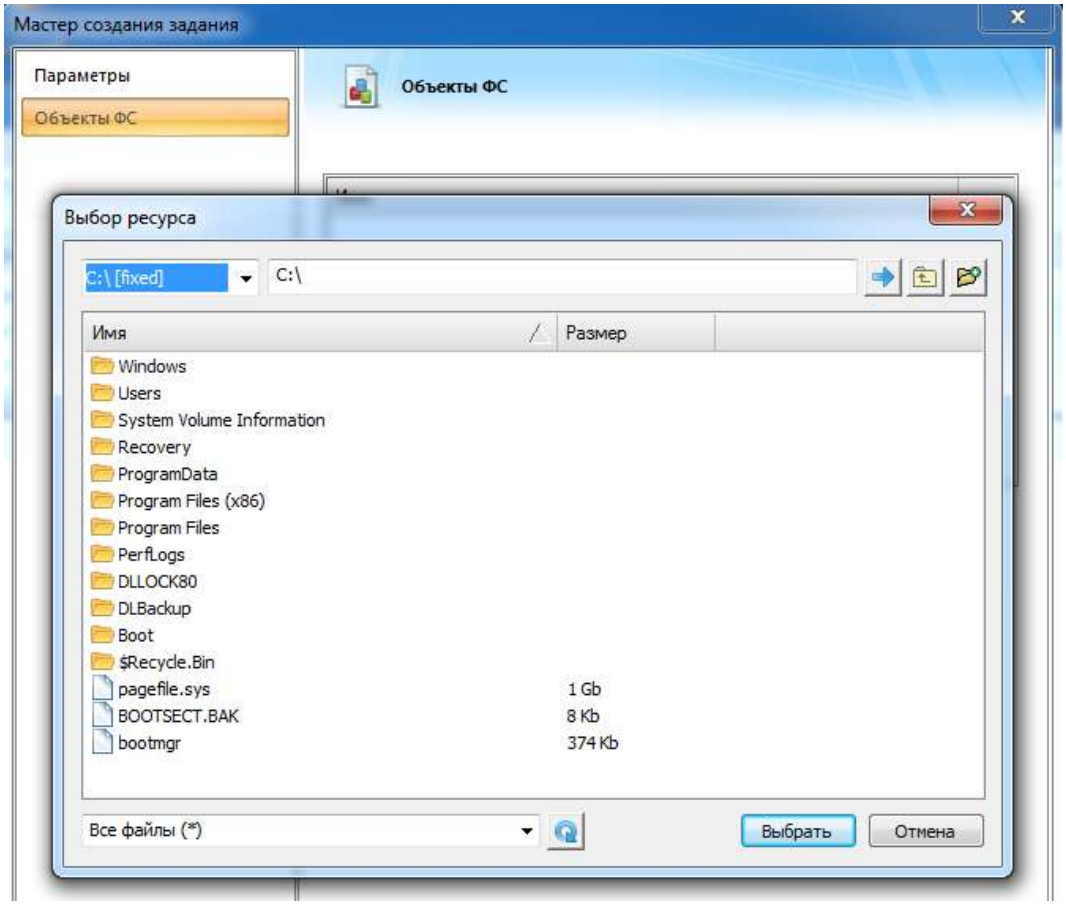


Рис. 211. Выбор объекта ФС для резервного копирования

Внимание! Для резервного копирования невозможно выбрать файловый объект, которому назначен дескриптор.

Установить флаг в поле «Создать резервную копию, если часть объектов ФС не найдена» — в таком случае, резервная копия будет создаваться для всех обнаруженных объектов ФС, которые определены для резервного копирования. Если часть объектов окажется недоступна, в графе «Выполнение» в рабочей области будет отображен статус процесса «Архивирование выполнено частично».

В случае, если не обнаруживается ни одного из выбранных объектов ФС, процедура завершится ошибкой, а в графе «Выполнение» будет отображен статус процесса «Ошибка архивирования».

Для резервного копирования сетевого ресурса необходимо установить флаг в поле «При доступе к

сетевым ресурсам использовать следующую учетную запись» и ввести данные учетной записи для доступа к этому сетевому ресурсу.

Для создания копии выбранного задания необходимо нажать кнопку «Копировать», откроется окно «Мастер создания задания» с уже установленными параметрами для копирования задания, в поле «Имя задания» имя автоматически меняется на «Имя копируемого задания-копия». В окно можно внести изменения и нажать «ОК» после чего будет создано новое задание.

Чтобы удалить задание, необходимо нажать кнопку «Удалить» в панели «Действия» либо в контекстном меню задания. При этом будут удалены все резервные копии, созданные этим заданием, о чем предупредит соответствующее диалоговое окно (рис. 212).

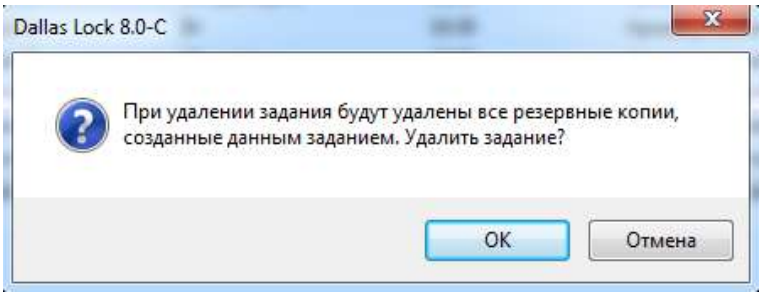


Рис. 212. Окно подтверждения удаления задания

Для просмотра параметров задания необходимо нажать на кнопку «Свойства…» в панели «Действия», откроется окно «Свойство задания», в котором можно изменить параметры выбранного задания и нажать кнопку «Применить» для сохранения измененных параметров.

Для просмотра созданных резервных копий и восстановления объектов ФС необходимо открыть свойства здания и в открывшемся окне перейти на вкладку «Резервные копии» (рис. 213). Для восстановления объектов ФС необходимо выбрать соответствующую резервную копию и нажать кнопку «Восстановить».

Примечание. Во время выполнения задания восстановление данных из резервной копии невозможно. В этом случае появится соответствующее информационное сообщение.

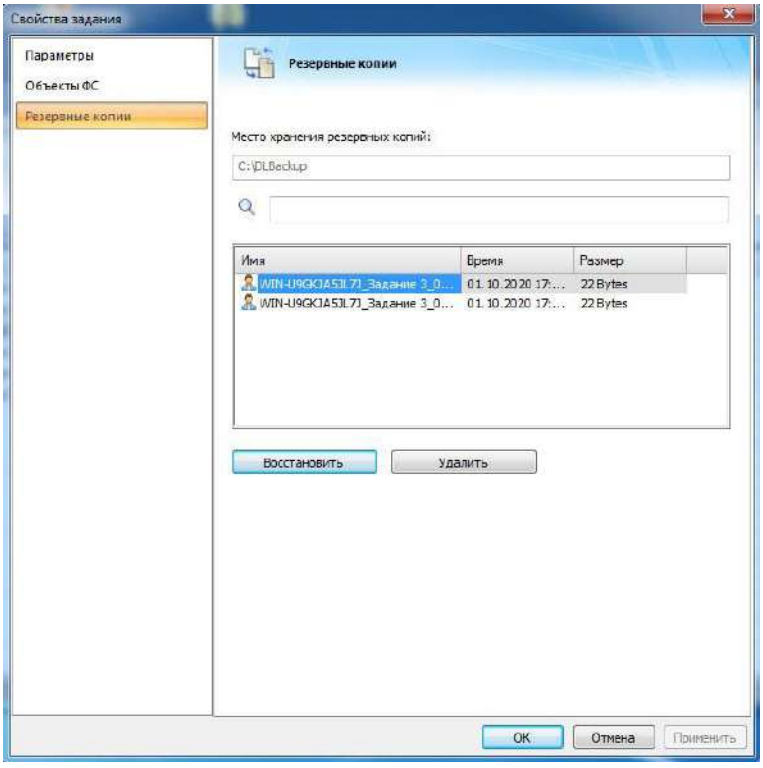


Рис. 213. Окно просмотра свойств задания

По завершению процедуры восстановления в графе «Выполнение» задания установится статус «Восстановление прошло успешно».

Примечание. Процецура восстановления реализована таким образом, что первоначально происходит очистка восстанавливаемых целевых объектов ФС. В случае, когда возникает ошибка при очистке каталога перед восстановлением, в журнале будет зафиксирована соответствующая запись с типом операции «Очистка каталога для восстановления».

Для обновления списка и статуса заданий необходимо нажать кнопку «Обновить».

Созданные задания запускаются с установленной периодичностью, однако, если необходимо запустить резервирование до запланированного времени, следует нажать кнопку «Запустить».

Если параметры задания заданы, но напротив задания имеется значок  , то это означает, что задание по резервированию не выполняется. Чтобы активировать неактивное задание, необходимо нажать кнопку «Активировать». При этом, если нет необходимости в периодическом выполнении задания, его можно запустить один раз, воспользовавшись кнопкой «Запустить». Для прекращения выполнения активного задания необходимо выбрать его в списке заданий и нажать кнопку «Деактивировать».

15 МЕЖСЕТЕВОЙ ЭКРАН

15.1 Назначение и общие принципы работы

Межсетевой экран (МЭ) является модулем СЗИ Dallas Lock 8.0 и предназначен для защиты рабочих станций и серверов от НСД посредством осуществления контроля и фильтрации, проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.

Для работы МЭ не требуется внесение изменений в структуру существующей сети.

15.1.1 Возможности межсетевого экрана

Примечание. Установка, удаление, активация и деактивация межсетевого экрана описаны в главе «Установка и удаление системы защиты».

Модуль МЭ осуществляет защиту как физических, так и виртуальных машин и поддерживает работу со всеми основными сетевыми протоколами.

Задавать ограничения можно по работе служебных и прикладных протоколов, сетевых интерфейсов, портов и т. д. А также распределять уровни доступа среди пользователей, компьютеров, групп пользователей. Функции МЭ осуществляются посредством контроля и фильтрации сетевых пакетов в соответствии с набором таких параметров, как параметры сетевых протоколов, профили, исключения, учетные записи пользователей, сетевые интерфейсы и приложения.

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность выполнить настройку правил МЭ для пользователей, работающих под различными уровнями доступа.

Работа МЭ осуществляется посредством:

- фильтрации сетевого трафика,
- работы правил исключения,
- разделения сетей на доверенные и не доверенные согласно профилям,
- контроля сетевых соединений,
- сбора и отображения статистической информации о функционировании МЭ,
- удаленного и централизованного управления.

Защита сетевых соединений осуществляется посредством проверки подлинности сетевых ресурсов, источника и приемника данных, сообщений, проведения контроля доступа к ресурсам сети.

При помощи функций удаленного и централизованного управления Dallas Lock 8.0 реализована возможность выполнения всех необходимых операций по администрированию настроек МЭ с одного рабочего места. Есть возможность осуществлять такие операции, как: включение, выключение, установка и изменение правил для входящих/исходящих пакетов данных (соединений), просмотр журналов событий и статистики.

При работе с СБ для всех компьютеров, включенных в Домен безопасности, устанавливаются глобальные правила, которые могут корректироваться для отдельных групп пользователей. Набор правил и их порядок вне зависимости от того, работают они или нет, будет сохраняться.

Доменные настройки межсетевого экрана описаны в разделе «Доменные настройки МЭ».

Сбор информации о работе сети ведется на всех компьютерах системы, на которых установлен МЭ Dallas Lock 8.0.

Примечание. Модули СОВ и МЭ позволяют обнаруживать атаки внутри виртуальной сети VipNet.

15.2 Эксплуатация

Управление настройками межсетевого экрана доступно пользователям, которым назначена возможность изменения настроек МЭ — администраторам ЗАРМ Dallas Lock (по умолчанию членам

группы «Администраторы»), и происходит из оболочки администратора во вкладке «Межсетевой экран».

Для просмотра и изменения политик и других параметров МЭ пользователь должен быть указан в значении параметров «Межсетевой экран: Изменение настроек» и «Межсетевой экран: Просмотр настроек» категории «Права пользователей» либо состоять в группе, указанной в данном параметре.

15.2.1 Адреса

В данной категории отображается список локальных адресов компьютера, посредством которых к нему можно обратиться (рис. 214).

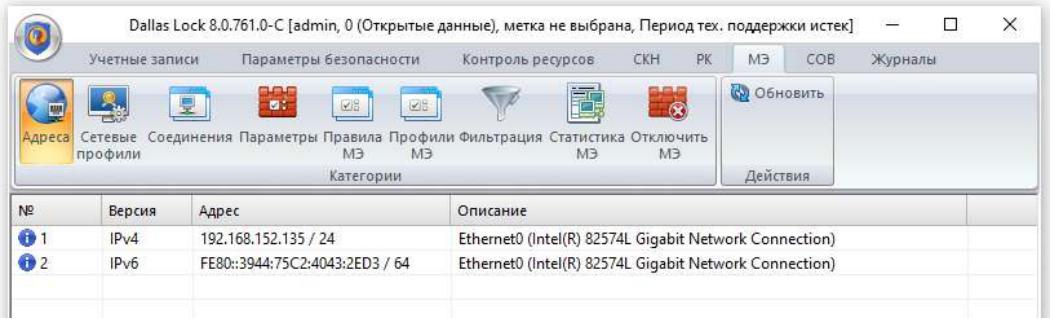


Рис. 214. Список адресов

15.2.2 Сетевые профили

Механизм «Сетевых профилей» позволяет применять правила МЭ и фильтрации не безусловно, а в зависимости от параметров сети, через которую получен сетевой пакет. Доступно семь возможных сетевых профилей сетей, определяемых по адресам и используемым сетевым адаптерам. В случае, если для сетевого пакета не подходит ни один из активных сетевых профилей — пакет будет считаться принадлежащем к сети, определенной сетевым профилем «По умолчанию». Для редактирования сетевого профиля нужно выбрать его на информационной панели и нажать кнопку «Свойства» на панели «Действия». Появится окно «Свойства сетевого профиля», в котором возможно задать IP-адрес или подсеть, выбрать сетевой интерфейс и ввести название сетевого профиля (рис. 215).

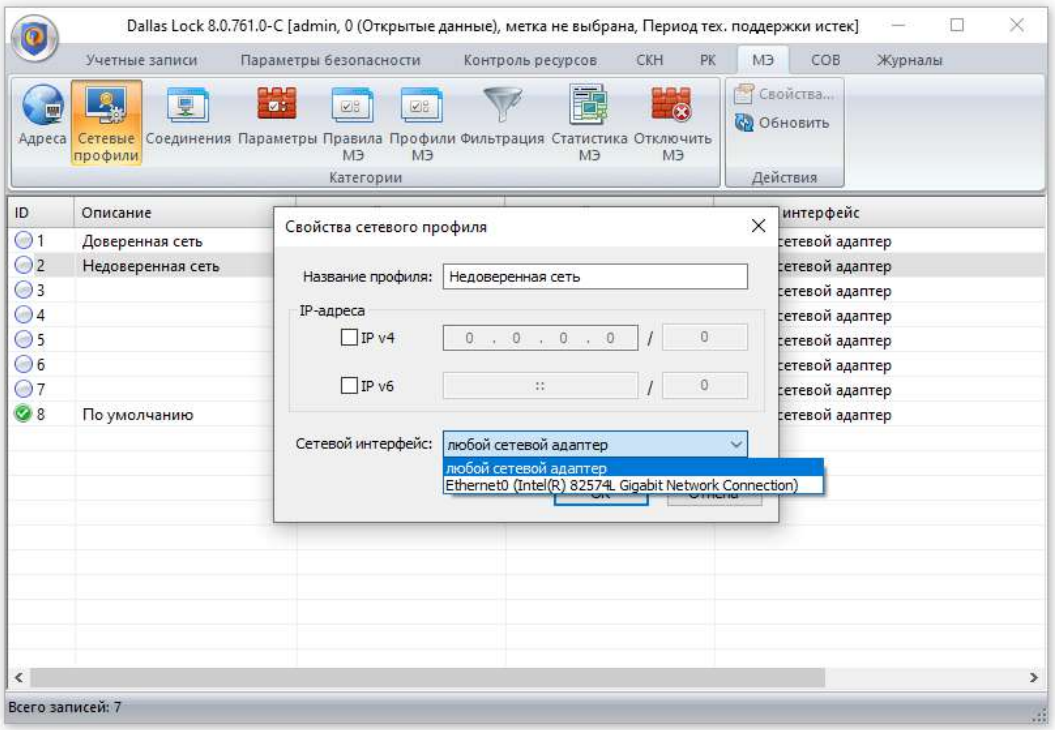


Рис. 215. Свойства сетевого профиля

Пример 1

Администратор хочет разрешить использование сети Интернет только из доверенной (корпоративной) сети.

1. Администратор задал подсеть компании и сетевой адаптер для сетевого профиля «Доверенная сеть».
2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сетевой профиль «Доверенная сеть» (см. «Правила МЭ») (рис. 216).

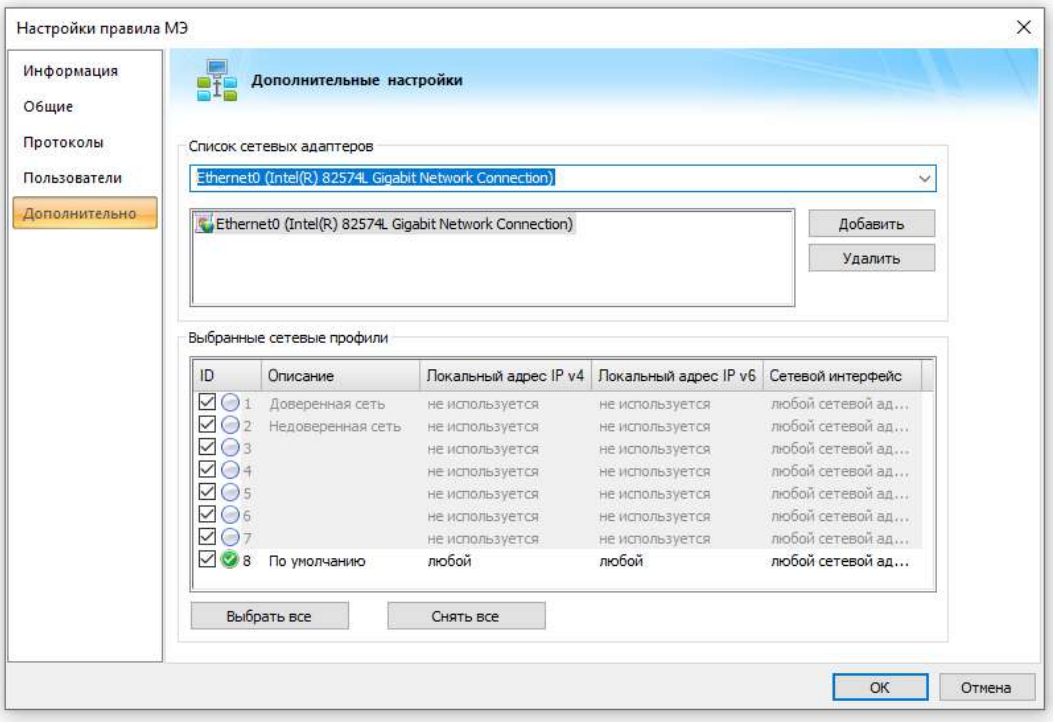


Рис. 216. Список соединений

3. Администратор отключил параметр «Глобальное правило — пропускать пакеты по умолчанию».

   В результате пользователь сможет пользоваться сетью Интернет на ЗАРМ только подключившись к подсети компании через заданный сетевой адаптер.

Пример 2

Администратор хочет разрешить использование сети Интернет только через доверенную (корпоративную) сеть для надежной антивирусной проверки трафика и принудительной защиты всего трафика от перехвата.

1. Администратор задал подсеть компании для сетевого профиля «Доверенная сеть».
2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сетевой профиль «Доверенная сеть» (см. «Правила МЭ»).
3. Администратор создал разрешающее правило для VPN подключения и выбрал для него сетевой профиль «По умолчанию». Правило VPN подключения разрешит защищенное соединение с доверенной сетью из любых сетей. После установления соединения с доверенной сетью возможно использование сети Интернет при получении через VPN адреса из диапазона доверенной сети.
4. Администратор создал запрещающее правило для всех остальных подключений и выбрал для него сетевой профиль «По умолчанию». При этом необходимо, чтобы запрещающее правило было ниже по приоритету (проверялось после разрешающих правил).

В данной конфигурации для получения доступа к сети Интернет на ЗАРМ из неизвестной сети, пользователю необходимо сначала установить VPN соединение к доверенной сети (которое должно быть сконфигурировано таким образом, чтобы выдать пользователю IP-адрес из доверенной сети, и предоставить маршрутизацию через доверенную сеть в интернет).

15.2.3 Соединения

В данной категории отображается список текущих сетевых соединений компьютера. В данном списке отображается детальная информация по каждому соединению с привязкой к процессам и ведением статистики (рис. 217).

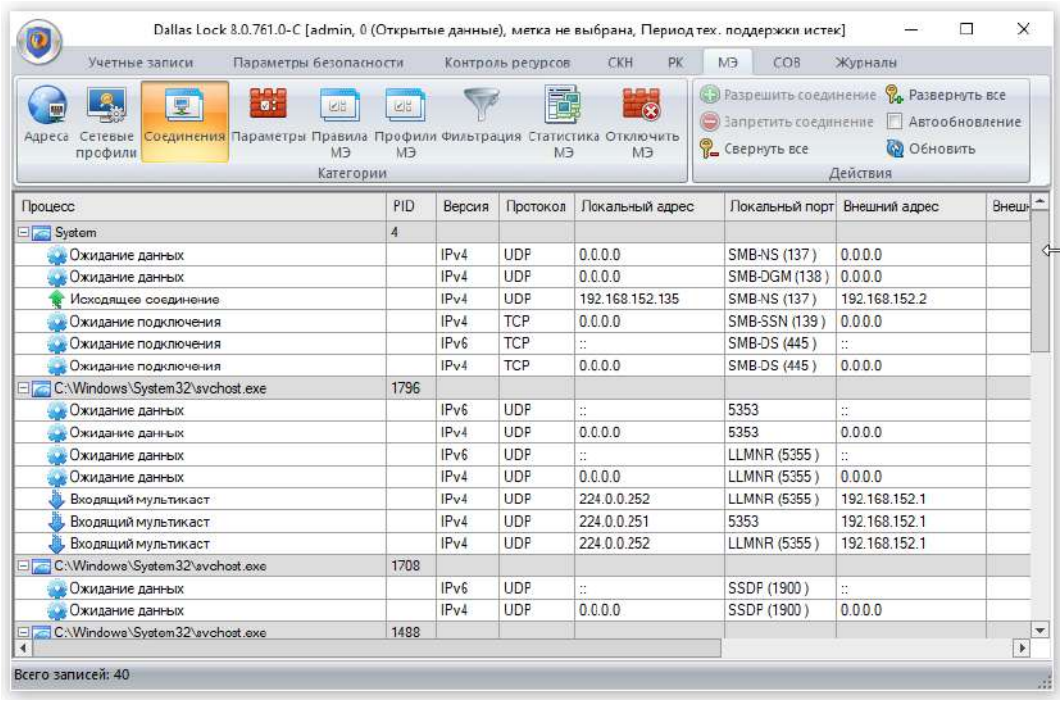


Рис. 217. Список соединений

Существует возможность запретить или разрешить соединение, создать запрещающее или разрешающее правило для соединения (см. «Правила МЭ»), создать исключение для соединения (см. «Исключения»), свернуть или развернуть список соединений, и обновить информационную панель. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

Активированное действие «Автообновление» позволяет автоматически обновлять список соединений раз в 5 секунд.

15.2.4 Параметры

В данной категории для настройки доступны основные параметры МЭ (рис. 218).

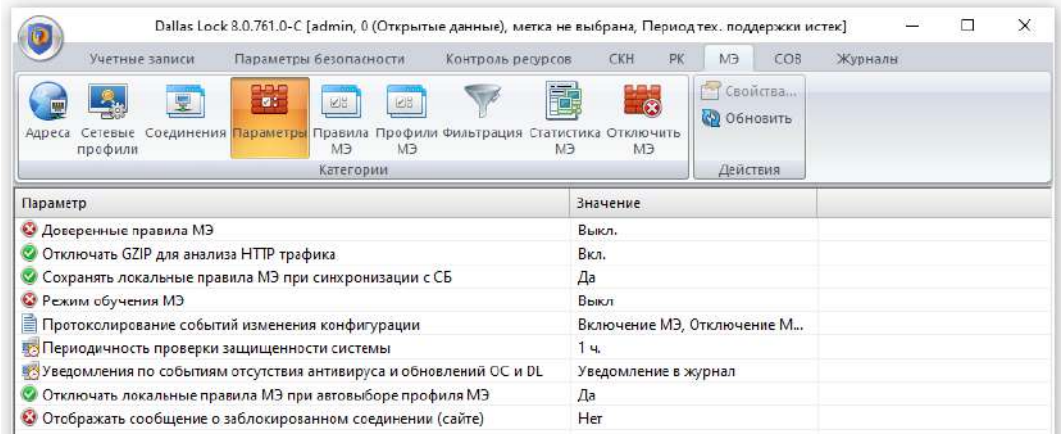


Рис. 218. Параметры МЭ

Управление параметрами осуществляется на панели «Действия» через нажатие кнопки «Свойства» при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню «свойства» интересующего пункта редактирования параметров безопасности.

Доступны следующие параметры.

Доверенные правила МЭ
Данный параметр необходим для поддержания работы по умолчанию следующих протоколов: • ARP; • DNS; • ICMP;

- DHCP;
- MSRPC;
- LDAP;
- DL (трафик управления Dallas Lock).

Данный параметр создан для осуществления бесперебойной работы базовых сетевых функций ОС вне зависимости от заданных пользователем настроек.

Наличие доверенных правил МЭ гарантирует возможность удаленного и централизованного управления по протоколам DL в случае ошибочного задания чрезмерных блокирующих правил.

Отключение доверенных правил МЭ не рекомендуется.

Отключать GZIP для анализа HTTP трафика

Данный параметр отключает сжатие трафика в независимости от настроек браузеров. Сжатие трафика ускоряет загрузку веб-страниц, но при этом препятствует возможности анализа трафика механизмами фильтрации МЭ (и при анализе сигнатур трафика СОВ). Если деактивировать данную политику — возможна некорректная работа механизма фильтрации (при использовании сайтами сжатия трафика).

Сохранять локальные правила МЭ при синхронизации с СБ

Параметр позволяет использовать локальные правила МЭ, которые не подчинены списку правил МЭ на СБ. Если на клиенте ДБ включен данный параметр, то при синхронизации локальные правила не будут удалены.

Режим обучения МЭ

Параметр позволяет включить и настроить режим обучения МЭ (см. «Режим обучения МЭ»).

Протоколирование событий изменения конфигурации

Данный параметр позволяет выбрать регистрируемые события об изменении конфигурации МЭ (и СОВ).

Периодичность проверки защищенности системы

Данный параметр позволяет настроить периодичность проверки защищенности системы с доступными интервалами от 10 мин до 1 дня. Доступна настройка (Включение/выключение; определение временного интервала, если доступно) оповещения об отсутствии обновлений для следующих объектов:

- обновление ОС — при двойном нажании на объект, открывается окно со списком всех обновлений ОС с возможностью сортировки по дате установки обновления;
- обновление антивируса;
- обновление сетевых сигнатур.

Также в окне свойств доступна информация о последнем обновлении объектов и времени проведения последней проверки.

Уведомление по событиям отсутствия антивируса и обновлений ОС и DL

Параметр позволяет настраивать (Включение/выключение) способы уведомления по событиям отсутствия антивируса и обновлений ОС и DL. Доступны следующие способы уведомления:

- уведомление в системный tray,
- уведомление в СБ,
- уведомление в журнал.

Отключать локальные правила МЭ при автопереключении профиля МЭ

С помощью данного параметра осуществляется настройка отключения локальных правил МЭ при автопереключении профиля МЭ. Значение по умолчанию «Да».

Отображать сообщение о заблокированном соединении (сайте)

С помощью этого параметра можно включить или отключить отображение сообщения о заблокированном соединении (сайте) (рис. 219).

Рис. 219. Сообщение о заблокированном соединении

Режим обучения МЭ

Для настройки списка правил МЭ возможно использовать «Режим обучения МЭ». Данный режим позволяет создавать разрешающие правила МЭ для текущих соединений пользователя в автоматическом и интерактивном режимах.

Чтобы выполнить настройку правил МЭ в автоматическом режиме используя режим обучения МЭ, необходимо:

1. Открыть категорию «МЭ» → «Параметры» и нажать два раза кнопкой мыши на параметр «Режим обучения МЭ». Появится окно настройки и выбора режимов (рис. 220).

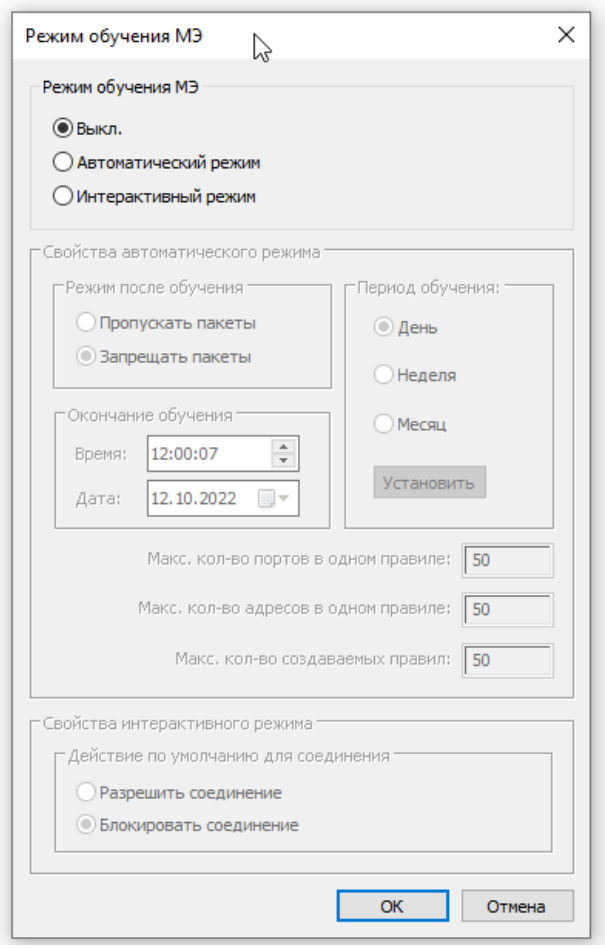


Рис. 220. Настройка автоматического режима обучения МЭ

2. Установить флаг «Автоматический режим».
3. Выбрать режим работы МЭ после завершения режима обучения:
   - пропускать пакеты — устанавливает значение «Да» для параметра «Глобальное правило — пропускать пакеты по умолчанию»;
   - запрещать пакеты — устанавливает значение «Нет» для параметра «Глобальное правило — пропускать пакеты по умолчанию».
4. Установить дату и время окончания режима обучения. Есть возможность установить период времени: день, неделя и месяц.
5. Для гибкой настройки правил возможно указать максимальное количество портов и IP-адресов в одном правиле.
6. Осуществить вход на все те веб-ресурсы, с которыми пользователь имеет право работать (но не открывать ничего лишнего).
7. Следует помнить, что не для всех веб-ресурсов является достаточным просто их открыть. Некоторые веб-ресурсы загружают не все данные, а только необходимое для работы конкретного веб-ресурса, остальное подгружается динамически, в процессе работы. Поэтому лучше выполнить все основные действия на веб-ресурсе для работы.

   На этом этапе создаются автоматические локальные правила МЭ (далее — АЛП). В списке правил МЭ АЛП выделяются зеленым цветом.

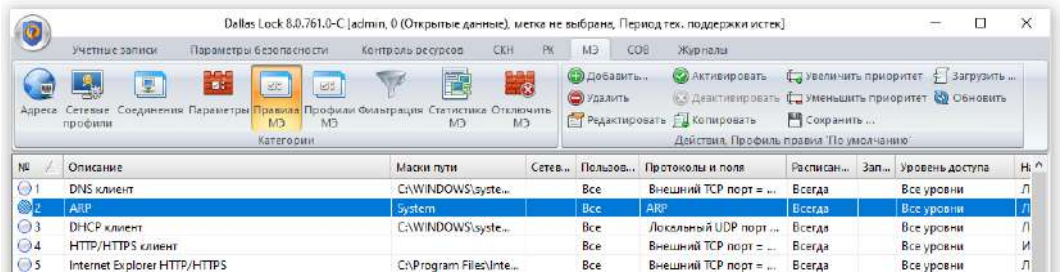


Рис. 221. Создание правил МЭ с помощью режима обучения МЭ

Созданное АЛП может автоматически дополняться, до тех пор, пока не завершится режим обучения или пользователь не произведет модификацию АЛП в момент работы режима обучения. Под модификацией АЛП понимается любое изменение данного правила.

Примечание. Если в процессе обучения будет выявлена сетевая атака, приводящая к созданию огромного количества АЛП, то в «Журнал управления политик» регистрируется ошибка и работа режима обучения автоматически завершится. Также будет удалены все созданные АЛП.

Примечание. Если в процессе обучения произойдет выключение компьютера, то сохранятся только модифицированные пользователем АЛП.

8. После завершения режима обучения, созданные и модифицированные АЛП добавляются в конец списка правил МЭ (низший приоритет) и становятся локальными правилами. Правила, созданные с помощью режима обучения МЭ выделяются синим цветом в списке правил МЭ.

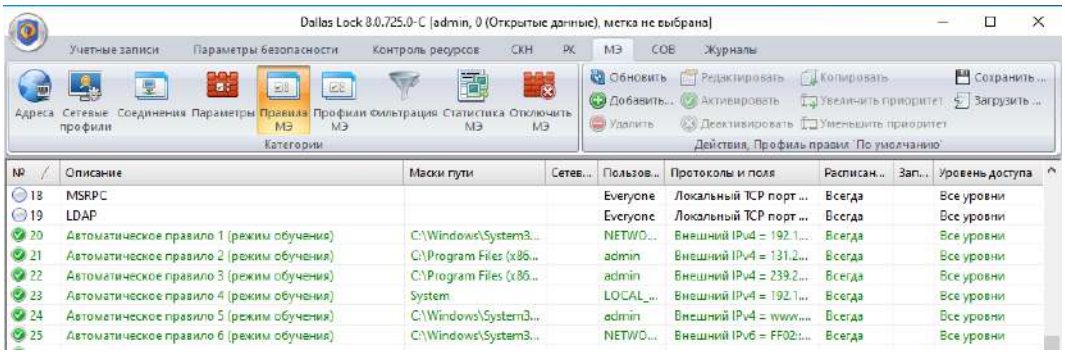


Рис. 222. Созданные правила МЭ с помощью режима обучения МЭ

Для ручного выключения режима обучения необходимо открыть категорию «МЭ» → «Параметры» и щелкнуть два раза кнопкой мыши на параметр «Режим обучения МЭ». В появившемся окне снять флаг «Включить режим обучения».

При включенном интерактивном режиме обучения сетевая активность будет анализироваться в соответствии с уже имеющимися правилами. Если для подключения нет доступных правил, пользователю при помощи диалогового окна будет предложено разрешить или запретить сетевое взаимодействие для приложения. Чтобы выполнить настройку правил МЭ в интерактивном режиме используя режим обучения МЭ, необходимо:

1. Открыть категорию «МЭ» → «Параметры» и щелкнуть два раза кнопкой мыши на параметр «Режим обучения МЭ». Появится окно подтверждения включения данного режима (рис. 220).

2. Установить флаг «Интерактивный режим» (рис. 223).

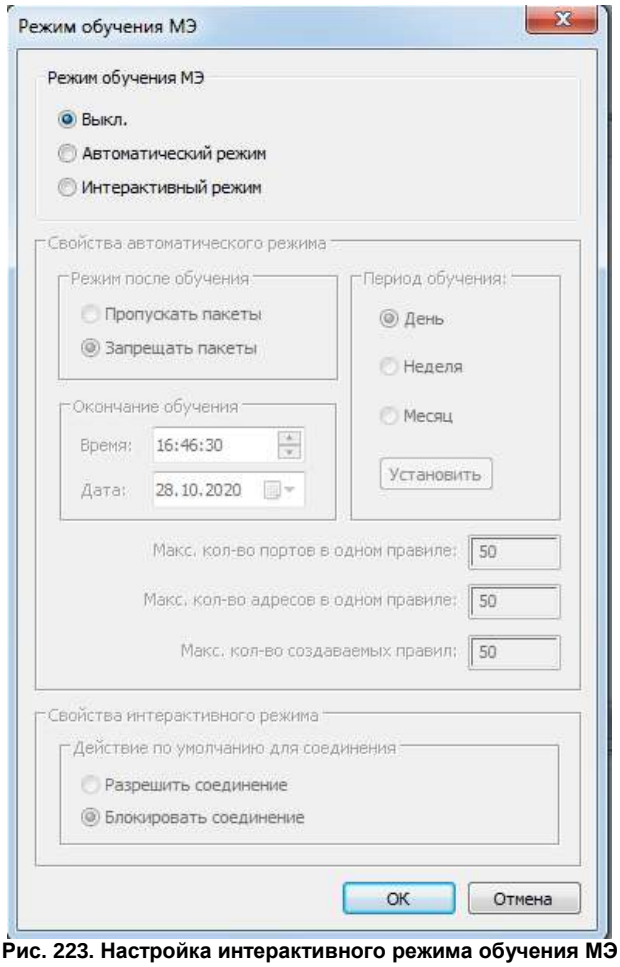


Рис. 223. Настройка интерактивного режима обучения МЭ

3. Установить флаг:
   - «Разрешить соединение»;
   - «Блокировать соединение»;
4. Нажать кнопку «ОК».

   При первой попытке приложения выполнить сетевую активность, в зависимости от выбранного действия по умолчанию, соединение будет соответственно разрешаться или блокироваться. При этом будет отображаться окно «Интерактивное обучение МЭ» (рис. 224).

Примечание. В случае, если для приложения с таким именем уже определено активное правило МЭ, удовлетворяющее текущим параметрам создания соединения, то окно «Интерактивное обучение МЭ» с возможностью создания правила для данного приложения отображаться не будет.

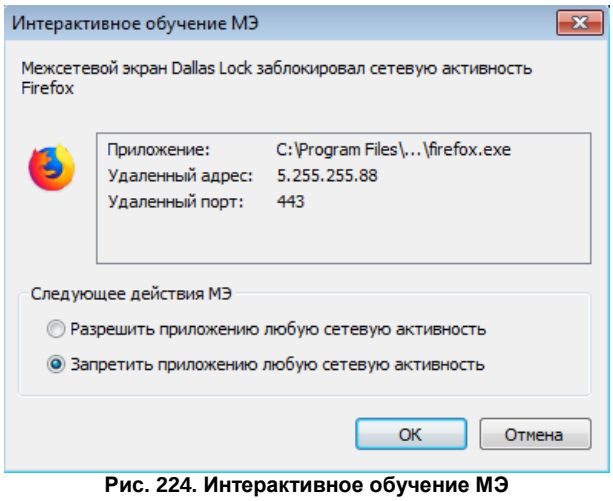


Рис. 224. Интерактивное обучение МЭ

5. Выбрать действие, которое необходимо выполнять МЭ для данного приложения:
   - «Разрешить приложению любую сетевую активность»;

- «Запретить приложению любую сетевую активность».

После выбора действия в списке правил МЭ появится новое правило интерактивного обучения. В случае, если окно «Интерактивное обучение МЭ» было закрыто без выбора действия, то правило не будет создано и при следующей сетевой активности данного приложения окно появится вновь (если не было создано правило для данного приложения и пользователя вручную).

Для того, чтобы окно «Интерактивное обучение МЭ» отобразилось снова, необходимо вручную удалить либо деактивировать правило МЭ, удовлетворяющее текущим параметрам создания соединения. В случае если правило было удалено, будет создано новое правило после выбора в окне «Интерактивное обучение МЭ», в случае, если правило было деактивировано — оно обновится в соответствии с заданными в окне значениями и автоматически станет активным.

15.2.5 Правила МЭ

Данная категория настроек является основным инструментом управления функциями межсетевого экрана и позволяет настраивать его работу.

Для перехода к управлению правилами необходимо открыть вкладку «МЭ» и выбрать категорию «Правила МЭ».

На информационной панели находится список правил и основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д. (рис. 225).

Примечание. При работе возможно наблюдать открытые порты 1000 и 1004 даже если создано запрещающее правило МЭ, но подключиться к этим портам невозможно, так как они используются службой DIIpsService.

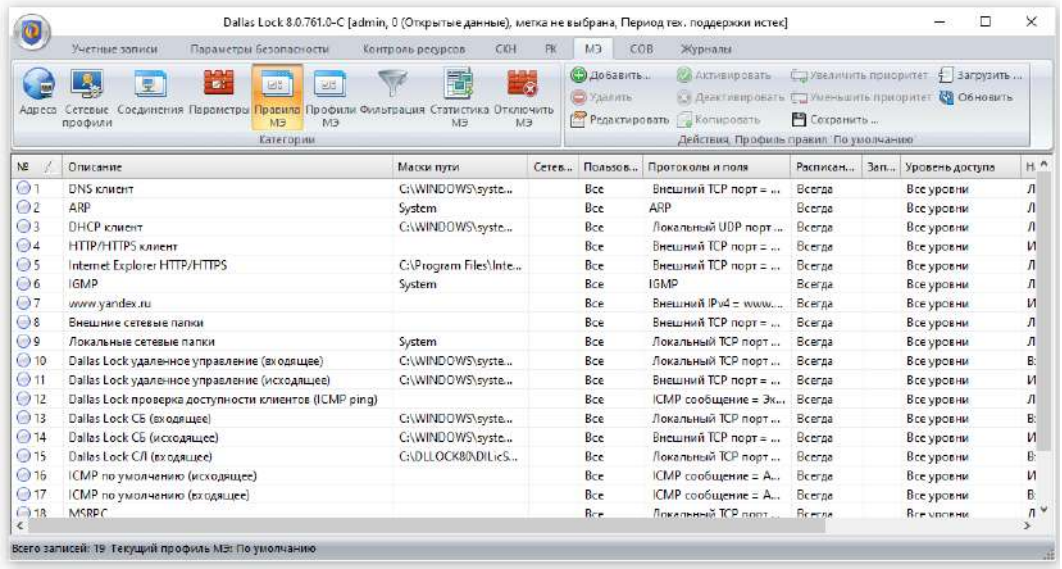


Рис. 225. Панель настройки правил межсетевого экрана

На каждом клиенте присутствуют следующие правила МЭ:

- правило по умолчанию (действие с пакетами, не попавшими ни под одно правило);
- общие правила МЭ;
- локальные правила МЭ (автоматические правила, создаваемые в режиме обучения, по умолчанию являются локальными, для изменения типа правила нужно выполнить: выбрать редактируемое правило → «Редактировать» на панели «Действия» → вкладка «Общие» → изменить значение параметра «Локальное правило»).

Локальные правила являются индивидуальными для каждого клиента. На панели настройки правил МЭ локальные правила выделяются синим цветом.

Создать новое правило можно как с помощью копирования наиболее подходящего примера, так и создав новое правило.

Для того, чтобы активировать готовый шаблон, нужно выбрать его на информационной панели и нажать кнопку «Свойства» на панели «Действия».

Существует возможность копирования имеющегося шаблона, его удаление, просмотра свойств и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

В появившемся меню «Настройки правила МЭ» можно осуществить несколько уровней настроек текущего шаблона.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 226).

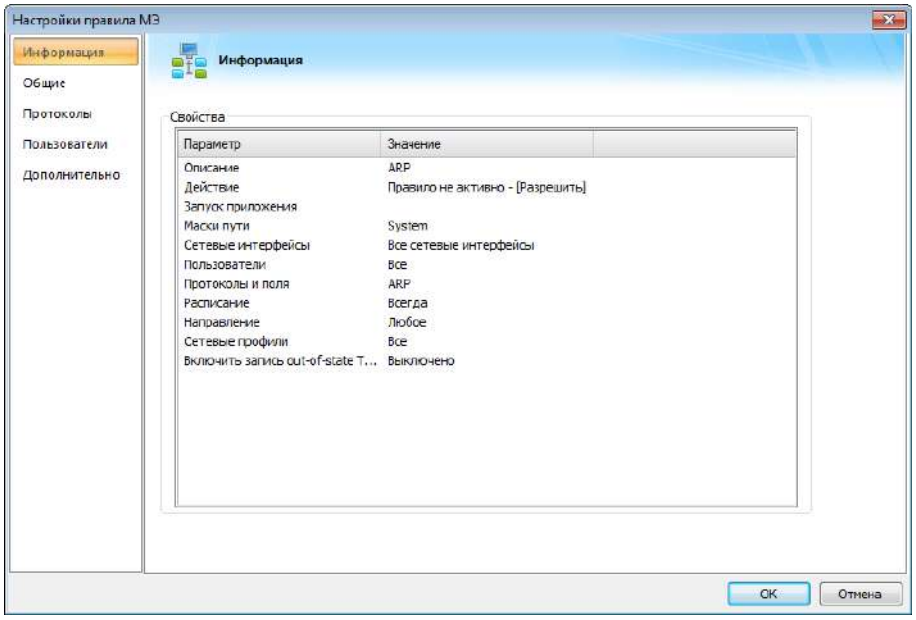


Рис. 226. Настройка правил межсетевого экрана

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

В версии «С» раздел «Информация» дополнен параметром «Мандатный уровень», информирующий о том, для каких мандатных уровней применяется правило (рис. 227).

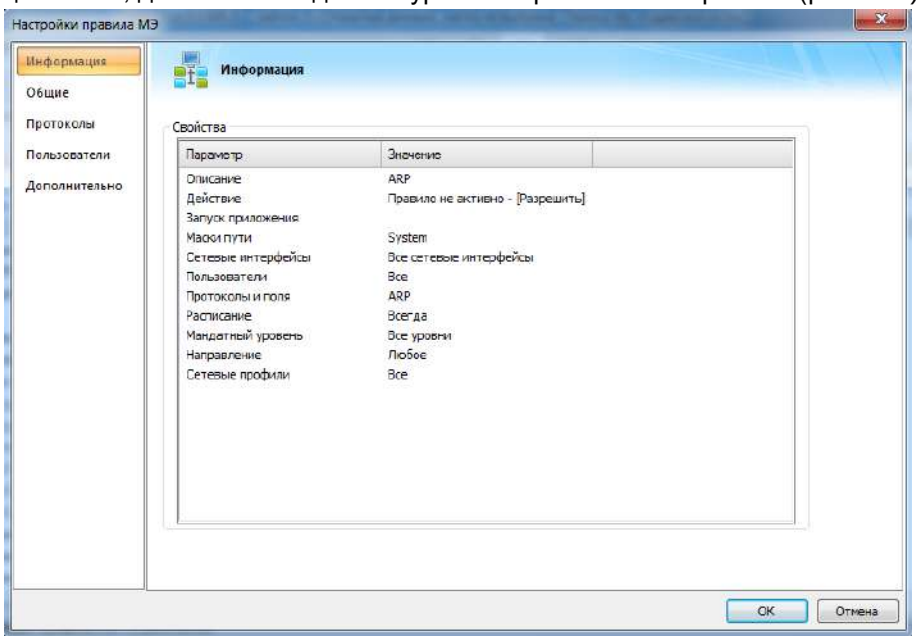


Рис. 227. Настройки правил межсетевого экрана для редакции «С»

В разделе «Общие» представлены основные настройки правила (рис. 228):

- описание правила;
- действие, которое должно выполняться согласно правилу: запретить/разрешить;
- расписание работы: настройка гибкого расписания;
- запустить приложение: указать путь к приложению, которое должно запуститься при срабатывании правила;
- применение правила только для указанных приложений: необходимо указать путь к приложению;
- параметры: необходимо указать все параметры (ключи), с которыми выполняется приложение, при указании приложения с неполным перечнем параметров корректное

выполнение правила не гарантируется.

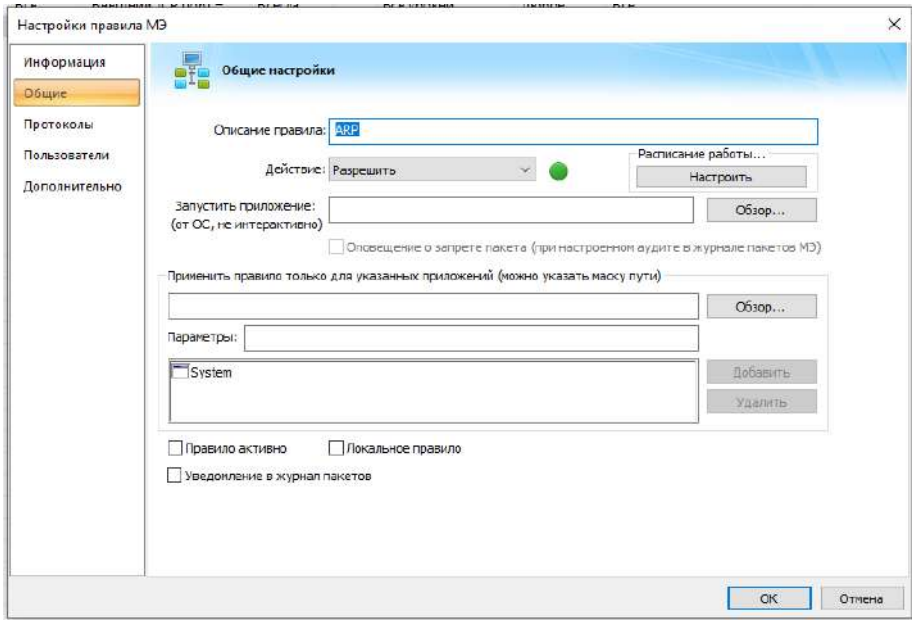


Рис. 228. Общие настройки правила МЭ

Примечание. Если был задан параметр «Запустить приложение», то при срабатывании правила, приложение запустится от имени ОС и не интерактивно. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе «Протоколы» можно задать детальные настройки отображаемой информации по принимаемым/отправляемым пакетам: направление передачи (входящие пакеты, исходящие пакеты, любое направление передачи, входящие соединения, исходящие соединения), вид протокола и его параметры (рис. 229). Есть возможность выбрать следующие направления передачи:

- Входящие пакеты — если правило разрешающее, то разрешаются все входящие пакеты.
- Исходящие пакеты — если правило разрешающее, то разрешаются все исходящие пакеты.
- Любое направление передачи.
- Входящие соединения — если правило разрешающее, то при успешном входящем соединении разрешается обратное исходящее соединение. Если правило запрещающее, то запрещаются все входящие соединения.
- Исходящие соединения — если правило разрешающее, то при успешном исходящем соединение, разрешается обратное входящее соединение. Если правило запрещающее, то запрещаются все исходящие соединения.

Примечание. Возможно использование DNS-адресов, но стоит учитывать, что это менее безопасно ввиду возможности атак на DNS-сервер, DNS-протокол и неожиданных внешних изменений DNS-записей их владельцами.

Для настройки доступа к некоторым веб-ресурсам, таким как «www.gosuslugi.ru», может потребоваться настройка разрешений на дополнительные ресурсы, в зависимости от настроек работы самого сайта. Например, на момент написания документации в случае доступа к ресурсу «www.gosuslugi.ru» для его корректной работы потребуется разрешение доступа к ресурсу «www.gu-st.ru». Подробнее то, какие дополнительные сайты требуются для работы основного, можно узнать через журнал запрещенных пакетов после настройки правила.

Примечание. Для фильтрации протоколов, использующих различные и не зафиксированные порты, необходимо настроить правила МЭ таким образом, чтобы соединения (в том числе UDP) разрешались только для определенного списка портов, и все из этих портов включены в список перехватываемых исходящих портов (см. «Настройки фильтрации»). Таким образом, фильтрация протоколов будет осуществляться на всем диапазоне возможных портов сетевого трафика.

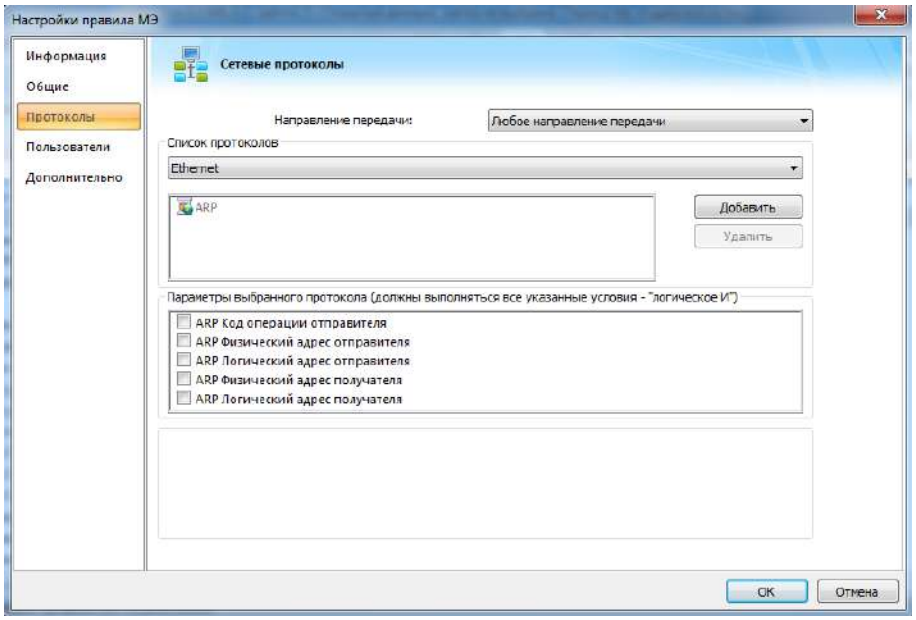


Рис. 229. Протоколы МЭ

В разделе «Пользователи» отображается список пользователей, к которым будет применяться созданное правило.

Отметив пункт «Автоматический поиск пользователей/групп» при последующем нажатии кнопок «Пользователи» и «Группы» будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки «Удалить» (рис. 230).

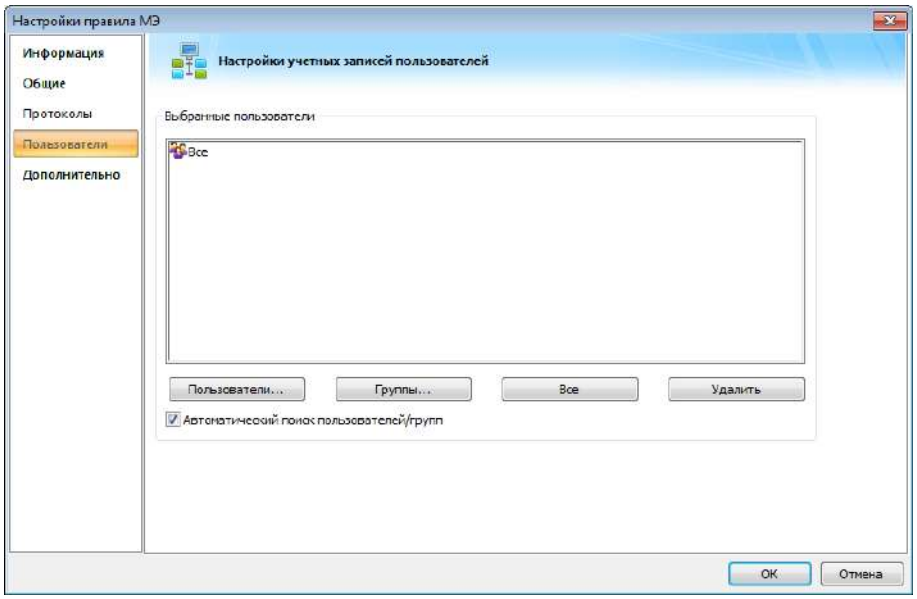


Рис. 230. Пользователи МЭ

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (рис. 231).

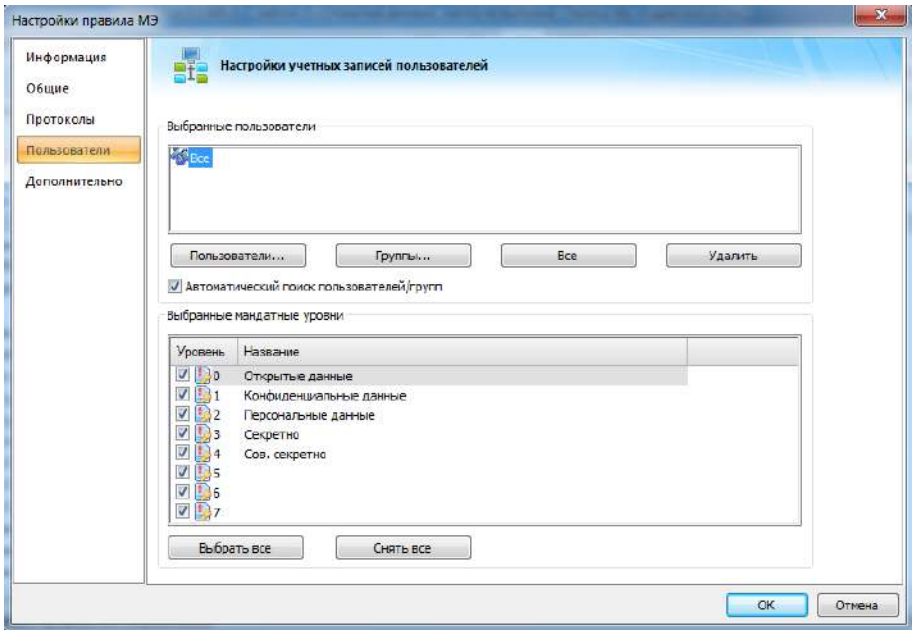


Рис. 231. Пользователи МЭ для редакции «С»

В разделе «Дополнительно» существует возможность применения текущего правила МЭ только для определенных сетевых адаптеров и (или) сетевых профилей. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку «Добавить». Удаление производится выбором адаптера из списка и нажатием кнопки «Удалить». Для редактирования списка сетевых профилей правила МЭ необходимо отметить сетевые профили (рис. 232).

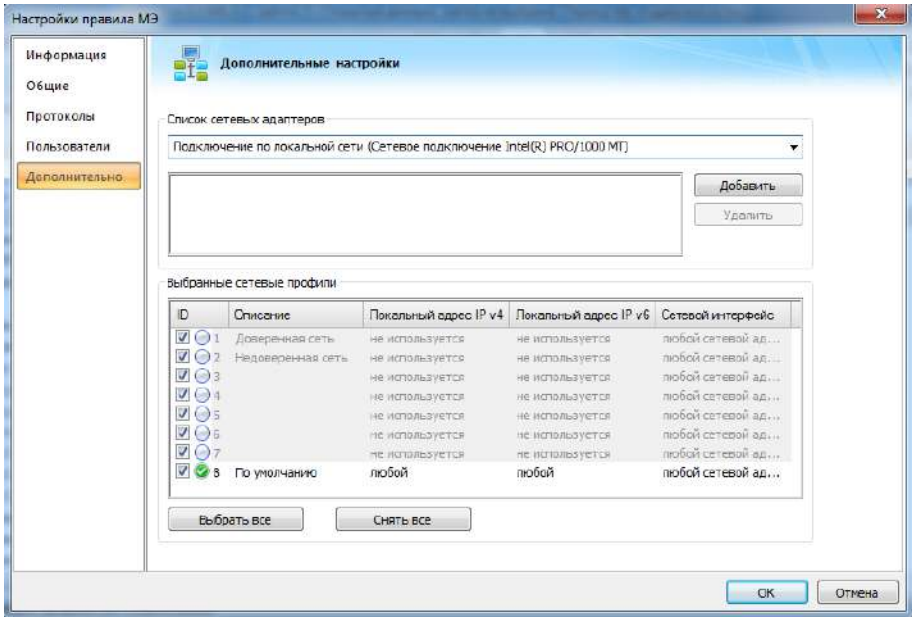


Рис. 232. Дополнительно

Задавать очередность исполняемых правил можно посредством назначения приоритетов. Правила с назначенным приоритетом выше, чем у других будут проверяться в первую очередь. После срабатывания правила, проверка правил останавливается.

Например, созданы два правила.

Правило 1 запрещает отправку/прием почты по протоколам SMTP/POP3/IMAP.

Правило 2 разрешает пользоваться почтой по протоколам SMTP/POP3/IMAP для серверов mx.yandex.ru.

Рассмотрим случай, когда правила находятся в указанной последовательности. То есть «Правило 1» находится выше «Правила 2», соответственно приоритет первого правила выше. В данном случае прием/отправка почты по указанным протоколам осуществляться не будет.

В случае если приоритет «Правила 2» будет выше приоритета «Правила 1», то тогда работа по указанным протоколам будет осуществляться только через сервер mx.yandex.ru.

Процесс создания нового правила происходит по тем же настройкам, что и корректировка уже

готового шаблона. Для создания нового правила нужно нажать правую клавишу мыши на информационной панели и выбрать «Добавить» в контекстном меню или нажать ту же кнопку на панели действий. Все последующие настройки аналогичны настройкам шаблонов.

Рассмотрим пример создания нового правила.

Например, требуется создание правила для запрета передачи IM-Messaging (чат) трафика по протоколу ICQ.

Во вкладке «Межсетевой экран» выбрать категорию «Правила МЭ» и щелкнув правой кнопкой мыши на информационном окне в выпадающем меню выбрать «Добавить».

В разделе «Общие» указывается описание правила и устанавливается действие для правила «Запретить».

Далее в разделе «Протоколы» в списке протоколов указывается нужный тип протокола «TCP […]». После нажатия кнопки «Добавить» в диалоговом окне необходимо отметить протокол «TCP […]» (ввиду того, что программа ICQ использует исключительно этот транспортный протокол). Нажать кнопку «ОК». Далее происходит настройка параметров выбранного протокола. Указывается внешний TCP порт «5190, 443», так как ICQ предусматривает работу с серверами по порту 5190 и, в случае безопасного подключения, по порту 443. Для того, чтобы правило не распространялось на HTTPS (SSL) трафик, требуются уточнения. В разделе «Протоколы» дополнительно добавляется протокол IPv4 с указанием «Внешний IPv4» и соответствующий адрес (для того, чтобы получить IP-адрес DNS-имени login.icq.com можно через меню «Пуск» → «Выполнить» → «nslookup.exe.»).

Конкретизированное правило будет работать только при точном совпадении указанных настроек. Правило, конкретизированное для протокола ICQ, сервера login.icq.com и клиента Miranda — не будет работать при любом несовпадении. Например, в случае, если используется официальный клиент ICQ, либо какой-то нестандартный сервер или порт. Конкретизированные правила удобны возможностью запретить всю работу по указанному протоколу, разрешая только определенный набор функций. Например, разрешить только работу с официальным сервером ICQ, только определенному пользователю и только с использованием определенного клиента. При создании такого разрешающего правила с детальными параметрами необходимо следующим правилом или правилом по умолчанию заблокировать трафик с отличными от указанных параметров.

IP-адреса, на которые ссылаются DNS-имена, могут изменяться. Также есть ситуации, когда для одного DNS-имени указываются несколько IP-адресов — в этом случае в графе «Внешний IPv4» необходимо указать диапазон адресов, или их перечисление через запятую, например, «217.69.139.70, 94.100.180.70» для DNS-имени www.mail.ru (на момент написания данного руководства).

Примечание. В случае **одновременного** задания нескольких параметров для одного протокола, например, одновременного задания пар «Локальный IPv4» **и** «Внешний IPv4» — для срабатывания правила должны выполниться **оба условия**. Это актуально и при указании пар «Локальный TCP порт» и «Внешний TCP порт»: при указанном локальном порте 1025 и удаленном 80 правило работает для HTTP(80/TCP) трафика ТОЛЬКО в случае если локальный порт равен 1025.

«Логическое И» действует между параметрами одного протокола, например, в случае протокола IPv4 логическое «И» действует с «Локальным» и «Внешним» адресом, в случае указания портов (TCP или UDP) — точное соответствие локальных и внешних портов (TCP и отдельно между собой UDP соответственно) и т. д.

Для правил «по умолчанию», работоспособность которых зависит от параметра «Доверенные правила МЭ», добавлен индикатор, который указывает на то, будет ли работать данное правило.

Черный индикатор указывает на то, что правило работать не будет, так как включены «Доверенные правила МЭ» (Рис. 233). Если выключить доверенные правила, индикатор будет зеленым (в случае действия «Разрешить») или красным (в случае «Запретить»).

В других правилах, которые не пересекаются с доверенными, данный индикатор не отображается.

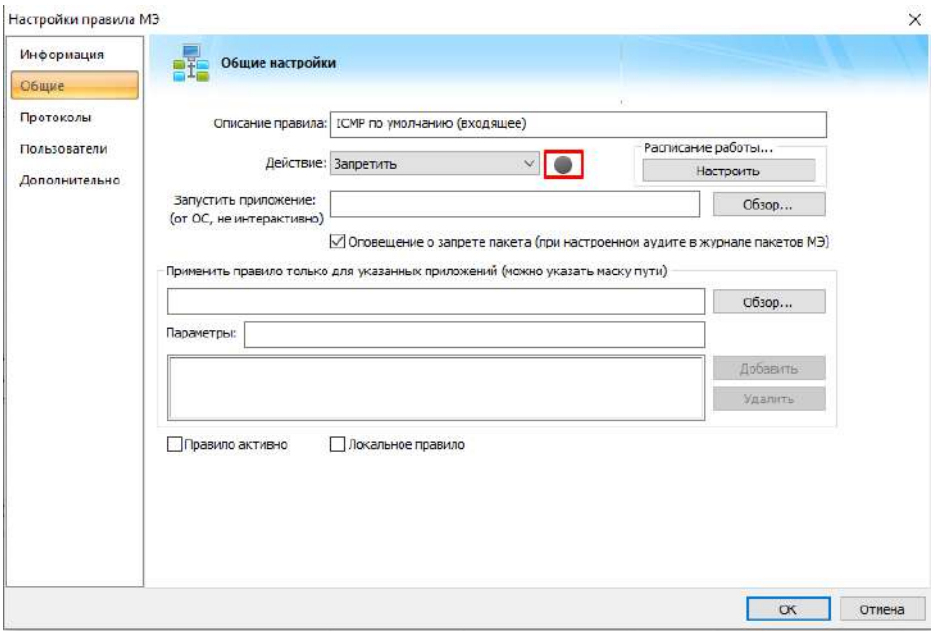


Рис. 233. Черный индикатор правила МЭ

15.2.6 Профили МЭ

Профиль МЭ представляет собой совокупность состояний правил МЭ (активировано/деактивировано) и значение для правила по умолчанию.

В профиль правил МЭ входят правила:

- правило по умолчанию,
- общие правила МЭ.

Для перехода к управлению правилами необходимо открыть вкладку «МЭ» и выбрать категорию «Профили МЭ» (рис. 234).

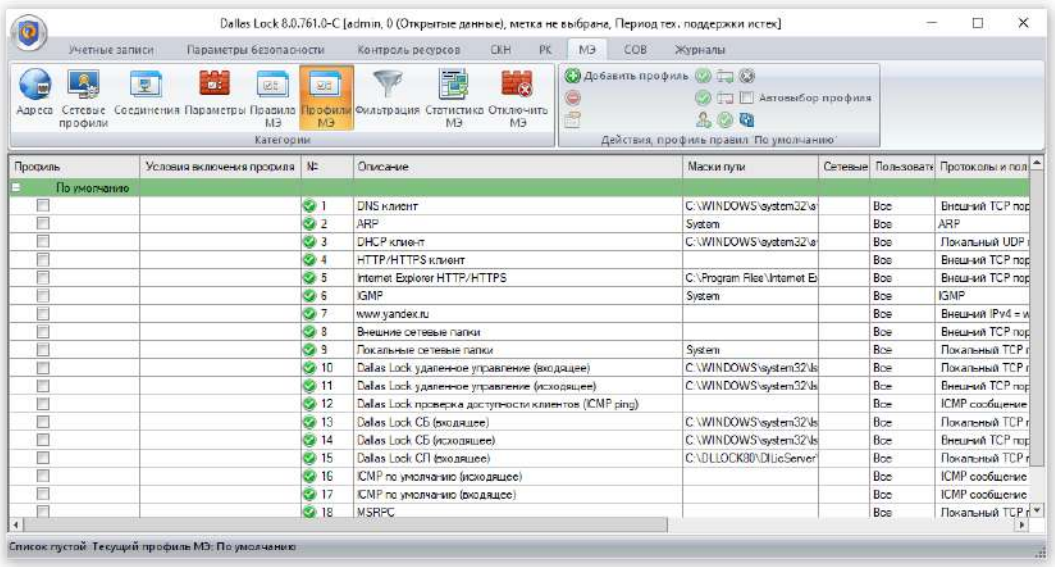


Рис. 234. Панель настройки профилей межсетевого экрана

На информационной панели находится список профилей, каждый из которых представляет из себя таблицу с полями:

- профиль («№*Приоритет профиля* *Имя профиля*» — для профилей с условием включения», «*Имя профиля*» — для ручных профилей);
- список условий включения профиля.

Для каждого профиля список правил МЭ одинаковый, но может быть индивидуально настроен. Чтобы посмотреть список правил МЭ с их настройками для конкретного профиля, нужно нажать на символ «+», находящийся слева от названия этого профиля. Список представляет из себя таблицу с полями (рис. 235):

- статус правила МЭ (активно/деактивировано), управление которым осуществляется путем

переключения чекбокса, либо кнопками «Активировать» / «Деактивировать» на панели «Действия»;

- № правила МЭ;
- основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д.

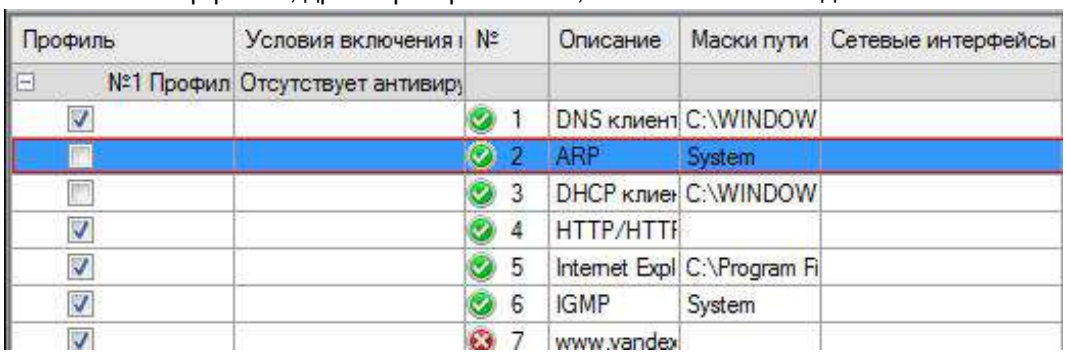


Рис. 235. Профиль МЭ

Примечание. Изменение параметров правил МЭ в режиме редактирования профилей МЭ невозможно. При выборе правила МЭ и нажатии кнопки «Свойства» на панели «Действия», доступна только информация о настроенных для правила МЭ параметрах.

Для выбора условий включения профиля, необходимо выбрать его в таблице, нажать кнопку «Свойства» на панели «Действия» и перейти на вкладку «Общие» (рис. 236).

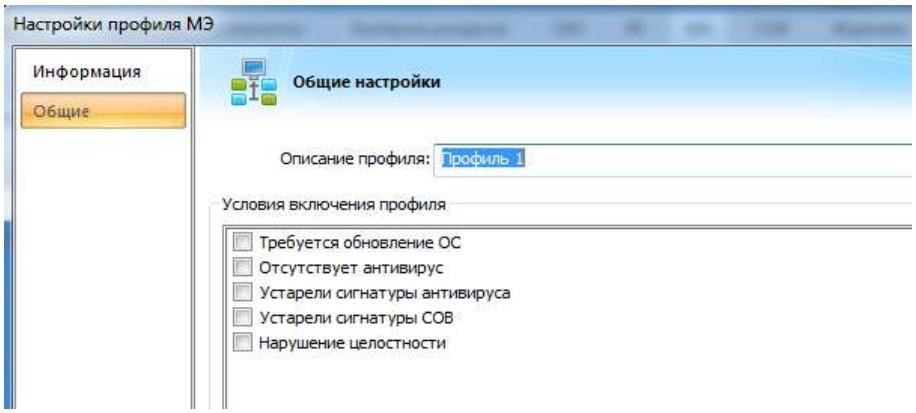


Рис. 236. Настройка автоматического включения профиля

Доступны следующие условия включения профиля:

- Требуется обновление ОС.
- Отсутствует антивирус.
- Устарели сигнатуры антивируса.
- Устарели сигнатуры СОВ.
- Нарушение целостности.

При выборе нескольких условий включения профиля действует правило «ИЛИ», т. е. при срабатывании любого из выбранных условий — активируется профиль.

Каждое условие включения может принадлежать нескольким профилям, но при одинаковых условиях у разных профилей, должен сработать профиль с наивысшим приоритетом.

Если для профиля не указаны условия включения, то данный профиль считается ручным и переключается только по команде администратора кнопкой «Переключить профиль» на панели «Действия». После переключения профиля необходимо нажать кнопку «Обновить» на панели «Действия».

Если ручному профилю задано хотя бы одно условие включения, ему присваивается самый низкий приоритет.

Для изменения приоритета профиля необходимо выбрать этот профиль и нажать кнопку «Увеличить приоритет» / «Уменьшить приоритет» на панели действия (рис. 237).

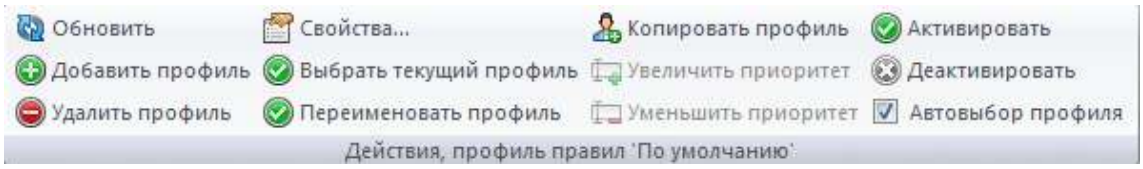


Рис. 237. Панель «Действия»

На панели «Действия» расположен параметр «Автовыбор профилей», предназначенный для автоматического включения профилей в соответствии приоритетам и условиям включения. По умолчанию параметр отключен.

Примечание. При отключенном параметре «Автовыбор профилей» доступны любые изменения списков профилей МЭ и правил МЭ (кроме редактирования правила в категории «Профиля МЭ»), в том числе их статус.

При автоматическом переключении профиля МЭ на клиенте появляется всплывающее уведомление на панели задач (рис. 238).

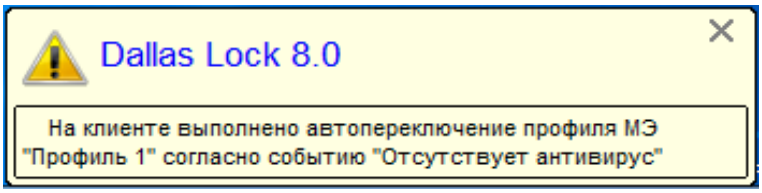


Рис. 238. Автопереключение профиля МЭ при срабатывании условия

Примечание. При включенном параметре «СОВ» → «Параметры СОВ» → «Глобальные параметры» → «Маскирование датчика СОВ» → «Вкл.», всплывающее уведомление об автопереключении профиля на клиенте не появляется.

После нейтрализации условий включения профиля выполняется автоматическое переключение на профиль «По умолчанию».

При попытке смены профиля после его автоматического переключения появляется предупреждающее диалоговое окно о том, что для переключения необходимо отключить параметр «Автовыбор профиля» (рис. 239).

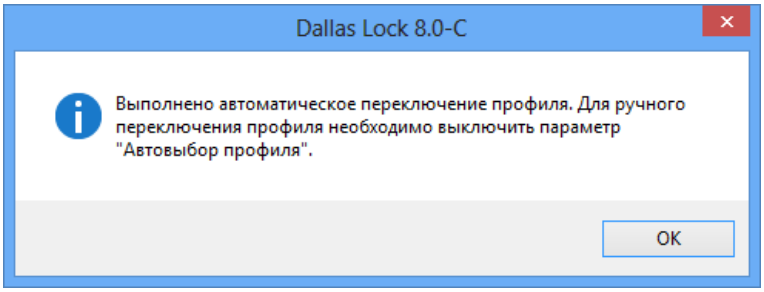


Рис. 239. Ручное переключение профиля при активном параметре «Автовыбор профилей»

Название текущего профиля МЭ отображается на нижней части панели в категориях «Профили МЭ» и «Правила МЭ» (рис. 240).

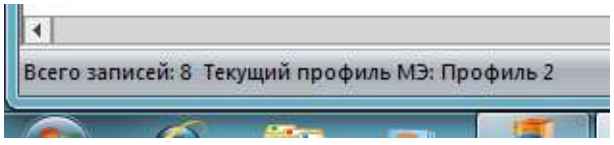


Рис. 240. Текущий профиль МЭ

15.2.7 Фильтрация

Посредством фильтрации возможно контролировать сетевой трафик по его содержимому (анализируется присутствие известных протоколов, медиа-контента и мобильный код) во всем фильтруемом трафике.

Внимание! При установленном антивирусе для работы механизма фильтрации необходимо добавить файл «C:\DLLOCK80\DlIpsService.exe» в список исключений антивируса.

Настройки фильтрации

В данной категории доступны настройки фильтрации МЭ (рис. 241).

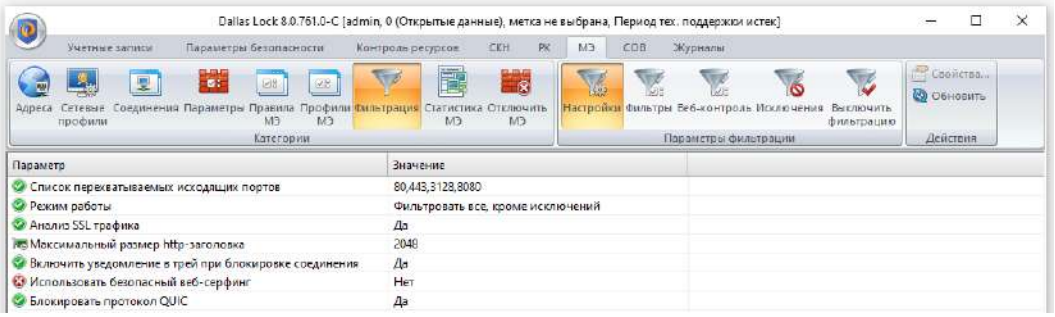


Рис. 241. Настройки фильтрации

Управление параметрами осуществляется на панели «Действия» через нажатие кнопки «Свойства» при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню «Свойства» интересующего пункта редактирования параметров безопасности.

Список перехватываемых исходящих портов

Параметр позволяет задать список перехватываемых исходящих портов для фильтрации трафика. По умолчанию имеет значение: 80, 443, 3128, 8080. Диапазон портов указывается через «,», «-», также можно использовать слово «any» для указания всех портов. Анализ трафика ведется только для соединений, проходящих по указанным портам.

Смена настроек, связанных с формированием списка перенаправлений (Сетевые профили МЭ, Параметры МЭ/СОВ, Фильтрация МЭ, Сигнатуры трафика СОВ), приводит к освобождению всех ресурсов, занятых службой фильтрации, повторному созданию потоков и привязке портов для нового списка.

При возникновении ошибок в процессе формирования перенаправлений служба показывает всплывающее окно и добавляет запись в журнал политик.

Режим работы

Данный параметр позволяет выбрать режим работы фильтрации относительно добавленных исключений. Доступно два режима:

- фильтровать все, кроме исключений;
- фильтрация активна только для хостов-исключений. Фильтрация будет применяться только к добавленным исключениям.

Анализ SSL трафика

Данный параметр позволяет осуществлять фильтрацию в том числе для HTTPS (SSL) соединений. При включении данного параметра осуществляется внедрение в HTTPS трафик и анализ трафика прозрачно для пользователя путем подмены SSL сертификата.

Внимание! При включении параметра «Анализ SSL трафика» возможно проявление конфликтов со сторонним ПО, детально проверяющим принадлежность своего SSL сертификата, например:

- блокировка скачивания обновлений ПО;
- блокировка взаимодействия Kaspersky Endpoint Security с Kaspersky Security Center и т.д.

Для решения подобной проблемы необходимо добавить URL серверов обновлений ПО или NetBios-имя сервера с KSC в список исключений (хосты из списка исключений не подвергаются подмене сертификата, при установленном режиме работы «Фильтровать все, кроме исключений»).

Внимание! В целях обеспечения бесперебойного получения обновлений ОС служба обновлений ОС Windows исключена из анализа SSL трафика (подмена сертификата Microsoft не осуществляется) в любом режиме работы Фильтрации МЭ.

Внимание! Инсталляторы некоторых приложений, чувствительных к подмене сертификата, могут не работать при включенном анализе SSL, поэтому для установки этих приложений нужно либо добавлять исключения либо на время установки выключать анализ SSL.

Максимальный размер http-заголовка

Данный параметр позволяет осуществлять фильтрацию с целью выявления аномальности HTTP-заголовка по размеру. Доступны значения максимального размера HTTP-заголовка от 2048 символов до 16 384 символов. По умолчанию параметру присвоено значение 2048.

Включить уведомление в трей при блокировке соединения

Параметр предназначен для управления всплывающими уведомлениями при блокировке соединения. По умолчанию уведомления отключены.

Использовать безопасный веб-серфинг

Данный параметр позволяет осуществлять безопасный веб-серфинг. Для настройки доступны следующие параметры:

- Phishing (интернет-мошенничество с целью получения доступа к конфиденциальным данным пользователей);
- Malware (использование веб-ресурсов, предназначенное для получения НСД к вычислительным ресурсам ТС или к информации, хранимой на ТС, с целью несанкционированного использования ресурсов ТС или нанесения ущерба владельцу информации путем копирования, искажения, удаления или подмены информации);
- Adult (контент только для взрослых).

Для каждого из параметров реализован выпадающий список настроек, способный принимать значения:

- «Блокировать» — ресурс проверяется с помощью сервиса «Safe Browsing API» по списку небезопасных интернет-ресурсов (создан и поддерживается Яндексом). В случае обнаружения запрашиваемого ресурса в указанном списке производится блокировка доступа к данному ресурсу. В браузере пользователю выводится сообщение о блокировке.
- «Журналировать» — ресурс проверяется с помощью сервиса «Safe Browsing API» по списку небезопасных интернет-ресурсов (создан и поддерживается Яндексом). В случае обнаружения запрашиваемого ресурса в указанном списке блокировка доступа к данному ресурсу не производится. При этом производится соответствующая запись в журнал.
- «Отключить» — никакие действия с проверкой ресурса не осуществляются.

По умолчанию безопасный веб-серфинг не используется.

Блокировать протокол QUIC

Параметр предназначен для блокированния передачи данных по протоколу QUIC.

Фильтры

На информационной панели расположены фильтры, анализирующие присутствие известных сетевых протоколов и мобильного кода в фильтрующемся трафике (рис. 242).

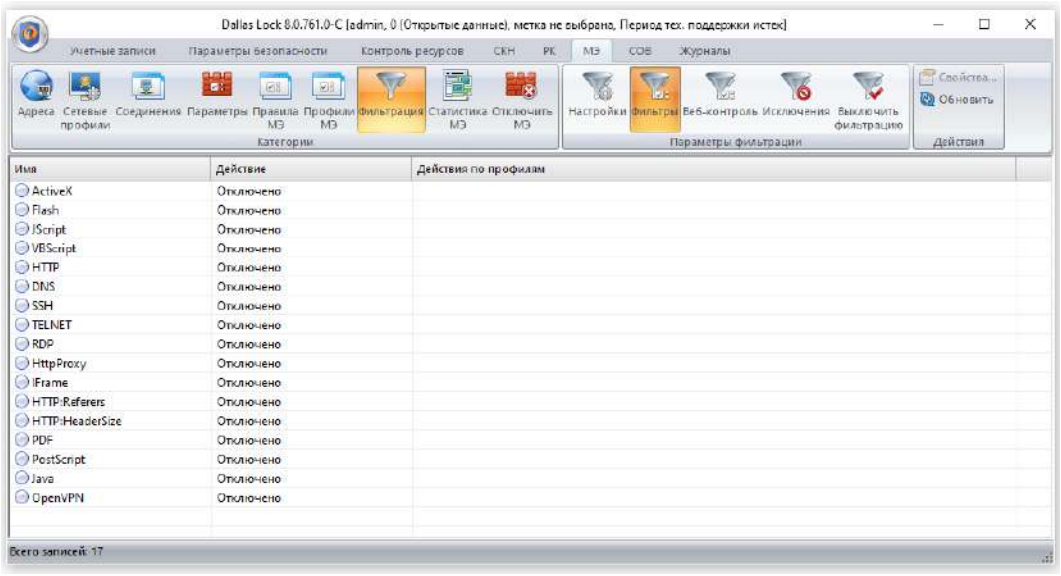


Рис. 242. Фильтры

Доступны следующие действия фильтрации для каждого отдельного фильтра:

- блокировать — при обнаружении блокируемого ресурса происходит его блокировка в браузере и событие заносится в журнал;
- вырезать — доверенному ресурсу разрешен доступ в браузере, остальные действия в браузере блокируются;
- журналировать – событие при выполнении заносится в журнал;
- отключено — выбранный фильтр отключен.

Для активации определенного фильтра нужно два раза щелкнуть левой кнопкой мыши по фильтру на информационной панели, после чего появится окно «Свойства фильтра». Далее необходимо выбрать действие фильтра для всех профилей или действия для каждого профиля индивидуально, после чего нажать «ОК».

Пример

Рассмотрим случай, когда требуется доверенный доступ к сайту «mail.ru», а для всех остальных необходимо вырезать ресурсы содержащие мобильный код, чтобы исключить известные и неизвестные уязвимости браузеров.

Открыв категорию «Фильтрация» → «Исключения» необходимо нажать правой кнопкой на информационной панели и в контекстном меню выбрать «Добавить». На информационной панели появится новое правило с пустым полем «URL», где нужно ввести IP-адреса или DNS-имя соответствующего хоста или сайта. В данном случае введя «mail.ru», поле «Адрес» автоматически заполнится всеми IP-адресами, принадлежащими DNS-имени «mail.ru» (и, при необходимости, другим доверенным адресами).

Затем на вкладке «Фильтрация» → «Настройки» необходимо для параметра «Режим работы» выбрать режим «Фильтровать все, кроме исключений».

Для фильтрации мобильного кода для всех остальных сайтов необходимо на вкладке «Фильтрация» → «Фильтры» включить фильтры мобильного кода (ActiveX, Flash, JScript, VBScript) с действием фильтра «Вырезать».

При выполнении описанных настроек пользователю будет доступен хост «mail.ru» без ограничений, но для остального трафика фильтрация вырежет заданный мобильный код, значительно уменьшая возможность эксплуатирования уязвимостей браузеров.

Примечание. После загрузки страницы веб-сервиса, в кэш браузера помещаются загруженные объекты (html-страница, flash-файл и т. п.). При последующих загрузках данной страницы веб-сервиса, flash-файл больше не будет передаваться по сети, как и html-страница. Поэтому для корректной работы фильтров необходимо очистить кэш браузера.

Примечание. Для перехвата трафика по протоколу DTLS, выполните одно из следующих действий.

1. Создать правило МЭ по блокировки протокола DTLS.

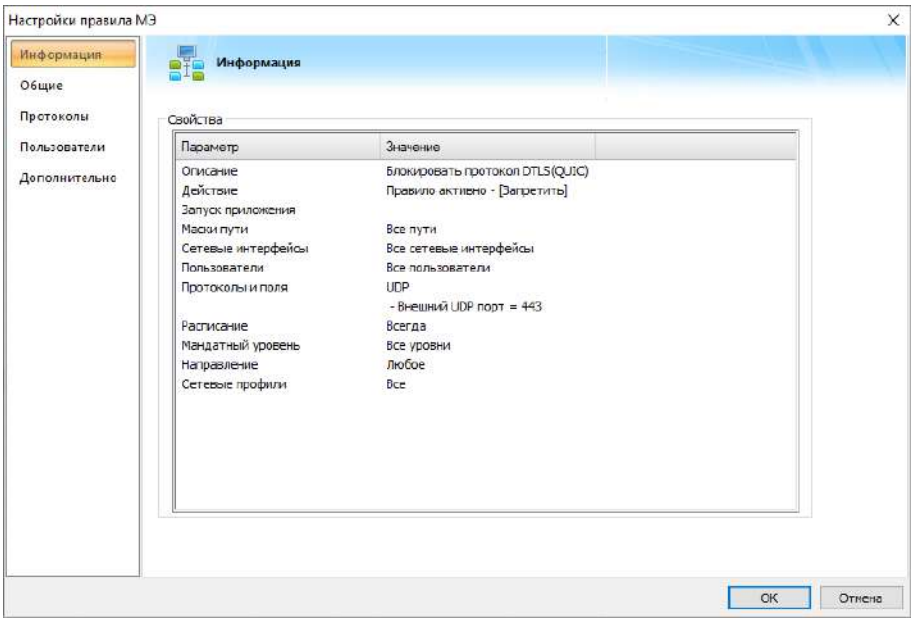


Рис. 243. Блокировка протокола DTLS (QUIC)

2. Отключить протокол в браузере на базе Chromium (например, Google Chrome, Edge Chromium) с помощью команды *//flags/#enable-quic.* **Пример**: в поисковой строке Google Chrome набрать команду chrome:*//flags/#enable-quic,* найти в списке строку «Experimental QUIC protocol» и отключить протокол.

Веб-контроль

Принцип управления веб-контроля аналогичен принципу работы правил МЭ. Необходимо создать набор правил, которые могут быть запрещающими, разрешающими или информирующими. В правилах веб-контроля указывается на какие URL-адреса они действуют, к какому содержимому и для каких пользователей применяются. Правила проверяются в заданном порядке, после срабатывания правила, проверка прекращается. Если ни одно из существующих правил не сработало, применяется правило по умолчанию. После обработки правил веб-контроля возможны следующие события:

- доступ к запрошенной информации с сервера,
- уведомление пользователя о блокировке веб-ресурса,
- предупреждение о нежелательном доступе к запрошенному веб-ресурсу.

Для перехода к управлению правилами веб-контроля необходимо открыть подкатегорию «МЭ» → «Фильтрация» → «Веб-контроль».

На информационной панели находится список правил веб-контроля и основные данные по ресурсам и пользователям, для которых они назначены: расписание, приложения, сайты, типы данных, ключевые слова и т. д. (рис. 244).

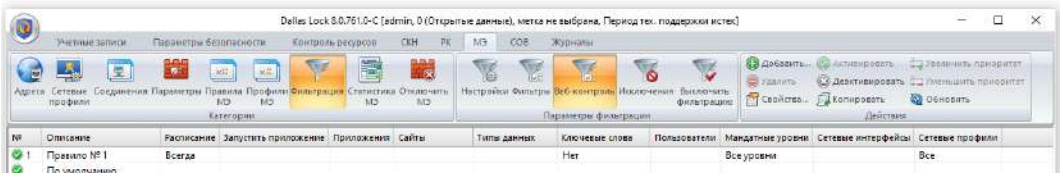


Рис. 244. Панель настройки правил веб-контроля

Существует возможность создания правила и копирования уже имеющегося, удаления, просмотра свойств и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

При создании правила веб-контроля появится окно «Создание правила веб-контроля» в котором доступно 6 разделов.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 245).

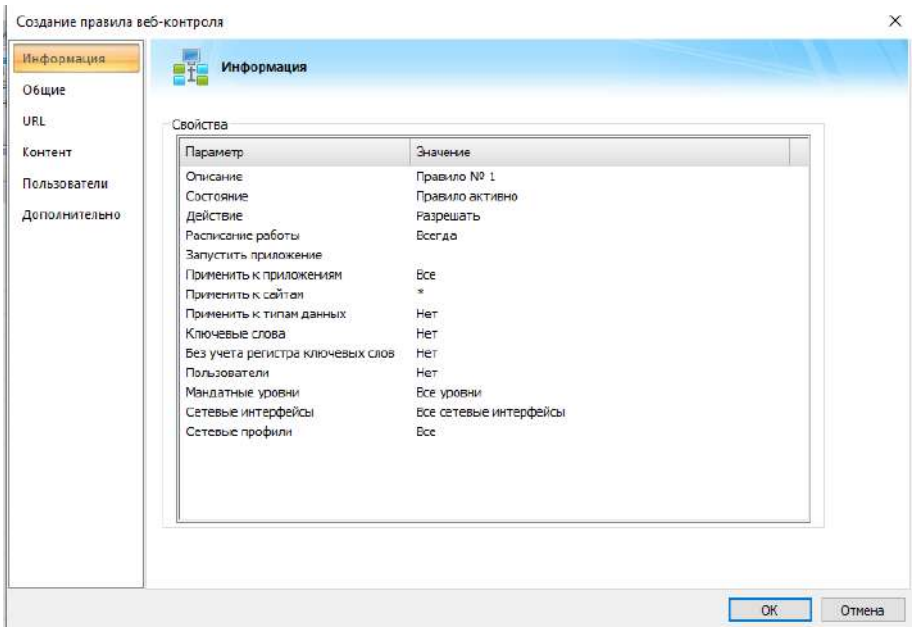


Рис. 245. Информация о правиле веб-контроля

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

В версии «С» раздел «Информация» дополнен параметром «Мандатный уровень», информирующий о том, для каких мандатных уровней применяется правило (рис. 246).

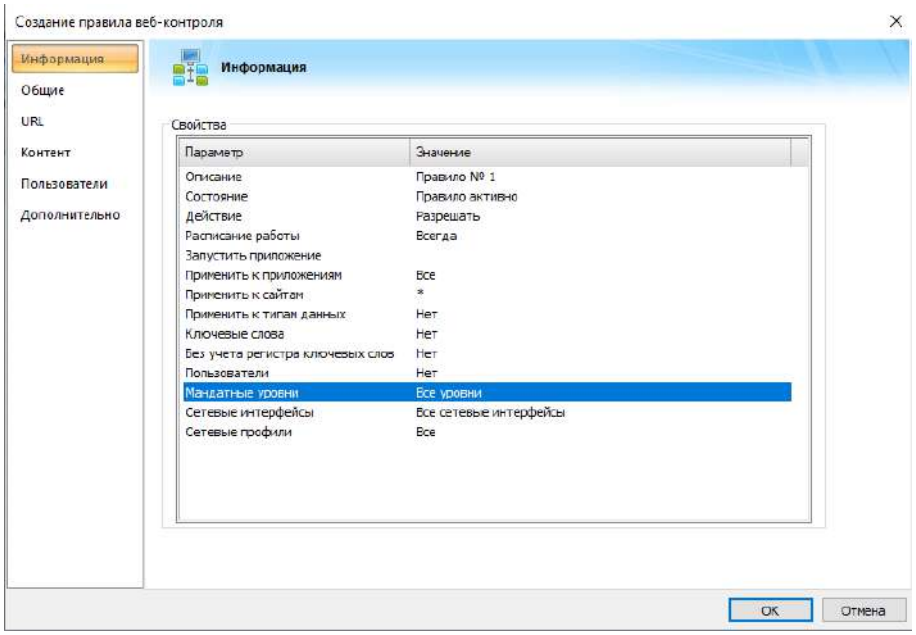


Рис. 246. Информация о правиле веб-контроля для редакции «С»

В разделе «Общие» представлены основные настройки правила веб-контроля (рис. 247).

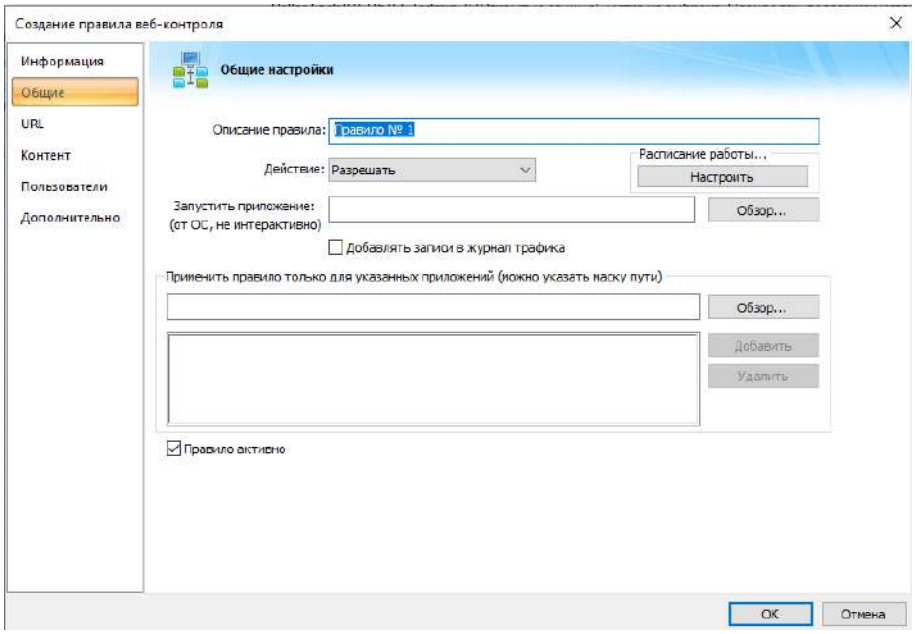


Рис. 247. Общие настройки правила веб-контроля

Примечание. Если был задан параметр «Запустить приложение», то при срабатывании правила, приложение запустится от имени ОС и не интерактивно. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе «URL» можно задать URL-адреса веб-ресурсов, к которым будет применяться данное правило (рис. 248). Также есть возможность указать маску, когда требуется применить правило для множества схожих URL-адресов веб-ресурсов, например, «mail.ru*». Символ «*» заменяет любую последовательность символов. Список URL-адресов возможно загрузить из файла, если предварительно он был составлен и сохранен.

Примечание. Составленный список URL-адресов должен быть сохранен в кодировке UTF-8 без маркера последовательности байтов (Byte Order Mark).

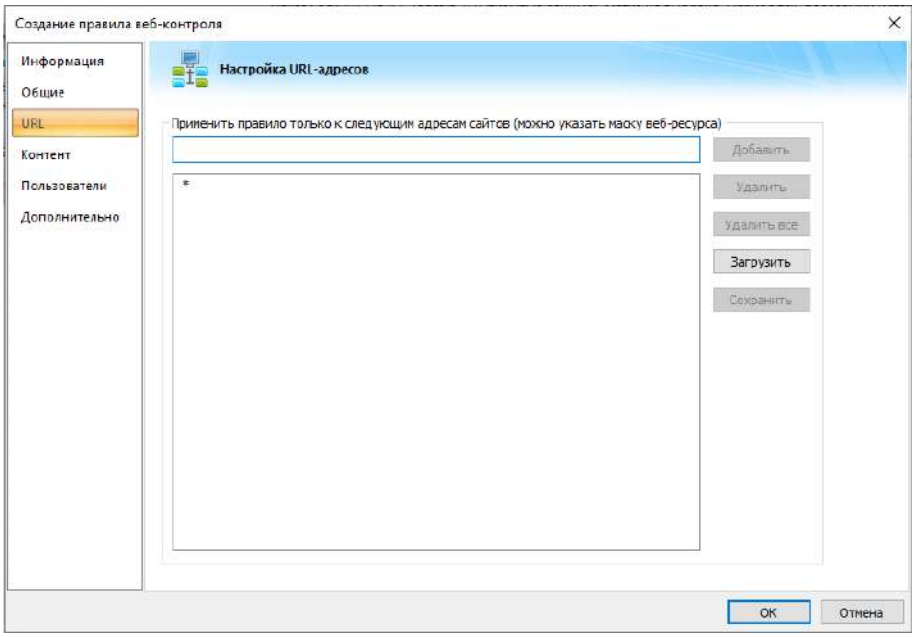


Рис. 248. URL-адреса

Раздел «Контент» позволяет настроить контроль доступа пользователей к веб-ресурсам по типам данных и ключевым словам, предотвращая показ нежелательного содержимого (рис. 249).

При фильтрации по типу данных (видео, звуковые файлы и т. д.) правило применяется ко всем веб-

ресурсам, которые содержат любой из выбранных типов.

При фильтрации по ключевым словам как правило применяется ко всем веб-ресурсам, которые содержат любое из введенных ключевых слов. Например, при наличии ключевых слов «открытые вакансии» и «калейдоскоп» для блокирования будет достаточно нахождения слова «калейдоскоп» или полного сочетания «открытые вакансии». Список ключевых слов возможно загрузить из файла, если предварительно он был составлен и сохранен. Возможна фильтрация ключевых слов без учета регистра.

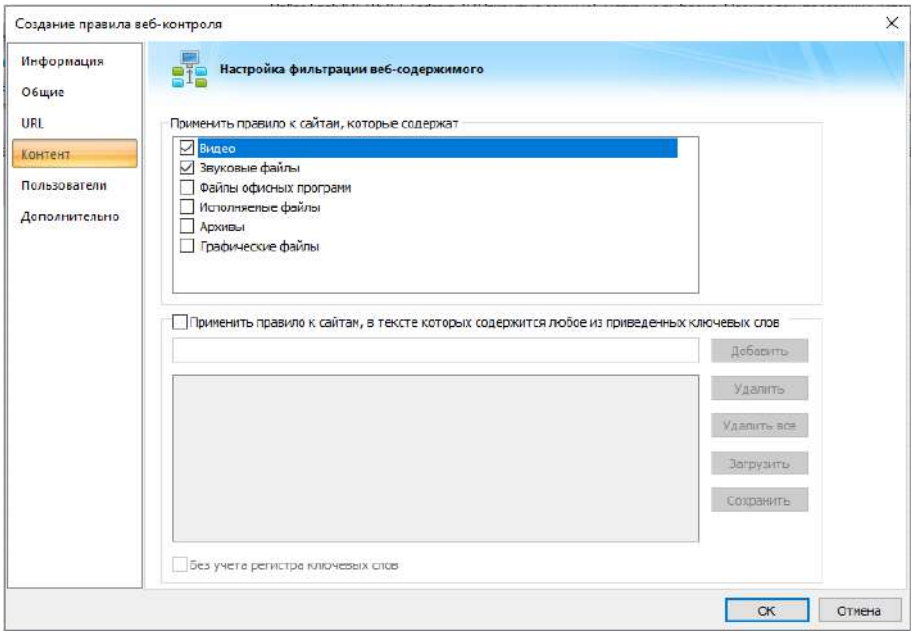


Рис. 249. Настройка блокируемого контента

В разделе «Пользователи» отображается список пользователей, к которым будет применяться созданное правило.

Отметив пункт «Автоматический поиск пользователей/групп» при последующем нажатии кнопок «Пользователи» и «Группы» будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки «Удалить» (рис. 250).

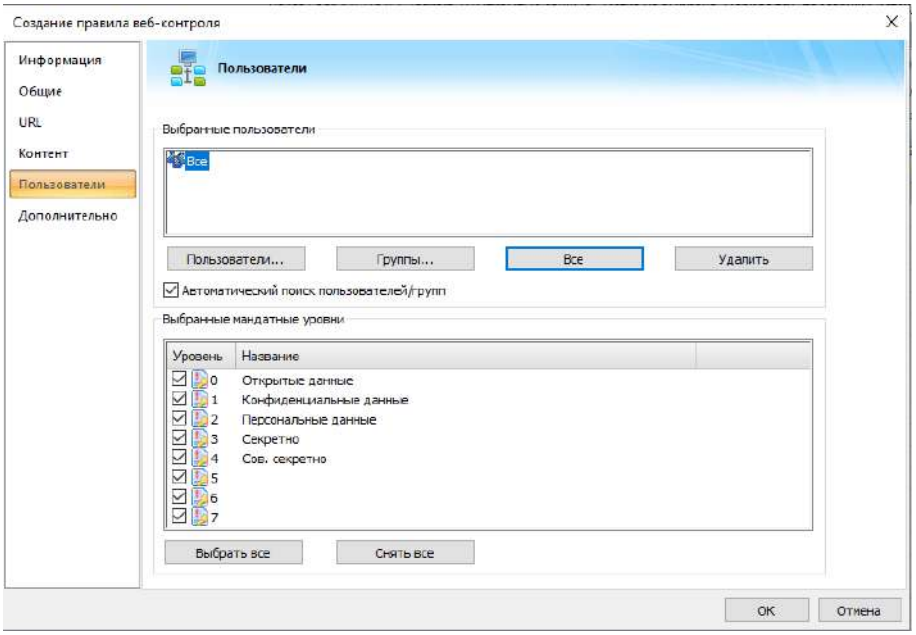


Рис. 250. Пользователи для правила веб-контроля

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (рис. 251).

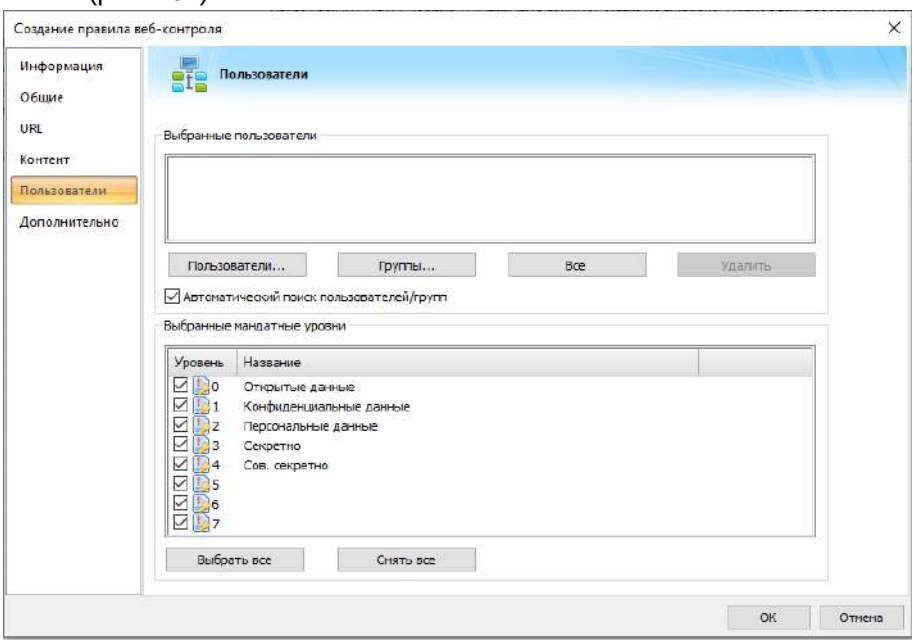


Рис. 251. Пользователи правила веб-контроля для редакции «С»

В разделе «Дополнительно» существует возможность применения текущего правила МЭ только для определенных сетевых адаптеров и (или) сетевых профилей. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку «Добавить». Удаление производится выбором адаптера из списка и нажатием кнопки «Удалить». Для редактирования списка сетевых профилей правила МЭ необходимо отметить сетевые профили (рис. 252).

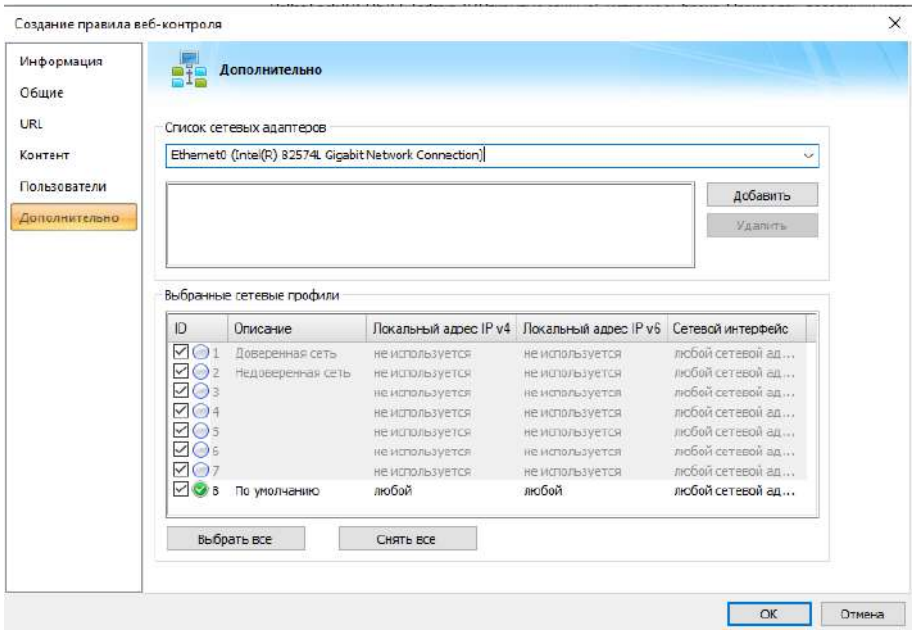


Рис. 252. Дополнительно

Примечание. Для перехвата веб-контента выполните одно из следующих действий.

1. Создать правило МЭ по блокировки протокола DTLS.

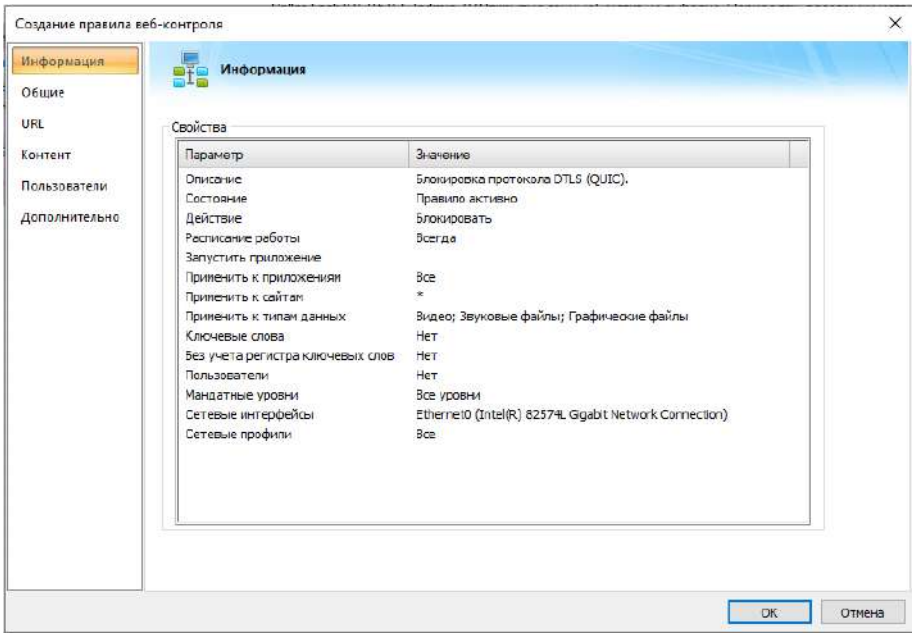


Рис. 253. Блокировка протокола DTLS (QUIC)

2. Отключить протокол DTLS в браузере на базе Chromium (например, Google Chrome, Edge Chromium) с помощью команды *//flags/#enable-quic*. **Пример**: в поисковой строке Google Chrome набрать команду chrome*://flags/#enable-quic,* найти в списке строку «Experimental QUIC protocol» и отключить протокол.

Исключения

Исключения необходимы для работы с указанными хостами вне зависимости от настроенной фильтрации при режиме работы «Фильтровать все, кроме исключений» (рис. 254). При режиме работы «Фильтрация активна только для хостов-исключений», фильтрация будет применяться только к указанным в исключениях хостам.

Для создания правила исключения, необходимо выбрать действие «Добавить», после чего на информационной панели появится новое правило с пустым полем, где необходимо ввести IP-адрес или DNS-имя.

Для поддержания актуальных адресов хостов исключений, адреса исключений периодически обновляются.

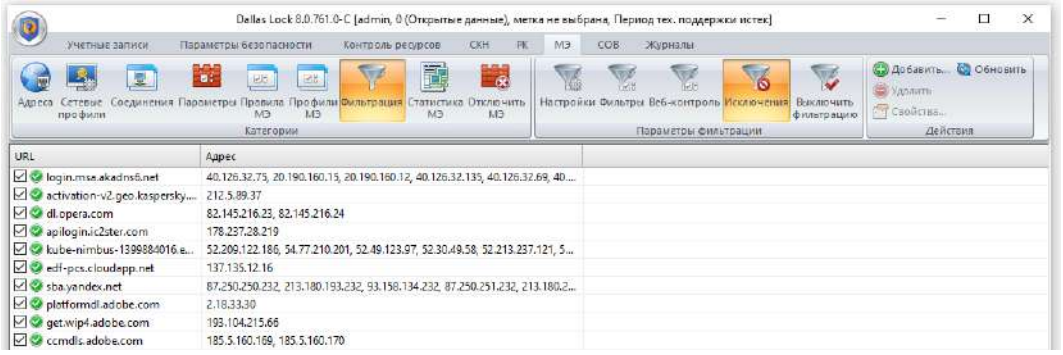


Рис. 254. Исключения фильтрации

Для того, чтобы удалить исключения нужно, выделив правило, нажать правой кнопкой мыши и выбрать в контекстном меню действие «Удалить».

Внимание! Для работы системы защиты в виртуальных инфраструктурах Dallas Lock с VMware vSphere 5.5, необходимо добавить СБ в исключения фильтрации Dallas Lock 8.0 Сервера виртуализации vCenter.

Выключение фильтрации

Для временного прекращения фильтрации МЭ необходимо нажать кнопку «Выключить фильтрацию» на вкладке «Фильтрация» и в появившемся окне подтвердить действие (рис. 255).

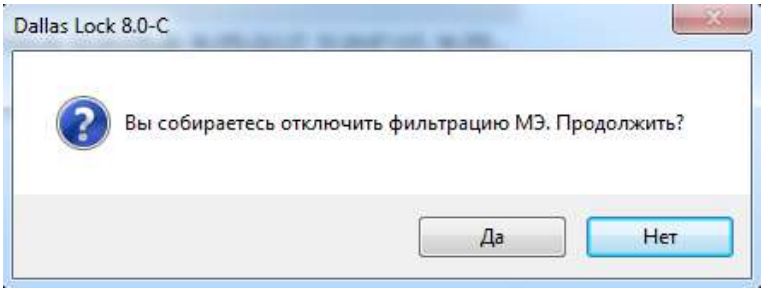


Рис. 255. Отключение фильтрации МЭ

15.2.8 Статистика МЭ

В категории «Статистика МЭ» содержится информация о принятом и отправленном трафике за указанный период. Полученные данные можно обновить и сбросить посредством нажатия соответствующих кнопок на панели «Действия». Справа от панели находится диаграмма, отображающая статистику всего входящего и исходящего трафика с указанием количества информации и времени, когда она была получена.

Весь трафик

Параметр «Весь трафик» отображает объем информации, полученный за сутки, неделю, месяц или весь период работы Dallas Lock.

Примечание. При ознакомлении с данными статистики нужно принимать во внимание то, что учет трафика производится с начала суток (00 часов 00 минут), с начала недели (понедельник), с первого дня месяца (1-е число отчетного месяца).

Для отображения информации нужно нажать кнопку «Весь трафик» на панели «Параметры статистики». Панель действий включает в себя опции обновления и сброса текущей информации (рис. 256).

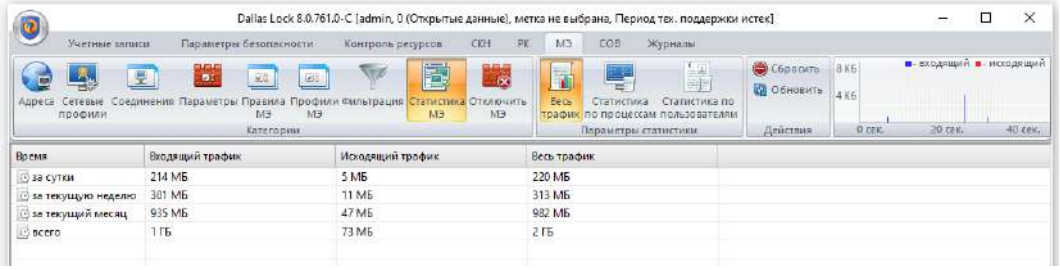


Рис. 256. Статистика межсетевого экрана

Статистика по процессам

В параметре «Статистика по процессам» отображается трафик, использованный рабочими процессами, с указанием отчетного периода (рис. 257).

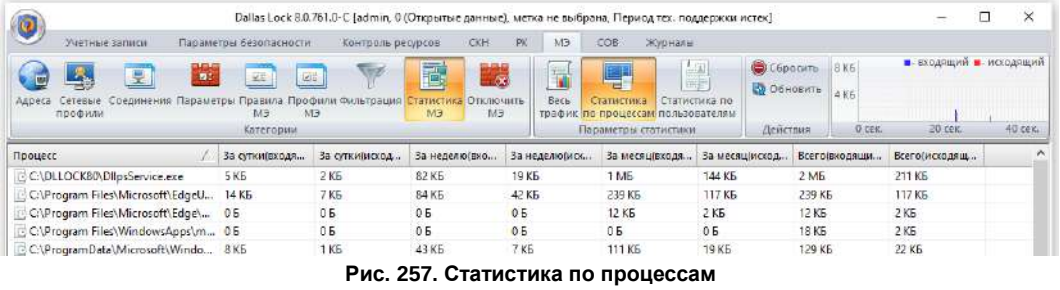


Рис. 257. Статистика по процессам

Статистика по пользователям

«Статистика по пользователям» показывает, сколько было отправлено/принято трафика во время работы каждого системного процесса за отчетный период (рис. 258).

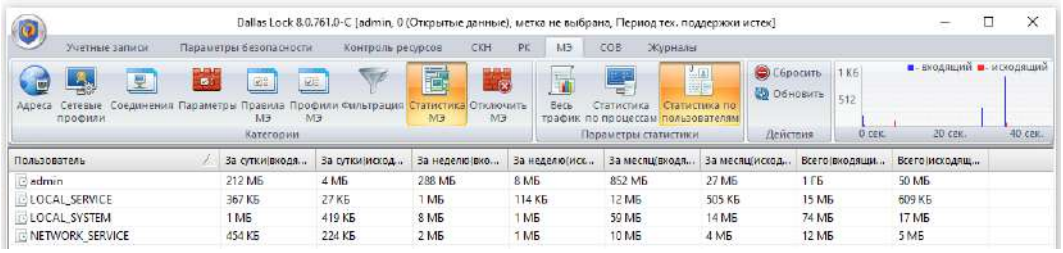


Рис. 258. Статистика по пользователям

15.2.9 Отключение МЭ

Для временного прекращения работы МЭ необходимо нажать кнопку «Отключить МЭ» и в появившемся окне подтвердить действие (рис. 259).

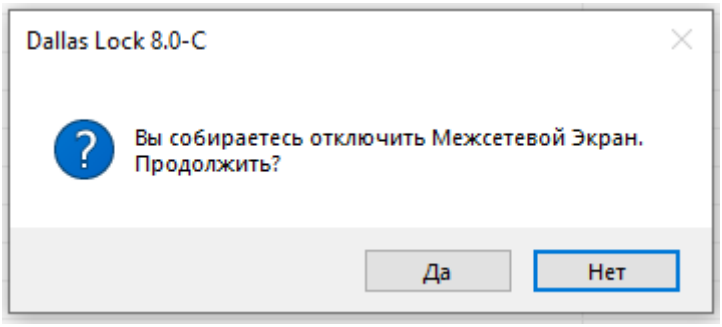


Рис. 259. Отключение межсетевого экрана

15.3 Журналы МЭ

В Dallas Lock 8.0 реализована функция сбора и отображения информации о сетевых пакетах и установленных соединениях ТС (или компьютера).

Для того, чтобы ознакомиться с данной информацией, нужно открыть общую вкладку «Журналы» и выбрать «Журнал пакетов МЭ» или «Журнал соединений МЭ» или «Журнал трафика фильтрации МЭ». По умолчанию журналы отключены, и сбор информации не ведется.

На панели «Действия» расположено три кнопки. При нажатии кнопки «Обновить» отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах МЭ, нужно нажать кнопку «Архивировать». После этого в папке программы появится файл с архивом данных. Для открытия такого файла нужно использовать категорию «Журнал из файла» и в ее окне на панели действий нажать кнопку «Открыть журнал», а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Кнопка «Экспорт» отвечает за сбор и конвертирование информации журналов межсетевого экрана в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку «Экспорт», указать имя файла и выбрать место для его хранения.

Примечание. При открытии «Журнала из файла», в окне выбора файлов возможно выбрать несколько журналов одного типа. При выборе разных типов появится сообщение об ошибке.

Для начала фиксирования и отображения информации в журналах МЭ необходимо внести уточнения в параметры. Настройки журналов МЭ находятся во вкладке «Параметры безопасности» → «Аудит» и задаются через четыре параметра (рис. 260).

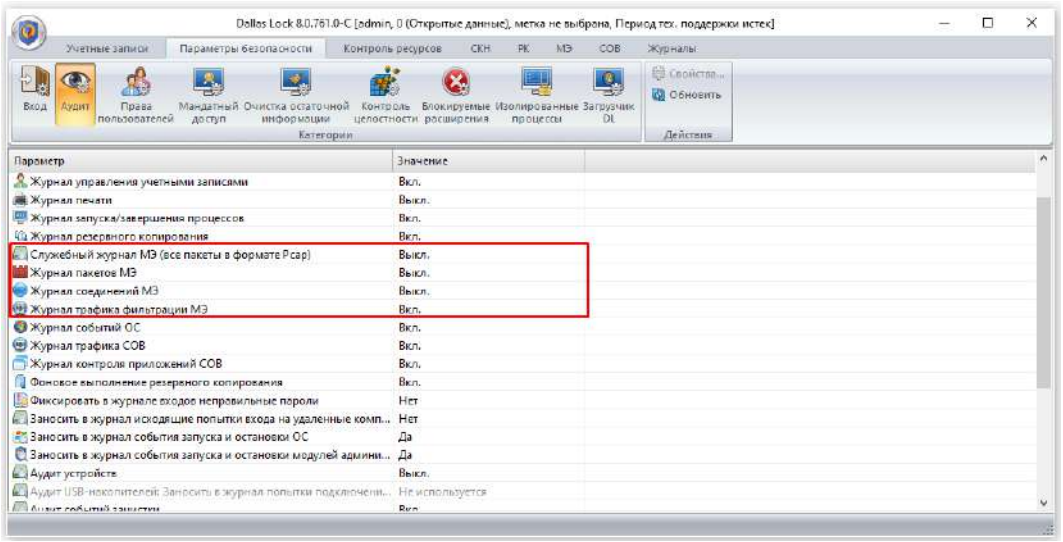


Рис. 260. Основные параметры работы журналов

15.3.1 Служебный журнал

Служебный журнал нужен для создания файла со списком всех зафиксированных пакетов в формате pcapng, в случае возможных проблем детектирования пакетов и может понадобиться при обращении в службу технической поддержки.

Чтобы включить служебный журнал МЭ, необходимо нажать правой кнопкой мыши на параметре «Служебный журнал МЭ (все пакеты в формате Pcap)» и в появившемся окне выбрать пункт «Вкл.» и нажать кнопку «ОК» (рис. 261).

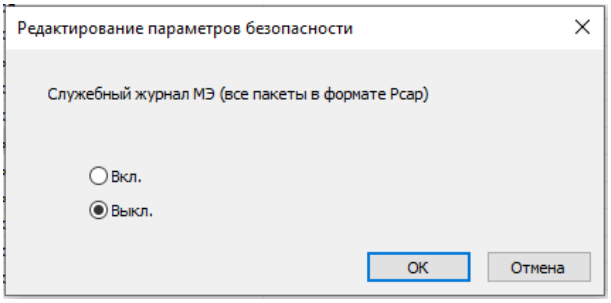


Рис. 261. Отключение ведения служебного журнала

Журнал располагается в папке DL, например, «C:\DLLOCK80\Firewall\Logs» и его имя может зависеть от названия используемого сетевого адаптера. Например, имя файла журнала может быть таким «C:\DLLOCK80\Firewall\Logs\VMware_Accelerated_AMD_PCNet_Adapter 2015-04-30.pcapng».

Внимание! Данный журнал необходимо включать только в случае возможных проблем детектирования пакетов, иначе будет проводиться слишком подробный аудит, что может привести к росту объема лог-файлов и уменьшению свободного места на жестком диске, а также к падению производительности работы в целом.

15.3.2 Журнал пакетов МЭ

Журнал пакетов содержит в себе сведения об отправленных и принятых сетевых пакетах, прошедших через межсетевой экран.

Для того чтобы включить «Журнал пакетов МЭ» необходимо перейти на вкладку «Параметры безопасности» → «Аудит»», нажать правой кнопкой мыши на «Журнал пакетов МЭ», выбрать «Свойства» и в появившемся окне выбрать пункт «Вкл.» и нажать кнопку «ОК» (Рис. 262).

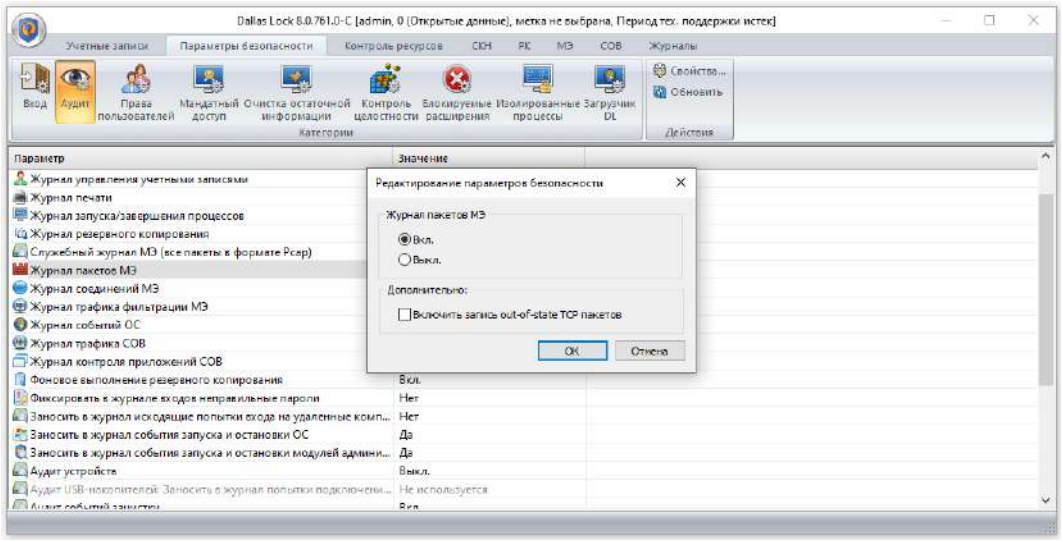


Рис. 262. Свойства журнала пакетов МЭ

Для отображения фиксируемой информации в журнале необходимо настроить правила межсетевого экрана (см. «Правила МЭ»). Следует на вкладке «Общие» в окне «Настройки правила МЭ» активировать правило и пункт «Уведомление в журнал пакетов»(Рис. 263).

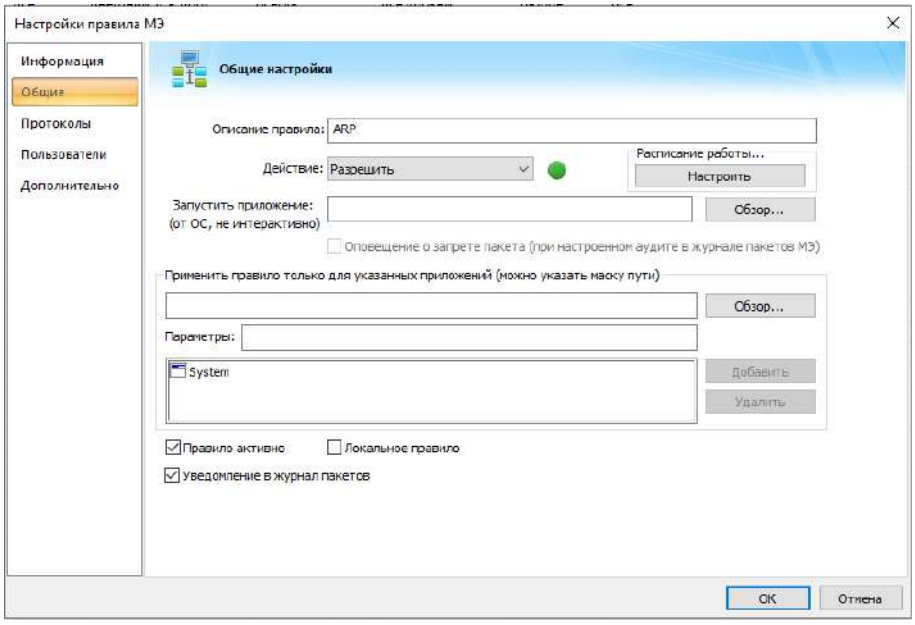


Рис. 263. Настройка уведомления в журнал пакетов

Параметр «Мандатный уровень» доступен только для Dallas Lock 8.0 редакции «С».

После настройки правил межсетевого экрана в журнале пакетов во вкладке «Журналы» начнется сбор и отображение информации по указанным при настройке сетевым пакетам (рис. 264).

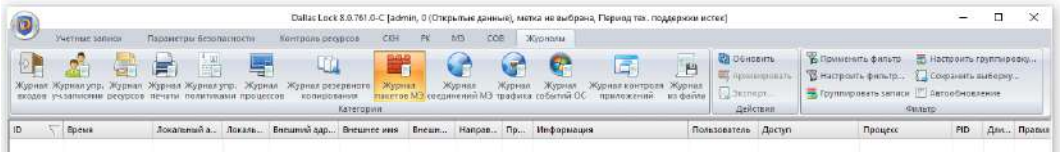


Рис. 264. Журнал пакетов МЭ

15.3.3 Журнал соединений

Журнал соединений отображает информацию об осуществленных в процессе работы МЭ сетевых соединениях. Для осуществления дальнейших настроек необходимо перейти на вкладку «Параметры безопасности», выбрать параметр «Журнал соединений МЭ» и вызвать окно настройки журнала через контекстное меню или панель «Действия» (рис. 265).

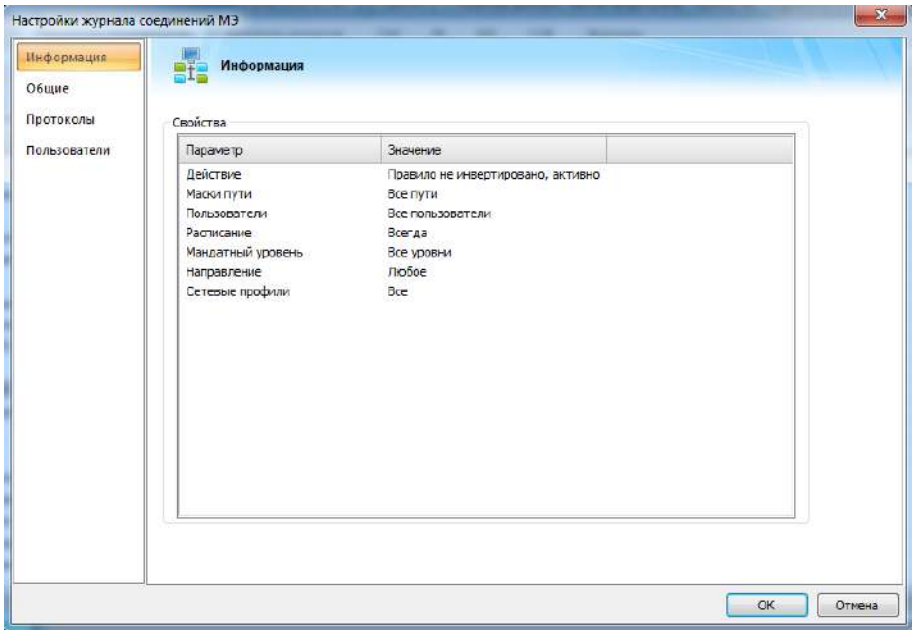


Рис. 265. Настройки журнала соединений МЭ

Настройки отображения информации, собранной журналом соединений МЭ идентичны настройкам правил работы межсетевого экрана (см. «Правила МЭ»). Исключение составляет отсутствие пункта «Дополнительно» и описание правила, оно присваивается по умолчанию.

Параметр «Мандатный уровень» доступен только для Dallas Lock 8.0 редакции «С».

После настройки параметров в журнале соединений в общей вкладке «Журналы» начнется сбор и отображение информации по указанным при настройке сетевым соединениям (рис. 266).

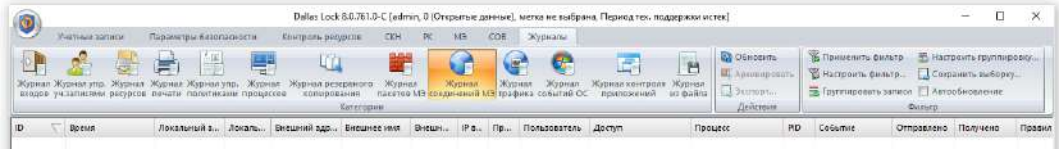


Рис. 266. Журнал соединений МЭ

15.3.4 Журнал трафика фильтрации МЭ

Журнал трафика фильтрации МЭ нужен для аудита трафика фильтрации для МЭ.

Чтобы включить журнал трафика фильтрации МЭ, необходимо нажать правой кнопкой мыши на параметре «Журнал трафика фильтрации МЭ» и в появившемся окне выбрать пункт «Вкл.» и нажать кнопку «Ок».

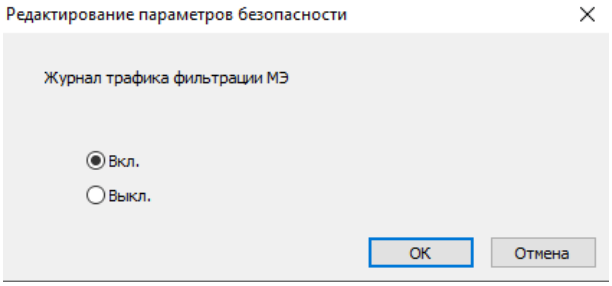


Рис. 267. Включение журнала трафика фильтрации МЭ

Журнал располагается в папке DL, например, «C:\DLLOCK80\Logs» и его имя может зависеть от названия используемого сетевого адаптера. Например, имя файла журнала может быть таким «C:\DLLOCK80\Logs\Journal.lg8».

16 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

16.1 Назначение и общие принципы работы

СОВ Dallas Lock является модулем СЗИ Dallas Lock 8.0, расширяющим функциональные возможности модуля «Межсетевой экран» СЗИ Dallas Lock 8.0. СОВ Dallas Lock обеспечивает обнаружение и блокирование основных угроз безопасности, выполняя одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализируя некоторые отдельные сетевые протоколы.

Модуль СОВ может быть установлен без активного модуля МЭ. В случае активности модуля МЭ модуль СОВ расширяет возможности МЭ. В случае неактивного модуля МЭ модуль СОВ работает независимо.

16.1.1 Возможности системы обнаружения вторжений

Примечание. Установка, удаление, активация и деактивация системы обнаружения воздействий описаны в разделе 2.2.

СОВ Dallas Lock обеспечивает защиту как от внутренних (локальных) нарушителей, так и от внешних нарушителей, включая угрозы со стороны сетей международного информационного обмена.

Ключевые особенности СОВ:

- возможность использования сигнатурных и эвристических методов для анализа сетевого трафика, журналов ОС и приложений на предмет нештатных ситуаций, а также попыток проведения вторжений;
- возможность обновления сигнатур сетевых атак и сигнатур анализа журналов ОС и приложений;
- обеспечение защиты от атак на сетевые протоколы на различных уровнях модели OSI;
- осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений;
- возможность анализа аномалий в поведении ОС и пользователей для выявления нештатных ситуаций;
- возможность анализа собранных данных СОВ о сетевом трафике в режиме, близкому к реальному масштабу времени.

Примечание. Модули СОВ и МЭ позволяют обнаруживать атаки внутри виртуальной сети VipNet.

Настройка СОВ доступна пользователям, которым назначена возможность изменения настроек СОВ, — администраторам ЗАРМ Dallas Lock (по умолчанию членам группы «Администраторы») и происходит из оболочки администратора во вкладке «СОВ».

Для просмотра и изменения политик и других параметров СОВ пользователь должен быть указан в значении параметров «СОВ: Изменение настроек» и «СОВ: Просмотр настроек» категории «Права пользователей» либо состоять в группе, указанной в данном параметре.

16.2 Основное

В категории «Основное» доступен просмотр статистики, обновлений и назначенных портов.

16.2.1 Статистика СОВ

В блоке «Основное» → «Статистика» отображаются следующие данные (рис. 268):

- статус СОВ;
- информация о состоянии сигнатур трафика;
- статистика по:
  - сетевым атакам,
  - сигнатурам трафика,

- подозрительной активности.

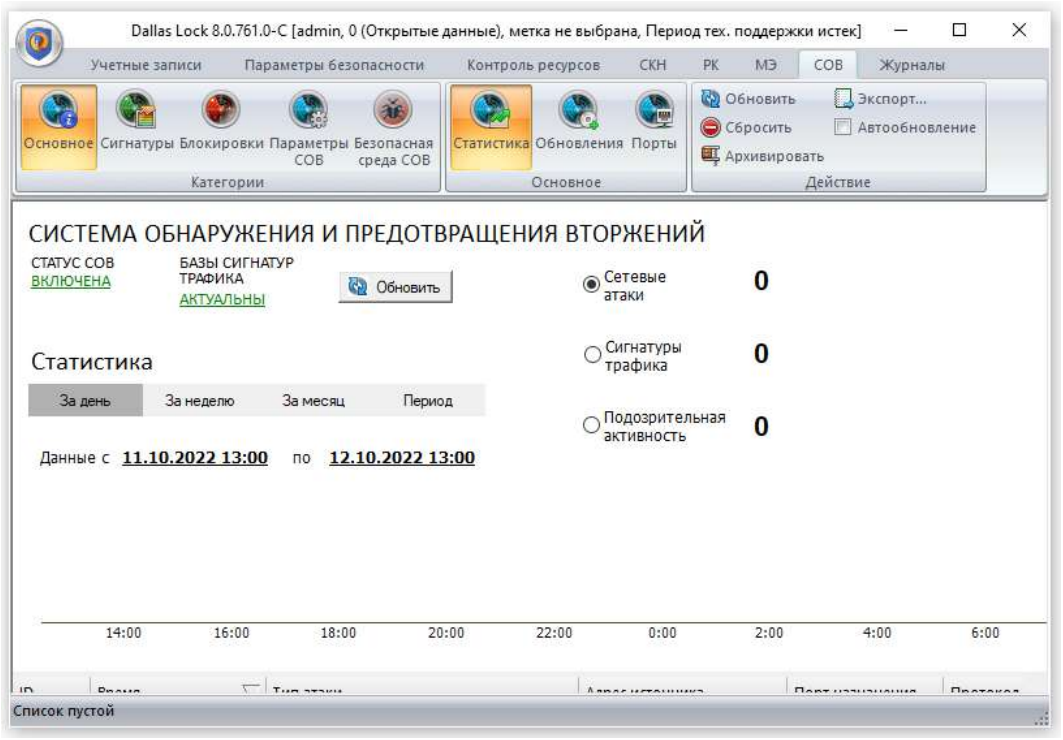


Рис. 268. Статистика сетевых атак

Статистика может быть отображена за день, неделю, месяц или другой выбранный период времени.

Примечание. При ознакомлении с данными статистики нужно принимать во внимание то, что учет трафика производится с начала суток (00 часов 00 минут), с начала недели (понедельник), с первого дня месяца (1-е число отчетного месяца).

Данные по статистике отображаются в гистограмме и в журнале под ней. События в журнале можно упорядочить по необходимому значению, кликнув на кнопку с названием столбца статистики. Дважды кликнув по записи в журнале можно получить полную информацию.

Панель действий позволяет обновить, сбросить статистику СОВ.

Для архивации собранной статистики необходимо нажать кнопку «Архивировать». Архивация записей будет произведена в формате «*.lg8».

По команде «Экспорт…» возможно экспортировать записи журнала статистики в одном из следующих форматов:

- Текст (видимы на экране);
- Текст (разделитель — табуляция);
- CSV (разделитель — точка с запятой);
- HTML;
- XML.

16.2.2 Обновления

Подкатегория «Обновления» отображает такую информацию как: название модуля, текущую версию обновления БРП, комментарий и статус работы автоматического обновления (рис. 269).

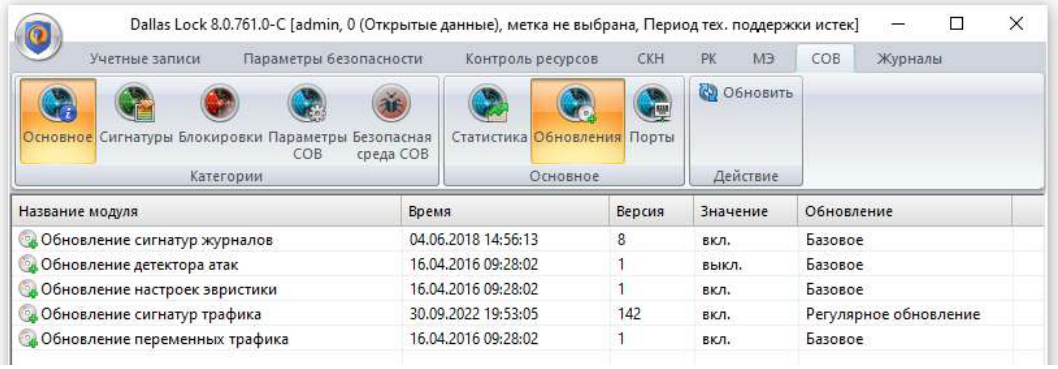


Рис. 269. Обновления

16.2.3 Порты

Подкатегория «Порты» отображает следующую информацию (рис. 270):

- Порты TCP для входящих и исходящих соединений (которые проверяются активными сигнатурами трафика).
- Порты UDP для входящих и исходящих соединений (которые проверяются активными сигнатурами трафика).
- Количество анализируемых входящих и исходящих TCP и UDP портов (которое проверяется активными сигнатурами трафика).
- Количество активных сигнатур трафика и журналов.

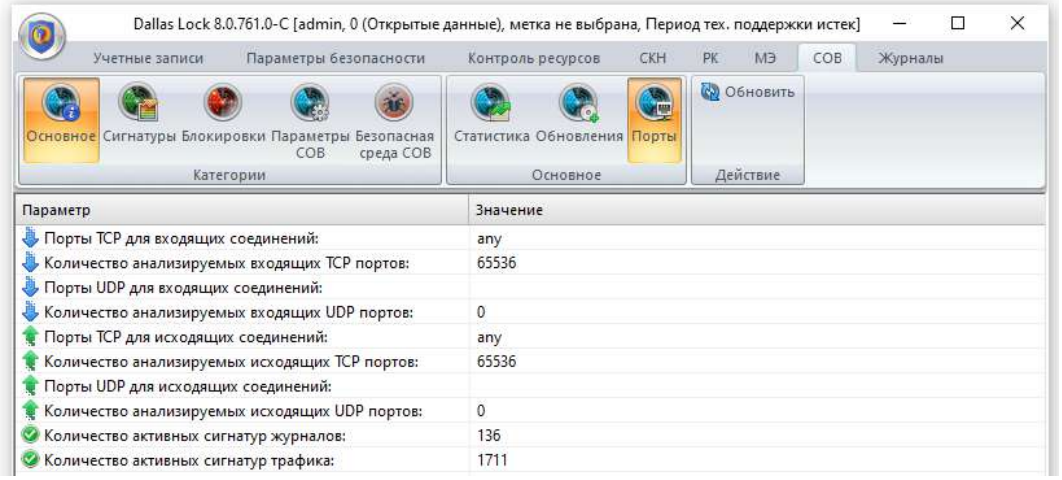


Рис. 270. Статистика портов

При двойном нажатии левой кнопкой мыши по одной из категории портов, откроется окно с детальным описанием.

16.3 Настройки сигнатур

Данная категория является инструментом управления сигнатурами СОВ. По умолчанию содержит готовые шаблоны наиболее типовых сигнатур.

Для перехода к управлению сигнатурами необходимо открыть вкладку «СОВ» и выбрать категорию «Сигнатуры».

Примечание. Если пользователь активировал/деактивировал сигнатуру через панель действий или контекстное меню, то она не считается измененной пользователем. При обновлении сигнатур каждая сигнатура заменяется только в том случае, если она не редактировалась пользователем через диалог редактирования настроек (т. е. не считается измененной пользователем) и находится в отключенном состоянии.

16.3.1 Сигнатуры журналов

На информационной панели находится древовидная структура сигнатур журналов и сведения о них: ID и статус правила, уровень тревоги, частота срабатывания и т. д. (рис. 271).

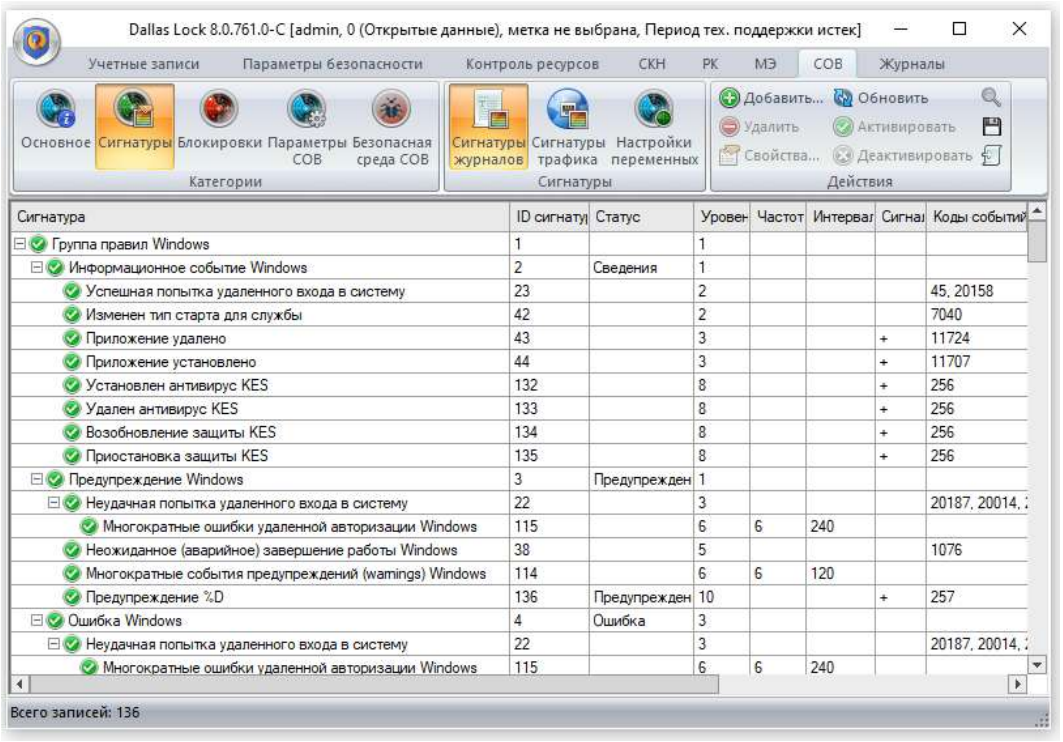


Рис. 271. Информационная панель настройки сигнатур журналов

Сигнатуры журналов анализируют журналы Windows и журналы антивируса Kaspersky Endpoint Security. Данные сигнатуры делятся на две группы правил.

Примечание. Для работы некоторых сигнатур группы правил KES, необходимо в настройках уведомлений антивируса Kaspersky Endpoint Security активировать режим «Информационные сообщения».

В зависимости от состояния сигнатуры значки могут принимать следующий вид:

— сигнатура активирована;

— сигнатура деактивирована;

— сигнатура активирована, но не функционирует, так как родительская сигнатура деактивирована.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели (рис. 272). Для отображения поисковой строки необходимо нажать на кнопку «Поиск» на панели «Действия».

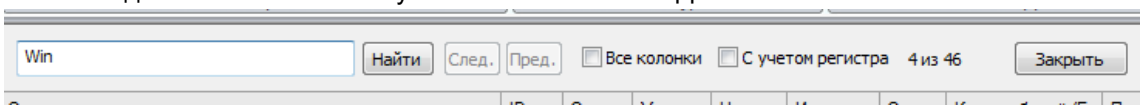


Рис. 272. Поиск по ключевым словам

Для того, чтобы изменить сигнатуру, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Свойства».

Существует возможность добавления новой сигнатуры, ее удаление, активации, деактивации, поиска и обновления. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

В меню «Настройка сигнатуры журналов» можно осуществить несколько уровней настроек текущей сигнатуры.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 273).

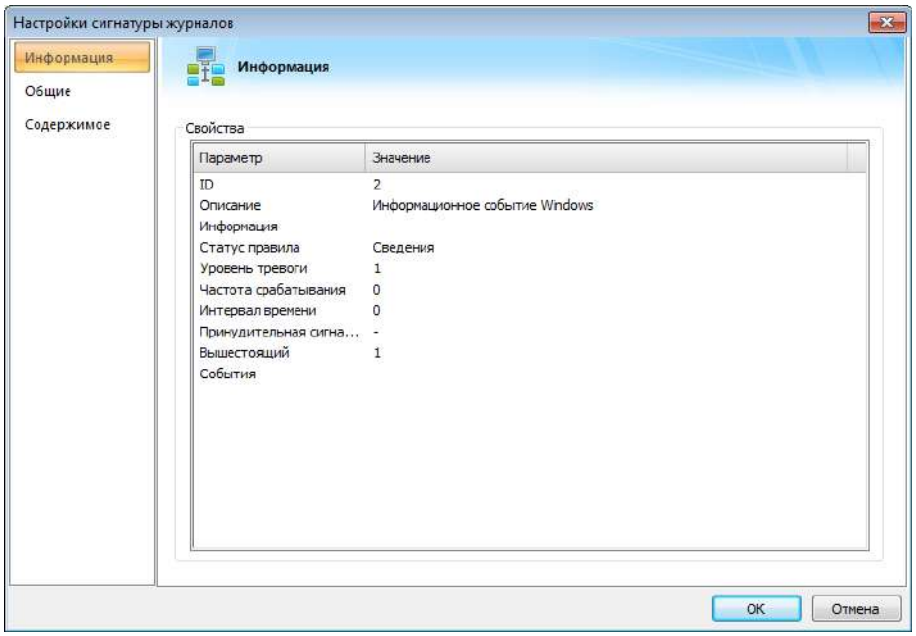


Рис. 273. Информация

В разделе «Общие» представлены основные настройки сигнатуры (рис. 274).

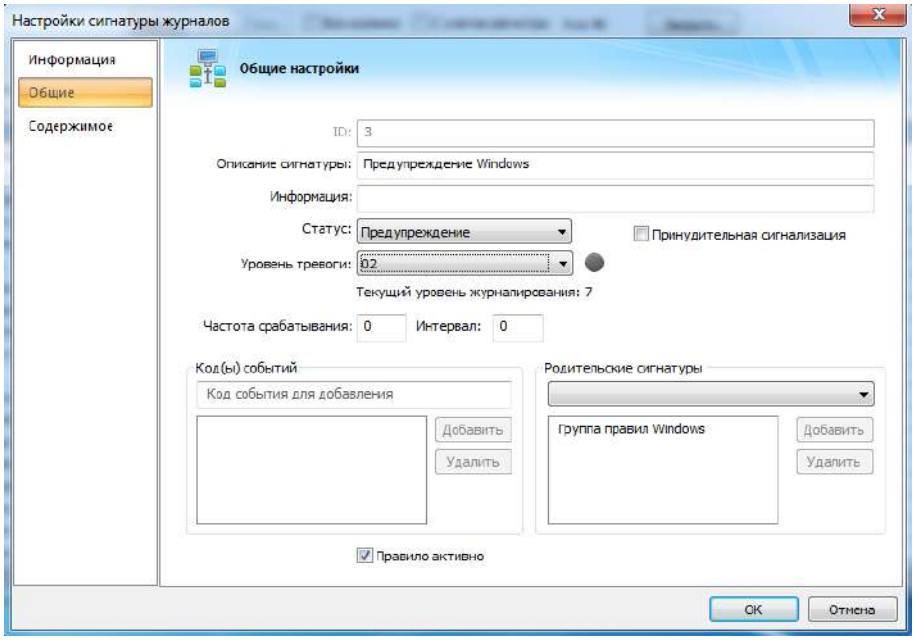


Рис. 274. Общие

В разделе «Содержимое» возможно указать ключевые слова (маску), которые должны содержаться в тексте описания события для срабатывания данной сигнатуры (рис. 275).

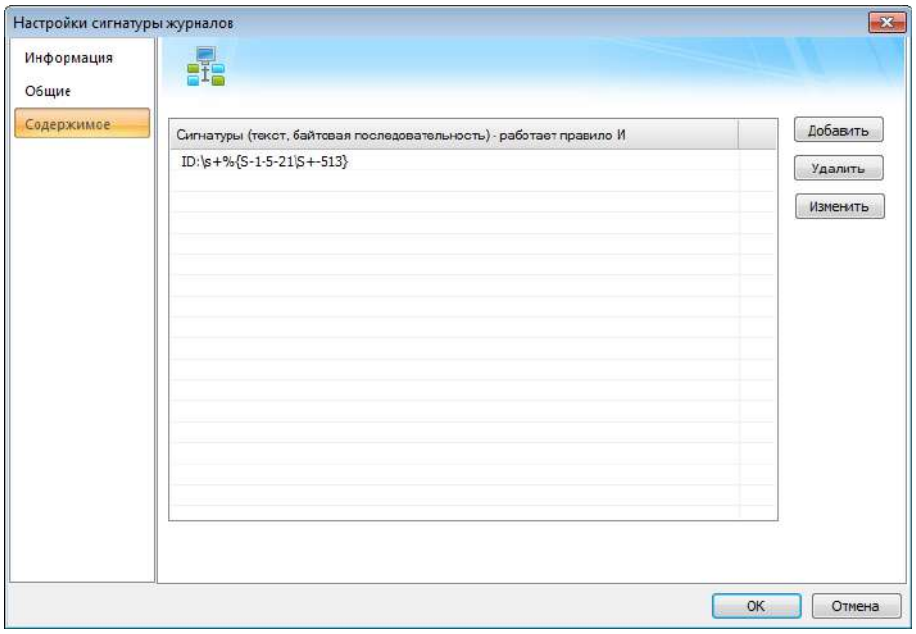


Рис. 275. Содержимое

Примечание. При отключении родительской сигнатуры дочерние сигнатуры будут неактивны. Включенные, но нефункционирующие сигнатуры, отмечаются иконкой восклицательного знака.

Действия по изменению сигнатур журналов фиксируются в журнале управления политиками.

16.3.2 Сигнатуры трафика

На информационной панели находится список сигнатур трафика и сведения о них: действие, протокол, источник, порт источника, направление и т. д. (рис. 276).

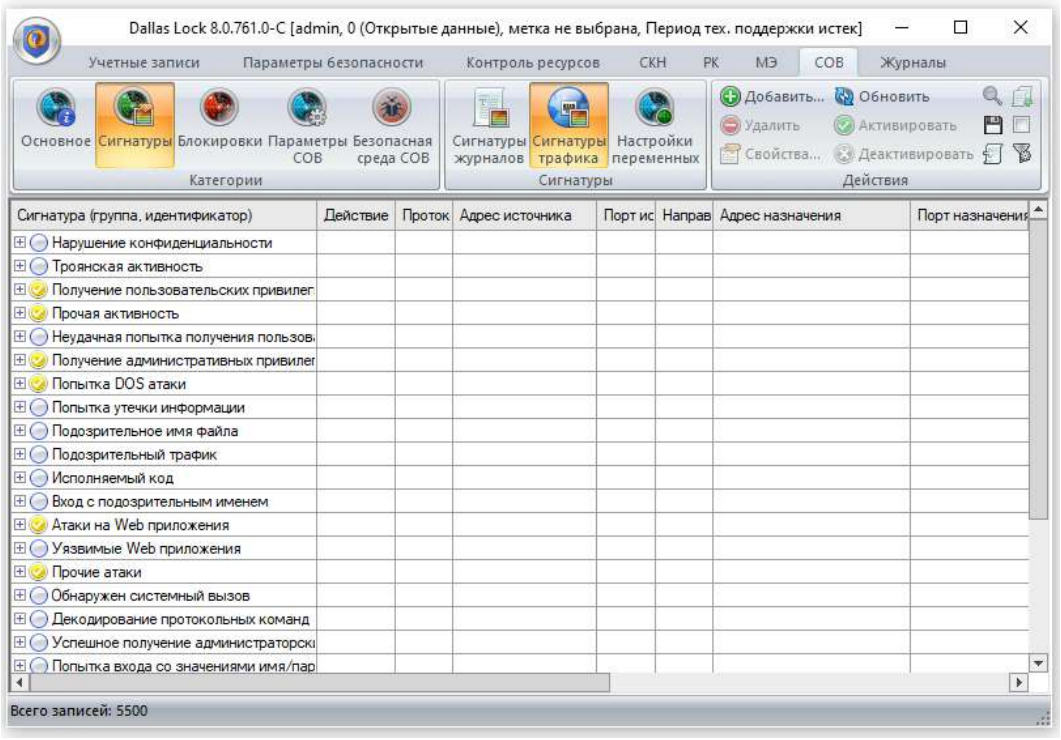


Рис. 276. Информационная панель настройки сигнатур трафика

В зависимости от состояния сигнатуры трафика, значки могут принимать следующий вид:

- — сигнатура или вся группа активированы;
- — сигнатура или вся группа деактивированы;

— активированы не все сигнатуры, входящие в группу.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку «Поиск» на панели «Действия».

Для того, чтобы изменить сигнатуру трафика, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Свойства». Кроме редактирования существующих сигнатур, есть возможность добавления новых сигнатур, удаление, активация, деактивация и поиск. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

В меню «Настройка сигнатуры трафика» можно осуществить несколько уровней настроек текущей сигнатуры.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 277).

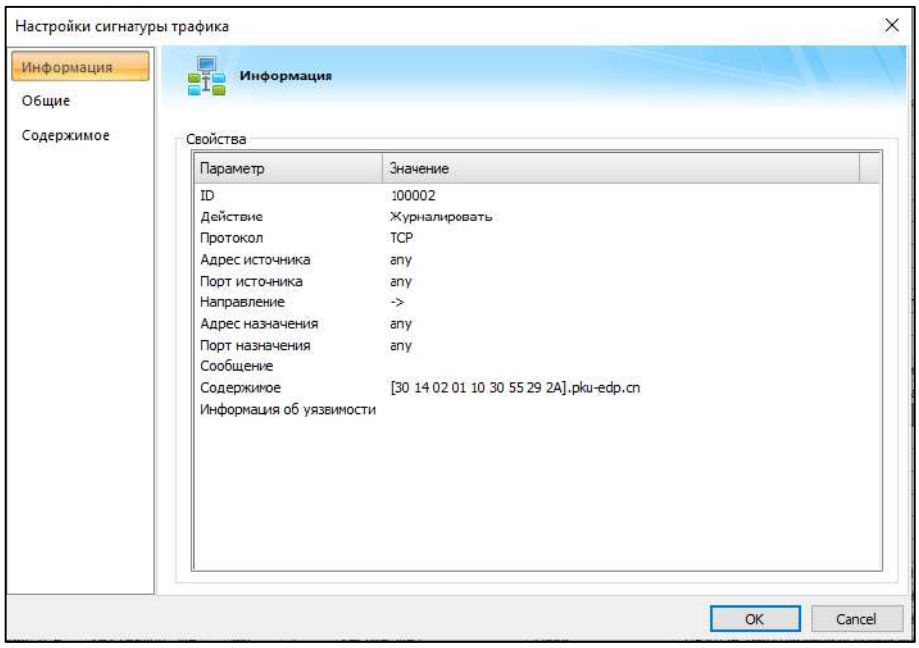


Рис. 277. Информация

В разделе «Общие» представлены основные настройки сигнатуры (рис. 278). Для упрощения настройки адресов и портов доступен выпадающий список для выбора переменных СОВ (см. «Настройки переменных»).

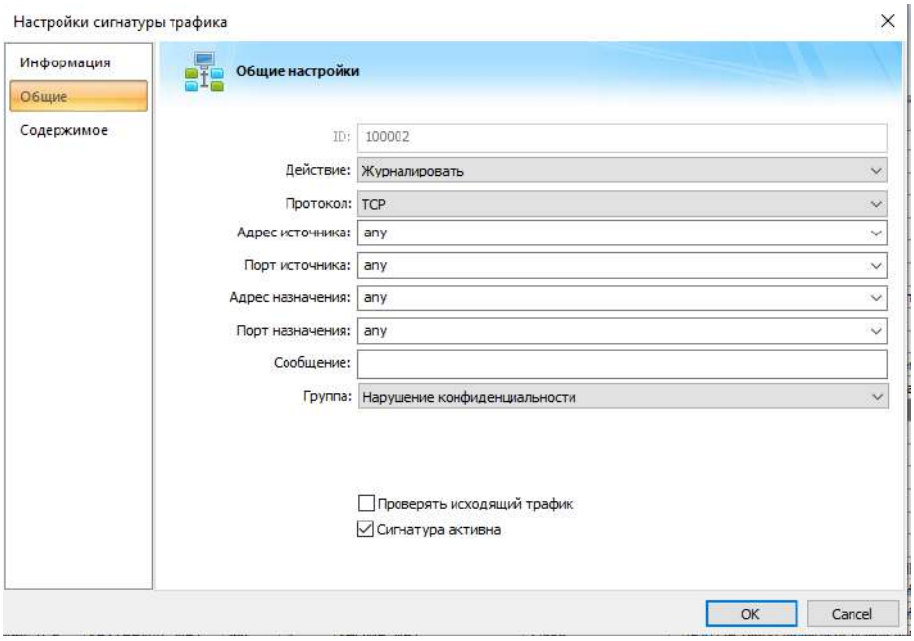


Рис. 278. Общие

В разделе «Содержимое» для срабатывания сигнатуры необходимо добавить ключевые слова или

байтовую последовательность, которая должна будет содержатся в проходящем сетевом трафике (рис. 279). Данный раздел активен только при ручном создании сигнатур трафика. Содержимое сигнатур трафика, поставляемых компанией ООО «Конфидент», может быть закрыто для просмотра.

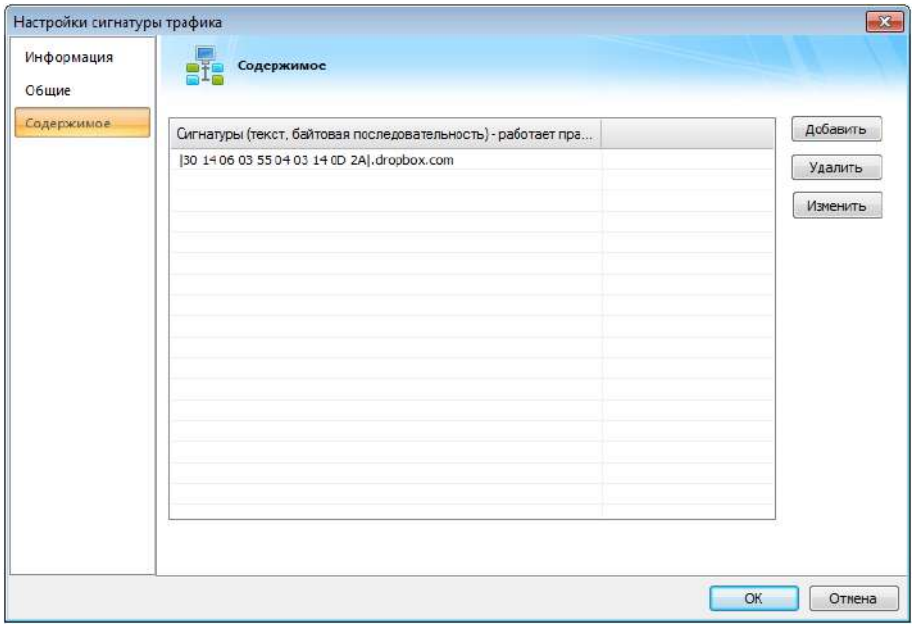


Рис. 279. Содержимое

При создании новых сигнатур трафика важно учитывать алгоритм их проверки:

1. СОВ проверяет сетевой трафик на соответствие протоколу, адресам и портам источника и назначения, указанным в настройках сигнатуры, и при обнаружении совпадения (в любом направлении) анализирует это соединение на содержимое.
2. Анализ соединения на содержимое выполняется в зависимости от параметра «Проверять на содержимое» либо только входящего трафика соединения, либо только исходящего трафика соединения, либо всего трафика этого соединения.
3. При обнаружении всех ключевых слов и байтовых последовательностей, указанных на вкладке «Содержимое», сигнатура срабатывает. При этом выполняется «Действие», указанное на вкладке «Общие».

Пример.

С сайта «www.lenta.ru» идет подозрительный трафик, поэтому необходимо разорвать соединение и заблокировать адрес.

Процесс создания новой сигнатуры происходит по тем же настройкам, что и корректировка уже готовой. Для создания новой сигнатуры нужно нажать правую клавишу мыши на информационной панели и выбрать «Добавить» в контекстном меню или нажать ту же кнопку на панели действий.

В разделе «Общие» устанавливается действие «Разорвать соединение и блокировать адрес», после чего указывается нужный тип протокола «TCP». Далее необходимо ввести адрес и порт источника, а также адрес и порт назначения. В данном случае изменяем только поле «Порт назначения» и вводим порт «80». После выбираем группу «Подозрительный трафик». Параметр «Двунаправленная» позволяет отслеживать трафик в обоих направлениях — в данном примере в этом нет необходимости.

Далее в разделе «Содержание», нажимаем «Добавить» и вводим ключевое слово «lenta.ru», которое будет содержаться в исходящем трафике с сайта «www.lenta.ru». После нажимаем кнопку «ОК» и активируем созданную сигнатуру.

Для более гибкой настройки условий обнаружения сигнатуры, можно использовать «Переменные трафика» (см. «Настройки переменных»).

Примечание. Сигнатура сработает ТОЛЬКО при точном совпадении указанных настроек. В случае **одновременного** задания нескольких ключевых слов или байтовых последовательностей для одной сигнатуры, например, два ключевых слова — для срабатывания сигнатуры должны выполниться **оба условия**.

Действия по изменению сигнатур трафика фиксируются в журнале управления политиками.

16.3.3 Настройки переменных

Параметр «Настройки переменных» позволяет задать сетевые адреса внутренней и внешней сети, серверы, TCP и UDP порты, используемые в сети, а также группировать их, чтобы затем использовать в пределах нескольких сигнатур (см. «Сигнатуры трафика») (рис. 280). При изменении значения переменной любая сигнатура, которая использует данную переменную, обновится в соответствии с новым значением переменной.

Переменные бывают двух типов — переменные диапазона адресов и переменные диапазона портов.

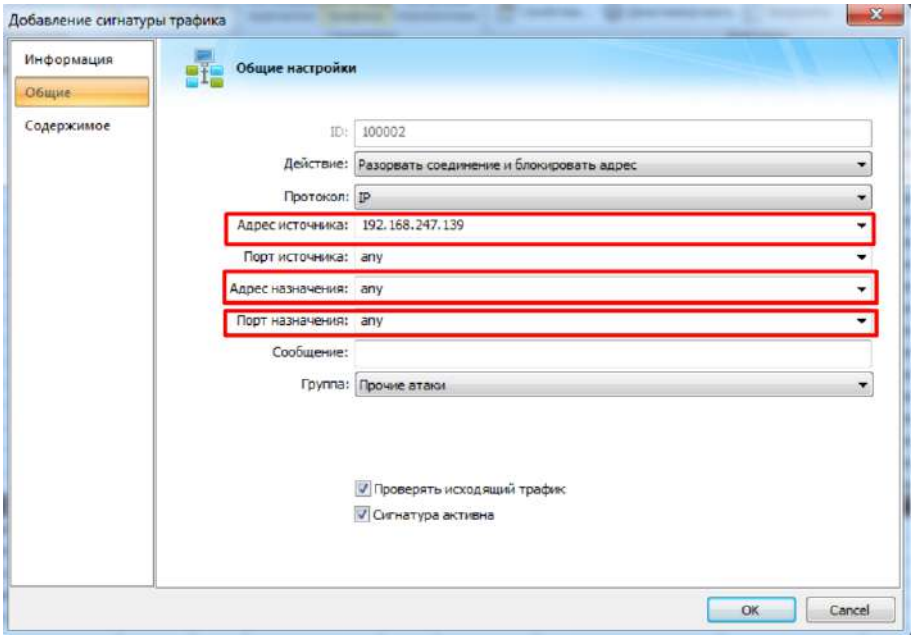


Рис. 280. Настройки сигнатуры трафика

На информационной панели находится список переменных трафика с их значениями (рис. 281).

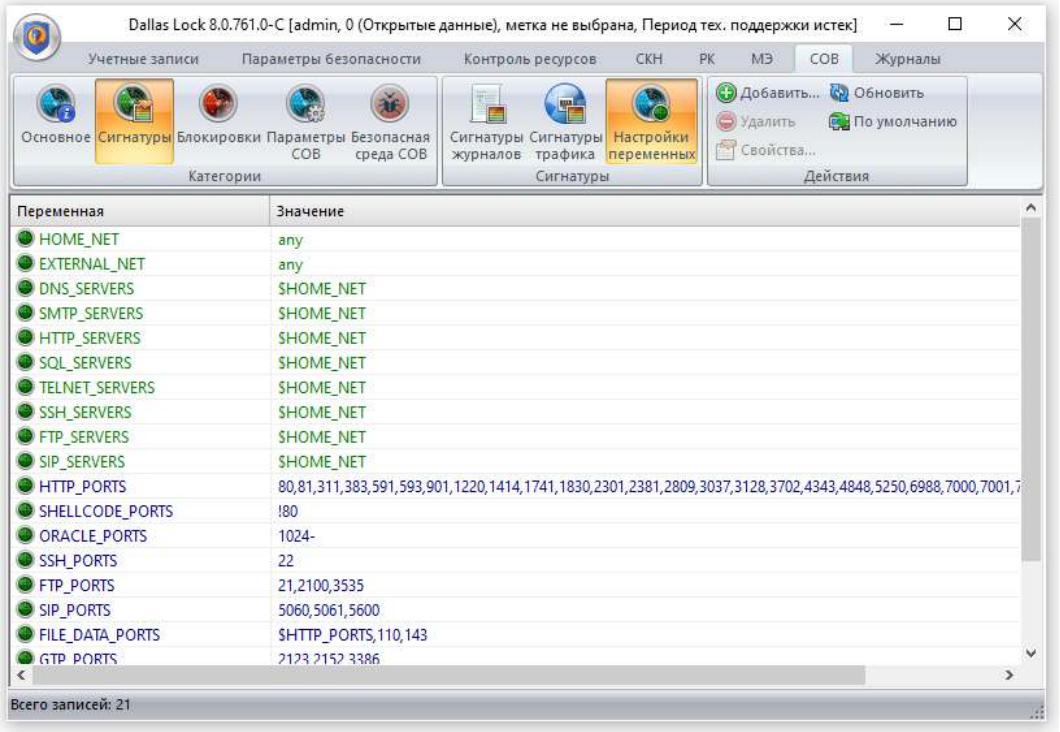


Рис. 281. Информационная панель настройки переменных трафика

HOME_NET
В данной переменной требуется задать диапазон внутренних IP-адресов. По умолчанию

переменная HOME_NET содержит значение «any», что относится к любому IP-адресу. Для того, чтобы изменить переменную, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Свойства». При настройке, возможно задать маску подсети и указать несколько IP-адресов включая их диапазон: «1.1.1.1, 1.1.2.1/24, 1.1.3.1-1.1.3.9»
EXTERNAL_NET
В переменной EXTERNAL_NET необходимо задать диапазон внешних IP-адресов. По умолчанию данная переменная содержит значение «any». СОВ будет реагировать на любой входящий или исходящий трафик. Для уменьшения нагрузки на ЗАРМ, возможно воспользоваться логическим отрицанием, используя символ «!». Например, сеть не являющееся HOME_NET имеет значение «!$HOME_NET».
Переменные SERVERS
Настройка переменных _SERVERS ничем не отличается от настройки переменных HOME_NET или EXTERNAL_NET.
Переменные PORTS
При настройке портов, возможно назначить один или несколько портов, непрерывный диапазон, инвертировать, а также указать значение другой переменной: • «80,81,311»; • «1024-»; • «!80»; • «$HTTP_PORTS». При задании избыточно широкого диапазона портов в рамках одного правила МЭ количество используемых для перехвата портов будет ограничено, и в первую очередь будут заполнены порты из списка подозрительных и неиспользуемых служебных портов (см. «Настройки эвристики»).

Действия по изменению переменных трафика фиксируются в журнале управления политиками.

16.4 Блокировки

16.4.1 Заблокированные адреса

В подкатегории «Заблокированные адреса» отображаются заблокированные IP и MAC адреса, а также сведения о них: дата, адрес, DNS, правило, описание блокировки и т. д. (рис. 282).

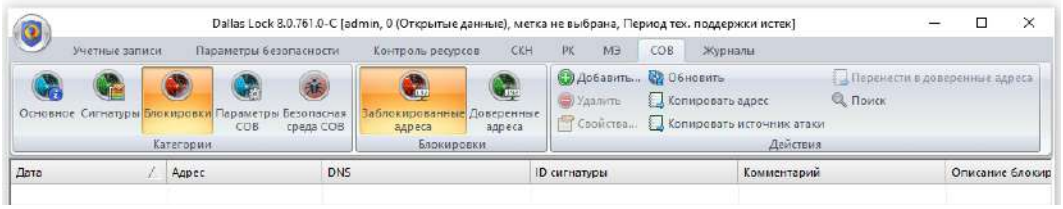


Рис. 282. Информационная панель заблокированных адресов

Существует возможность создания ручной блокировки адреса. Для этого необходимо выбрать действие «Добавить». Появится окно «Добавление блокировки СОВ», в котором необходимо указать IP или MAC и задать период блокировки (рис. 283).

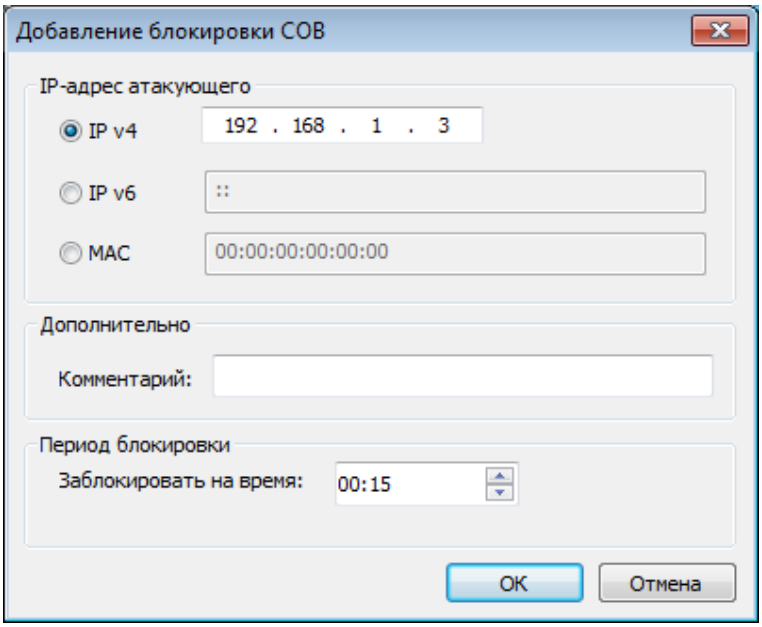


Рис. 283. Добавление блокировки СОВ

Примечание. Ручная блокировка несет в себе временный характер (максимальный период ручной блокировки — 23 часа 59 минут). Для бессрочной блокировки, необходимо добавить соответствующее правило в МЭ (см. «Правила МЭ»).

Для того, чтобы снять блокировку, нужно, выбрав один или несколько заблокированных адресов, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Удалить». Далее появится окно с просьбой подтвердить операцию.

Для копирования адреса или источника атаки необходимо выбрать заблокированный адрес и нажать соответствующую кнопку на панели «Действия» или воспользоваться контекстным меню.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку «Поиск» на панели «Действия».

Действия по изменению списка заблокированных адресов фиксируются в журнале управления политиками.

16.4.2 Доверенные адреса

В подкатегории «Доверенные адреса» отображаются доверенные IP и MAC адреса, а также сведения о них: адрес, комментарий, отметка в журнале (рис. 284).

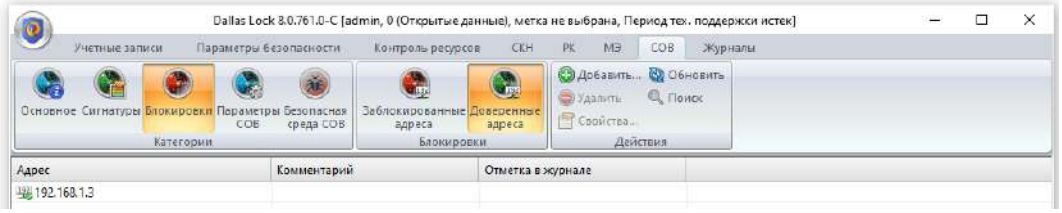


Рис. 284. Информационная панель доверенных адресов

Для того, чтобы добавить доверенный адрес, необходимо выбрать действие «Добавить». Дополнительно возможно написать комментарий и включить опцию «Заносить в журнал обнаруженные атаки» (рис. 285).

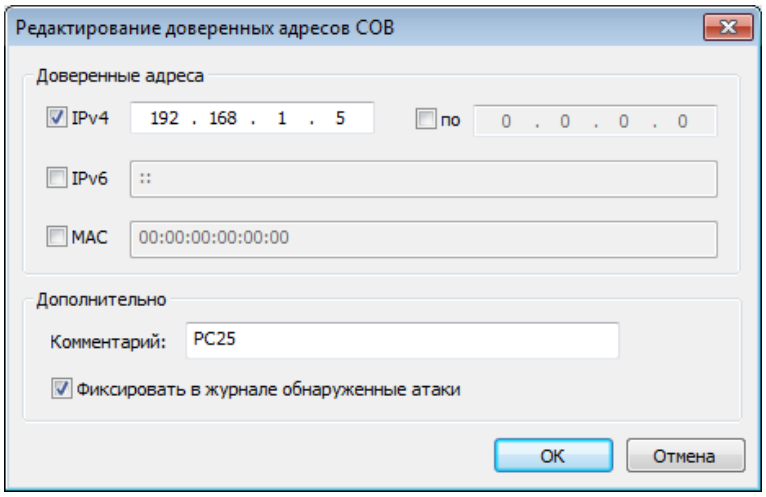


Рис. 285. Редактирование доверенных адресов СОВ

Примечание. В некоторых случаях может понадобиться занесение в белые адреса и IP и MAC доверенного узла, так как в одних случаях может срабатывать блокировка по IP-адресу, а в других случаях — по MAC.

Для того, чтобы удалить доверенный адрес, нужно, выбрав один или несколько доверенных адресов, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие «Удалить». Далее необходимо подтвердить операцию.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку «Поиск» на панели «Действия».

Действия по изменению списка доверенных адресов фиксируются в журнале управления политиками.

16.5 Параметры СОВ

16.5.1 Контроль приложений

Обнаружение аномалий в поведении приложений и ОС, может являться сигналом об осуществлении попытки вторжения. Для выявления таких попыток СОВ перехватывает вызовы функций от приложений к ОС и отслеживает следующие события:

- Обращения ПО к системному реестру и критическим объектам ОС. Критическими являются объекты, удаление, блокирование или модификация которых оказывает влияние на функционирование или безопасность ОС Windows — системные библиотеки, драйверы, файл hosts и т. п.
- Попытки модификации или удаления объектов ПО СЗИ.
- Обращения ПО к объектам ФС, в том числе прямой доступ к диску.
- Попытки внедрения компонент — подмена и установка сторонних библиотек, установка системных перехватчиков, через которые посторонний код может быть внедрен в другой процесс, оконные перехватчики.
- Внедрение в память процесса.
- DDE- и OLE- взаимодействие.
- Запросы на завершение и запуск процессов.
- Низкоуровневый сетевой доступ.
- Вызов DNS API.
- Попытки снятия скриншота экрана, НСД к буферу обмена или перехват нажатия клавиш приложениями.

Примечание. При помощи правила «Получение контекста десктопа или активного окна (возможность снятия скриншота)» можно заблокировать попытки снятия снимка экрана приложениями, использующими для этого возможности GDI API, например, «Ножницы», Shift+Win+S и т.д.

Попытки получения контекста десктопа с помощью других методов, таких как Windows.Graphics.Capture, не блокируются.

Если требуется исключить возможность снятия скриншота для конкретного приложения, например, «Ножницы», необходимо создать соответствующее правило Контроля приложений в соответствии с примером, приведенным в данном разделе.

Внимание! Если «Получение контекста десктопа или активного окна (возможность снятия скриншота)» заблокировано в правилах по умолчанию, то это может повлиять на работоспособность и быстродействие безопасных приложений, использующих те же возможности GDI API, но в иных, не связанных со снятием снимка экрана целях (например, Microsoft Edge).

В этом случае для доверенных приложений, с которыми наблюдаются такие проблемы, рекомендуется создать правило Контроля приложений, разрешающее получение контекста десктопа или активного окна.

Примечание. Если в СОВ созданы запрещающие правила для контроля приложений и реестра, и при этом была создана новая учетная запись пользователя, то для работы данного пользователя необходимо временно отключить СОВ и выполнить вход под новой учетной записью пользователя. При этом входе в системной папке ОС формируется профиль пользователя, необходимый для корректной работы с СОВ.

Примечание. Исполняемые модули ОС, входящие в состав внутреннего каталога Windows, считаются доверительными и проходят проверку подписи.

Внимание! В системе не контролируются системные процессы и защищенные процессы.

На информационной панели находится список правил контроля приложений и сведения о них (рис. 286).

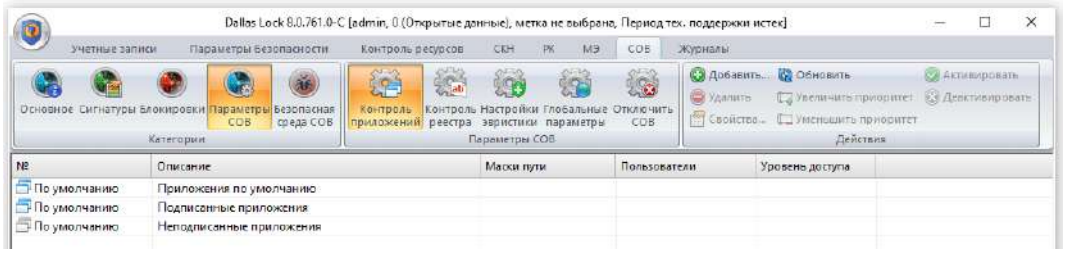


Рис. 286. Информационная панель контроля приложения

При запуске любого приложения СОВ производит его анализ (определяет, подписано приложение или нет) и ищет данное приложение в пользовательских правилах контроля приложений СОВ. При обнаружении приложения, СОВ выполняет проверку на наличие ограничений для системных функций приложения. В правиле для каждой функции возможно установить следующие значения:

- разрешить,
- запретить,
- наследуется.

Пользовательские правила могут наследовать настройки правил по умолчанию для подписанных и неподписанных приложений.

Если приложение не было найдено в пользовательских правилах, то СОВ проверяет доступ в правилах по умолчанию для подписанных и неподписанных приложений. Для системных функций возможно установить аналогичные значения, что и в пользовательских правилах.

Правила по умолчанию для подписанных приложений и неподписанных приложений, могут наследовать настройки у глобальных правил для приложений по умолчанию.

Поэтому приоритеты правил контроля приложений представляют собой следующую иерархию:

Таблица 7. Приоритеты правил контроля приложений СОВ

Правила	Приоритет
Пользовательские правила	Самый высокий
Правила по умолчанию для подписанных и неподписанных приложений	Средний
Глобальное правило для приложений по умолчанию	Самый низкий

Для того, чтобы изменить правило, нужно выбрать его на информационной панели и нажать кнопку «Свойства» на панели «Действия».

Существуют возможность удаления пользовательского правила, добавление нового и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели «Действия».

При изменении или добавлении правила появится меню «Настройка правила контроля приложений», где можно осуществить несколько уровней настроек.

В разделе «Информация» отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 287).

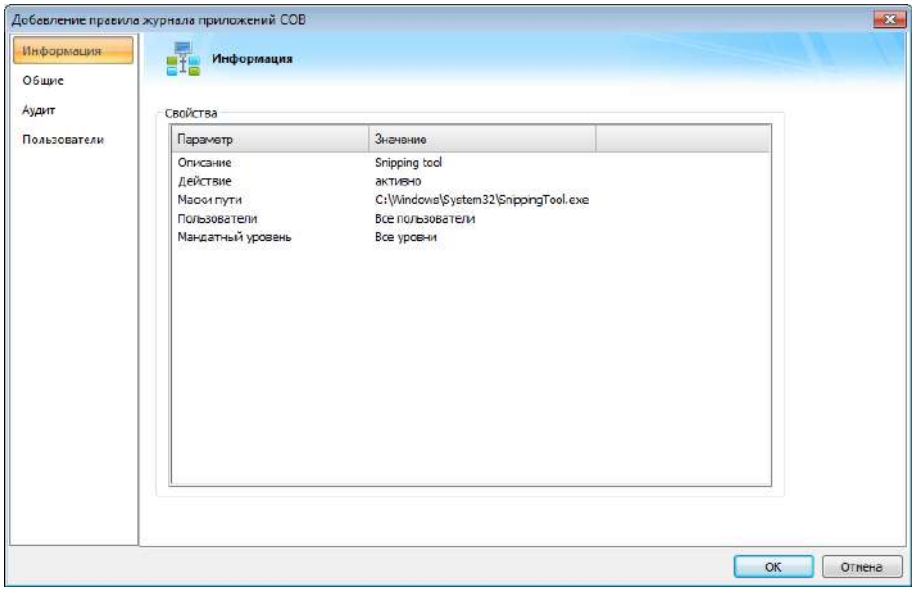


Рис. 287. Информация

В разделе «Общие» представлены основные настройки правила (рис. 288). Есть возможность наследовать настройки у правила по умолчанию для подписанных и неподписанных приложений. Для перечисленных системных функций приложения возможно разрешить или запретить доступ, или наследовать значения у правила выше приоритетом.

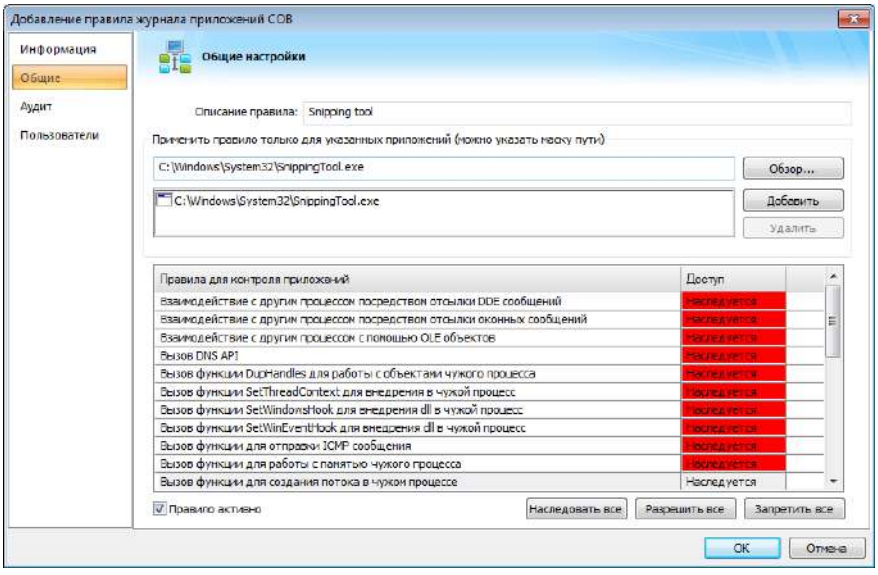


Рис. 288. Общие

В разделе «Аудит» есть возможность установить уровень журналирования событий успеха и отказа (рис. 289). Есть возможность наследовать значение параметров у правила выше приоритетом.

Внимание! Уровень журналирования правил контроля приложений должен быть равен глобальному уровню журналирования СОВ или быть выше (см. «Настройки эвристики»).

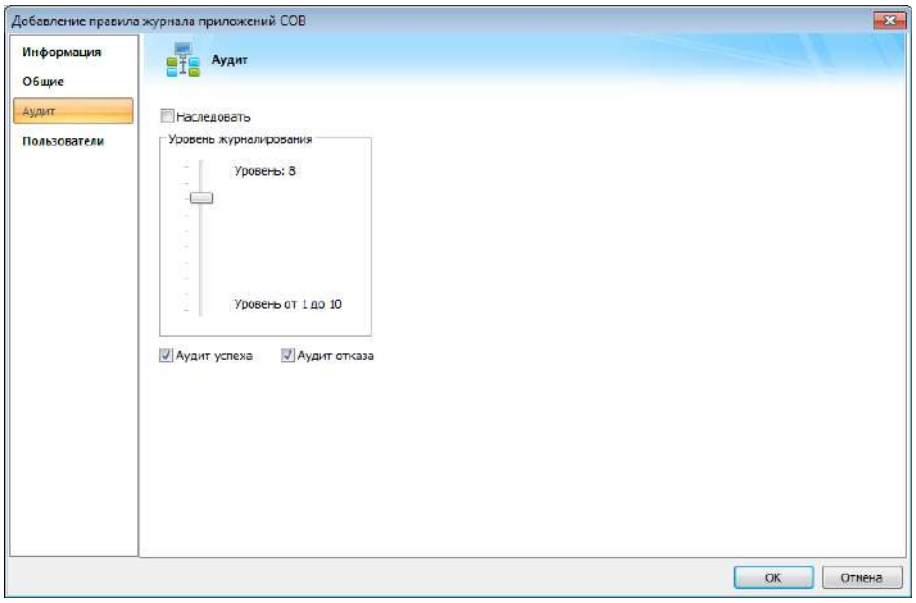


Рис. 289. Аудит

В разделе «Пользователи» отображается список пользователей, к которым будет применяться созданное правило.

Отметив пункт «Автоматический поиск пользователей/групп» при последующем нажатии кнопок «Пользователи» и «Группы» будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки «Удалить» (рис. 290).

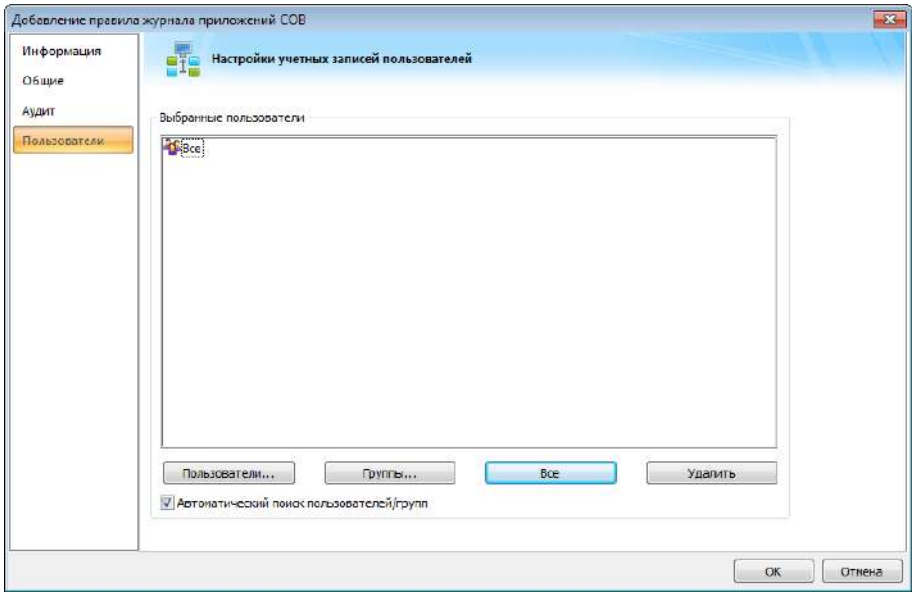


Рис. 290. Пользователи

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (рис. 291).

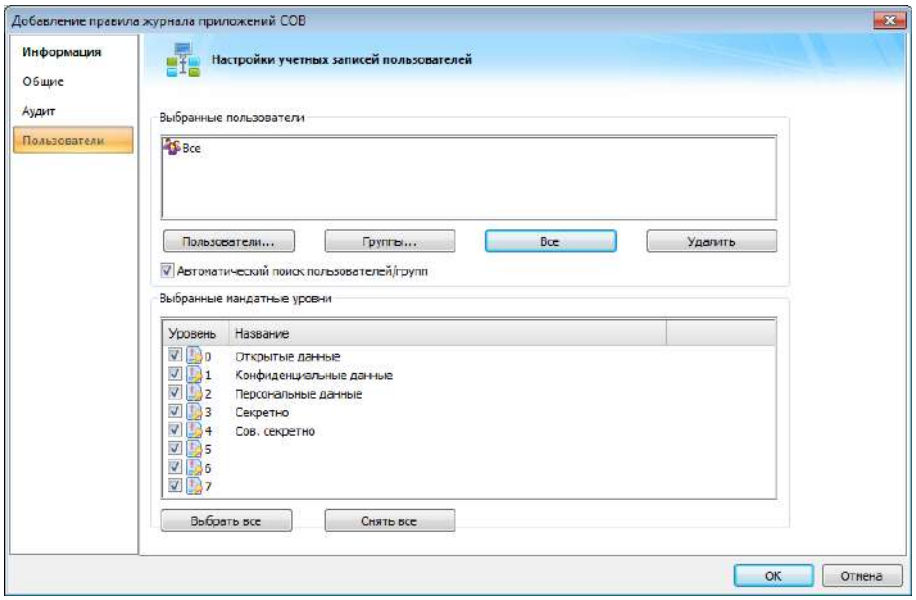


Рис. 291. Пользователи в редакции «С»

Рассмотрим пример создания нового правила.

Необходимо исключить возможность снятия снимка экрана приложением «Ножницы» для пользователя *user*. Для этого нужно перейти в категорию «Настройки СОВ» и нажать кнопку «Контроль приложений». Затем необходимо щелкнуть правой кнопкой мыши на информационной панели и выбрать контекстном меню действие «Добавить».

Далее в разделе «Общие» следует нажать кнопку «Обзор» и выбрать файл, расположенный по пути «C:\Windows\System32\SnippingTool.exe», после чего нажать кнопку «Добавить».

В нижнем окне требуется «Выбрать все» события, кроме «Получение контекста десктопа или активного окна (возможно снятие скриншота)» (рис. 292).

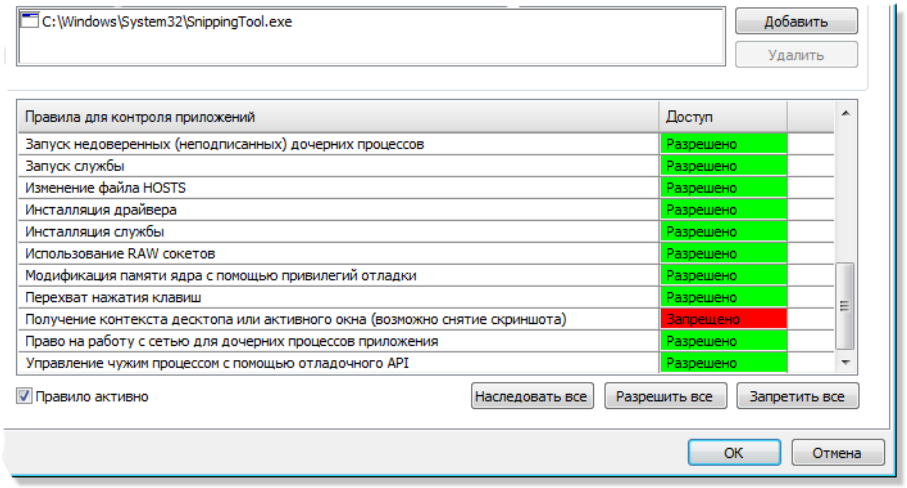


Рис. 292. Создание правила контроля приложений

В разделе пользователи можно выбрать пользователей, для которых будет применимо данное правило. По умолчанию все пользователи и группы получают права доступа согласно создаваемому правилу.

После необходимо активировать правило, это возможно сделать как в свойствах правила, так и на информационной панели действием «Активировать правило».

Действия по изменению правил контроля приложений фиксируется в журнале управления политиками.

16.5.2 Контроль реестра

Подкатегория «Контроль реестра» позволяет ограничивать попытки ПО изменять в системном реестре настройки критических объектов ОС, такие как: автоматический запуск приложений, автоматический запуск системных приложений, правила обработки расширений файлов, ветка автоматически запускаемых DLL и т. д.

На информационной панели находится список групп и контролируемых ключей реестра (рис. 293).

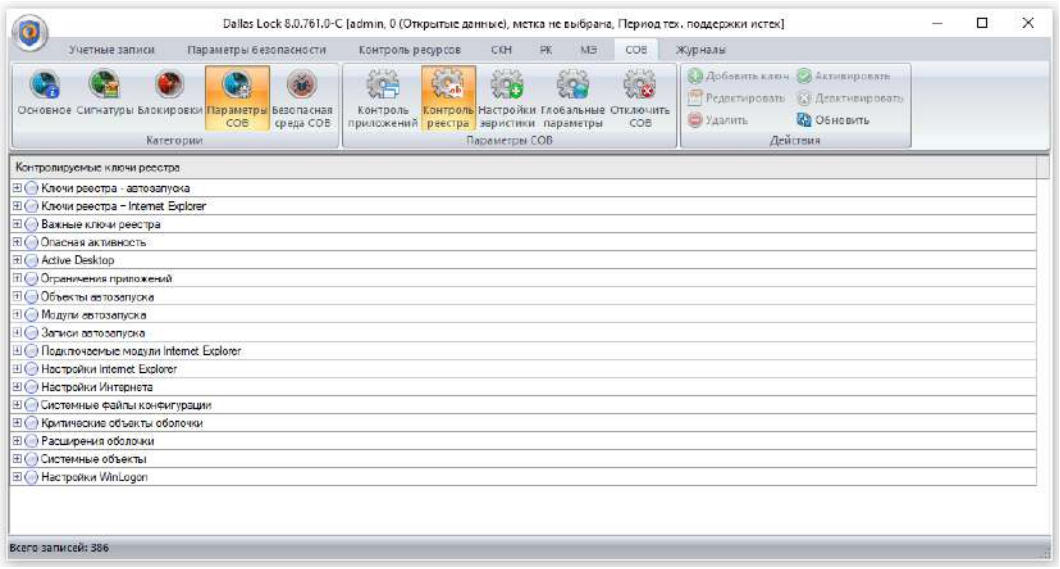


Рис. 293. Информационная панель контроля реестра

В настройках контроля реестра можно изменять ключи в фиксированном списке групп настроек, но нельзя добавлять или удалять произвольные группы. Возможна активация и деактивация как отдельных ключей, так и групп целиком. Редактирование осуществляется аналогично редактированию других настроек СОВ.

Действия по изменению настроек контроля реестра фиксируются в журнале управления политиками.

16.5.3 Настройки эвристики

Данная подкатегория позволяет произвести настройку эвристического анализа, с целью обнаружения аномалий сетевого трафика.

Информационная панель содержит следующие рабочие области (рис. 294):

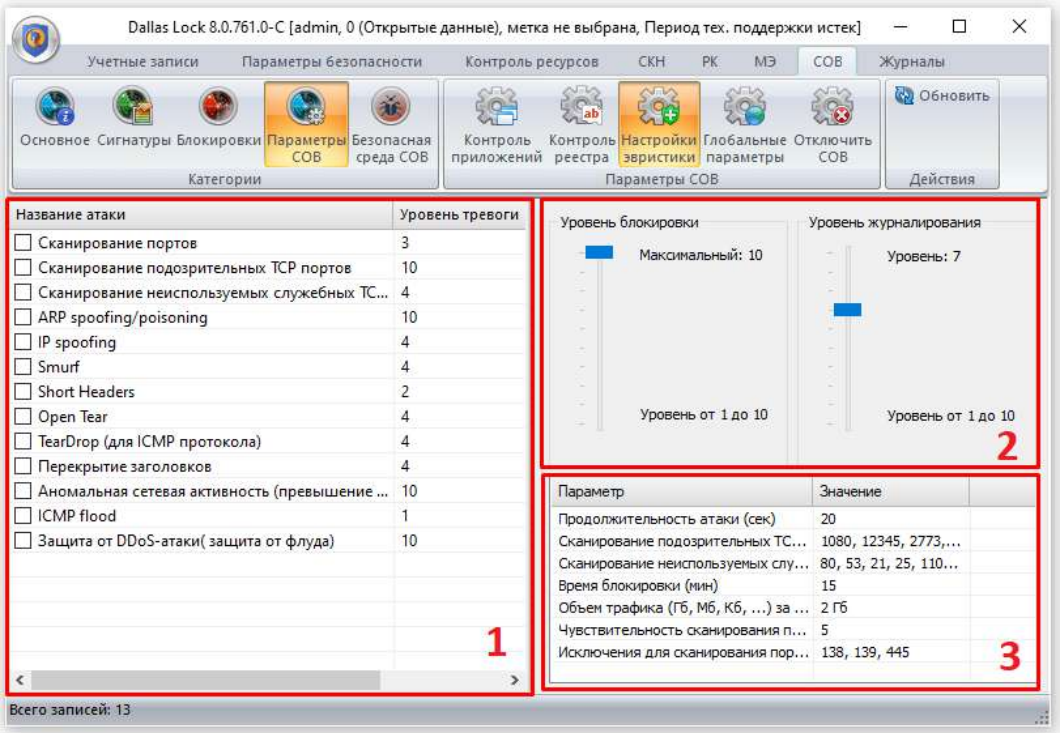


Рис. 294. Настройки эвристики

1. Список атак и их уровень тревоги. Для изменения уровня тревоги определенной атаки нужно щелкнуть два раза левой кнопкой мыши по значению и задать необходимое новое значение. Для того чтобы полностью отключить обнаружение отдельной атаки необходимо снять галочку у данной атаки.

Сканирование портов
Действие, предшествующее сетевой атаке, когда TCP и UDP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
Сканирование подозрительных TCP портов
Действие, предшествующее сетевой атаке, когда TCP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
Сканирование неиспользуемых служебных TCP портов
Действие, предшествующее сетевой атаке, когда TCP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
ARP spoofing/poisoning
Техника сетевой атаки, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.
IP spoofing
Атака, в процессе реализации которой в значении поля IP-пакета «адрес отправителя» адрес атакующего подменяется на адрес доверенного хоста, после чего данный IP-пакет отправляется жертве.
Smurf
Атака заключается в передаче в сеть широковещательных ICMP запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к существенному снижению пропускной способности канала связи или к полной изоляции атакуемой сети.
Short Headers
Атака, направленная на выход из строя программы обработчика (заголовок датаграммы содержит менее 8 байт).
Open Tear
Атака использует случайно измененный исходный адрес и отправляет случайным образом фрагментированные UDP-пакеты на случайные порты.
TearDrop (для ICMP протокола)
Атака, заключающаяся в отправке на атакуемый узел не всех фрагментов пересылаемого пакета, что приводит к ошибкам при сборке полученной датаграммы.
Перекрытие заголовков
Атака, заключающаяся в отправке на атакуемый узел датаграммы с некорректно установленными параметрами начала и длины фрагментов. Параметры фрагментов пересекаются при сборке полученной датаграммы в памяти компьютера, что приводит к ошибкам.
Аномальная сетевая активность (превышение трафика)
Неожиданно большой объем трафика, свидетельствующий об атаке на защищаемую систему.
ICMP (flood)
Атака на сетевое оборудование, ставящая своей целью отказ в обслуживании. Заключается в отправке большого количества ICMP Echo запросов жертве с разных IP-адресов.
Защита от флуда
Атака типа «Отказ в обслуживании», то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен.

2. Глобальные «Уровень блокировки» и «Уровень журналирования», применимые к сигнатурам трафика и правилам контроля приложений. Данные уровни отвечают за количество баллов, при

наборе которых произойдет реагирование на атаку. Для того, чтобы изменить уровень, необходимо передвинуть ползунок вверх или вниз. При срабатывании уровня журналирования — событие занесется в соответствующий журнал, при срабатывании уровня блокировки — произойдет блокировка атакующего (там, где это применимо).

3. Дополнительные настройки эвристики. Данные настройки позволяют настроить общие глобальные настройки эвристики, общие для всех атак.
   - Продолжительность атаки (сек) — время в течение которого учитываются атаки с одного источника для набора баллов тревоги и журналирования.
   - Сканирование подозрительных TCP портов — перечисляется список TCP портов, сканирование которых является атакой с высокой степенью вероятности.
   - Сканирование неиспользуемых служебных TCP портов — перечисляется список TCP портов, сканирование которых (в случае, если данные порты «закрыты») является атакой со значительной степенью вероятности.
   - Время блокировки (мин) — время блокировки обнаруженного источника атаки.
   - Объем трафика (Гб, Мб, Кб) за 10 мин., для определения аномальной сетевой активности — указывается объем трафика для определения аномальной сетевой активности.
   - Чувствительность сканирования портов — в данном параметре указывается количество сканируемых портов, для реагирования на атаки «Сканирования портов и «Сканирования неиспользуемых служебных TCP портов».
   - Исключения для сканирования портов — перечисляется список TCP портов, сканирование которых не является атакой.

Процесс настройки параметров эвристики для разных типов атак.

1. **«Сканирование портов»** и **«Сканирование неиспользуемых служебных TCP портов»**.

   Для атак на TCP-порты существует формула подсчета баллов:

   $$W = \frac{a*b}{c},$$

   где a — «Уровень тревоги», b — количество просканированных портов, c — «Чувствительность сканирования портов».

   Пример:

   Предположим, что «Уровень блокировки» равен 10, а «Уровень журналирования» 7.

   Атакующий произвел сканирование 15 портов в течение 20 секунд. Уровень тревоги для атаки «Сканирование портов» равняется 3, а «Чувствительность сканирования портов» 5. Исходя из этих данных, набрано 9 баллов:

   $$W = \frac{3 * 15}{5}$$

   Данная атака не заблокируется, но при этом будет зафиксирована в журнале трафика. Иначе говоря, если при условиях, представленных выше:
   - набрано 16 баллов — атака блокируется и журналируется;
   - набрано 7 баллов — атака не блокируется, но журналируется;
   - набрано 5 баллов — атака не блокируется и не журналируется.

   Примечание. Чтобы избежать ложных срабатываний СОВ, для атак на UDP-порты, значение параметра «Чувствительность сканирования портов» увеличивается в 3 раза.

2. **Остальные атаки.**

   Для всех остальных атак также существует формула подсчета баллов:

   $$K = a * b,$$

   где a — «Уровень тревоги» атаки, b — количество атак или просканированных портов.

   При срабатывании блокировки атаки, в области уведомлений Windows на панели задач появится сообщение с информацией о блокировке (рис. 295).

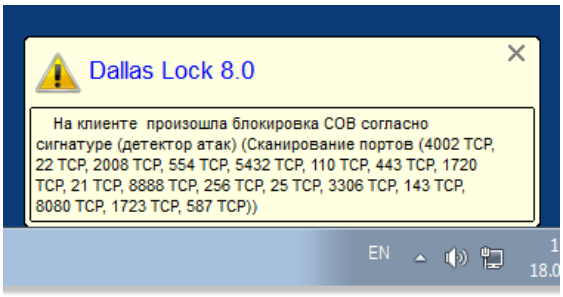


Рис. 295. Уведомление о блокировке источника атаки

Внимание! При централизованной установке/обновлении и проверке сетевой доступности реплицированных СБ при определенных условиях могут происходить события, схожие с сетевыми атаками. Рекомендуется добавить СБ в доверенные адреса для всего ДБ по IP и MAC адресам перед выполнениями данных действий (см. «Доменные настройки СОВ»). При значениях настроек СОВ не по умолчанию при возникновении сложностей с удаленными функциями, необходимо проверить, не произошло ли блокирование ЗАРМ функциями СОВ.

Действия по изменению настроек эвристики фиксируются в журнале управления политиками.

16.5.4 Глобальные параметры

В подкатегории «Глобальные параметры» предусмотрена настройка обновления базы решающих правил (далее — БРП), в частности сигнатур, и других параметров (рис. 296):

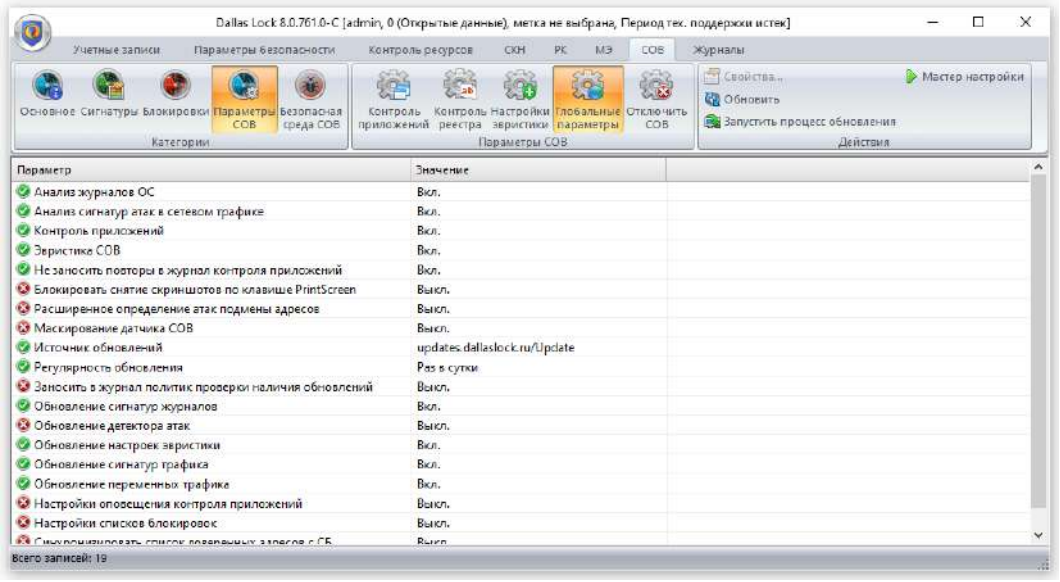


Рис. 296. Список глобальных параметров

Анализ журналов ОС
Данный параметр позволяет включать/отключать сигнатурный эвристический анализ, использующий журналы ОС и приложений.
Анализ сигнатур атак в сетевом трафике
Данный параметр позволяет включать/отключать сигнатурный эвристический анализ, использующий «Журнал трафика» (независимо от блокировки атак на протоколы).
Контроль приложений
Данный параметр позволяет включать/отключать функционирование контроля приложений.
Эвристика СОВ
Данный параметр позволяет включать/отключать блокировку атак на протоколы и сканирование портов (независимо от анализа сигнатур сетевого трафика).

Не заносить повторы в журнал контроля приложений

Включение данного параметра позволяет фильтровать повторяющиеся однотипные события в журнале контроля приложений.

Блокировать снятие скриншотов по клавиатуре PrintScreen

Включение данного параметра позволяет блокировать процесс копирования изображения текущего состояния экрана в буфер обмена при нажатии клавиши Print Screen.

Расширенное определение атак подмены адресов

Включение данного параметра позволяет минимизировать ложные срабатывания обнаружения некоторых атак при получении сетевым адаптером пакетов, адресованных не только непосредственно данному адаптеру (это актуально, например, при использовании виртуальных машин VMware в сетевом режиме Bridged).

Маскирование датчика СОВ

Данный параметр позволяет скрыть наличие датчика СОВ для пользователей, не имеющих прав на просмотр и изменение настроек СОВ. Для таких пользователей не будут появляться уведомления СОВ, а также в меню значка блокировки скроется пункт «СОВ».

Источник обновлений

Данный параметр позволяет задать источник обновления БРП.

Примечание. По умолчанию параметры подключения к интернету определяются автоматически. Если используется прокси-сервер, необходимо настроить параметры прокси-сервера в свойствах обозревателя или браузера в зависимости от версии Windows.

Регулярность обновления

Данный параметр отвечает за регулярность обновления БРП.

Примечание. При выполнении обновления Измененные пользователем значения параметров настроек сохраняются, при использовании мастера настройки защищенных механизмов СОВ данные изменения могут быть отменены обновлением СОВ.

Существует 3 режима обновлений: вручную, раз в час и раз в сутки. При выборе обновления вручную обновление не произойдет до тех пор, пока не будет нажата кнопка «Запустить процесс обновления» на панели «Действия» или в контекстном меню значка блокировки (рис. 297).

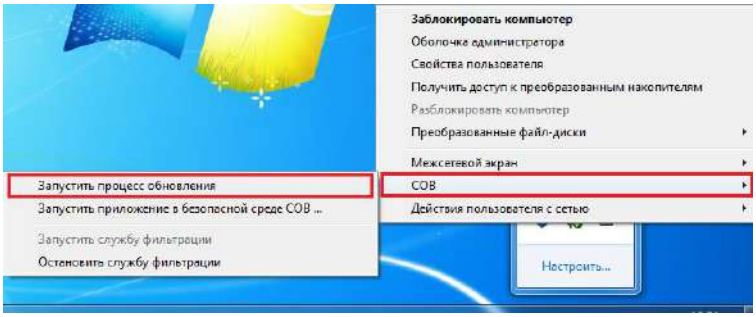


Рис. 297. Запуск процесса обновления БРП

Примечание. После применения обновления, в журнал управления политик производится соответствующая запись.

Заносить в журнал политик проверки наличия обновлений

Включение данного параметра позволяет вести учет проверок на наличие обновлений в журнале управления политиками.

Обновление сигнатур журналов
Включение/отключение обновления сигнатур журналов при ручном или автоматическом обновлении.
Обновление детектора атак
Включение/отключение обновления детектора атак при ручном или автоматическом обновлении.
Обновление настроек эвристики
Включение/отключение обновления настроек эвристики при ручном или автоматическом обновлении.
Обновление сигнатур трафика
Включение/отключение обновления сигнатур трафика при ручном или автоматическом обновлении.
Обновление переменных трафика
Включение/отключение обновления переменных трафика при ручном или автоматическом обновлении.
Настройки оповещения контроля приложений
Данный параметр позволяет произвести настройку оповещений для контроля приложений. Для каждой системной функции возможно указать следующее: • максимальное количество событий в день для информационного оповещения, • максимальное количество событий в день для оповещения об опасной активности, • максимальное количество событий в неделю для информационного оповещения, • максимальное количество событий в неделю для оповещения об опасной активности. При достижении порогового значения выводится соответствующее всплывающее сообщение на панели задач.
Настройки списков блокировок
Данный параметр позволяет включать/отключать использование файлов блокировки, управлять составом файлов блокировки и частотой их опроса. По умолчанию параметр имеет значение «Выкл.».  **Примечание.** В диалоговом окне свойств параметра «Настройка списка блокировок» можно добавлять следующие типы адресов файлов: • для файлов на сервере в сети Интернет http(s)://<Site>/<fileName>.txt; • для файлов на жестком диске <Drive>:\<Path>\<fileName>.txt; для файлов на сетевом диске \\<Server>\<Path>\<fileName>.txt, причем эти файлы должны быть доступны без ввода логина и пароля, то есть должен быть установлен общий доступ к этим файлам на чтение.  **Внимание!** Не функционирует опрос файла с блокировками, расположенный в сетевом каталоге из-за отсутствия доступа к нему у учетной записи System, под которой работает служба фильтрации DIIpsService на защищенном АРМе.
Синхронизировать список доверенных адресов с СБ
Данный параметр позволяет включать/отключать синхронизацию списка доверенных адресов с СБ. По умолчанию параметр имеет значение «Выкл.».

Для удобства настройки глобальные параметры имеют всплывающие подсказки с кратким описанием функциональных возможностей.

Действия по изменению глобальных параметров фиксируются в журнале управления политиками.

Мастер настройки

Назначением мастера настройки СОВ является снижение трудоемкости для эффективной настройки СОВ, позволяя в упрощенном интерфейсе определить требуемые уровни защищенности системы без проведения индивидуальных и точных настроек.

Для того, чтобы задать уровни защищенности с помощью мастера настроек, необходимо:

1. В блоке «Параметры СОВ» → «Глобальные параметры» нажать кнопку «Мастер настройки» на панели «Действия» или в контекстном меню рабочей области.
2. В появившемся окне «Мастер настройки защитных механизмов СОВ» (рис. 298) выбрать уровень защиты компонетов СОВ.
   - Для **защиты от сетевых атак** доступны следующие уровни защиты:
     - **«Высокий»** уровень защиты активирует набор настроек, включающий максимальное количество детектируемых атак, высокую чувствительность датчиков СОВ, расширенный набор сигнатур, используемых при анализе сетевого трафика. Данный уровень также включает в себя настройки «среднего» и «низкого» уровней защиты.
     - **«Средний»** уровень защиты активирует набор настроек, включающий рекомендуемый перечень детектируемых атак, наиболее часто применяемых или оказывающих критическое влияние на ЗАРМ, набор сигнатур трафика для наиболее распространенных (опасных) сетевых атак. Характеризуется оптимальным соотношением чувствительности датчиков СОВ и возможных ложных срабатываний. Средний уровень включает в себя настройки «низкого» уровня защищенности.
     - **«Низкий»** уровень защиты активирует набор настроек, обеспечивающий обнаружение (предотвращение) вторжений только наиболее опасных (для обеспечения конфиденциальности, целостности и доступности информации) атак, критически влияющих на защищенность системы, и характеризуется малым процентом ложных срабатываний.
     - **«Выкл»** — отключает защиту от сетевых атак СОВ. Переводит параметр «Анализ сигнатур атак в сетевом трафике» в состояние «Выкл.».

     При необходимости возможно включить «Расширенное определение атак подмены адресов», а также задать время блокировки атакующего компьютера.
   - Для **защиты реестра** доступны следующие уровни защиты:
     - **«Высокий»** уровень защиты активирует набор правил, обеспечивающий контроль всех важных ключей реестра, критически влияющих на защищенность системы.
     - **«Средний»** уровень защиты активирует набор правил, обеспечивающих контроль большинства ключей реестра критически влияющих на защищенность системы, за исключением групп правил «Active Desktop», «Ограничения приложений» и «Системные файлы конфигурации».
     - **«Низкий»** уровень защиты активирует набор правил, обеспечивающий контроль наиболее важных ключей реестра, критически влияющих на защищенность системы.
     - **«Выкл»** — отключает контроль реестра. Деактивирует все правила контролируемых ключей реестра (вкладка «Контроль реестра»).
   - Для **контроля приложений** доступны следующие уровни защиты:
     - **«Высокий»** уровень защиты задает ограничения для подписанных приложений, запрещая использовать сетевые небезопасные функции и отладочные функции управления потоками, вызывать DNS API, запускать службы и неподписанные дочерние процессы. Для неподписанных приложений ограничивается вызов DNS API, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Данный уровень также включает в себя настройки «среднего» и «низкого» уровней защиты.
     - **«Средний»** уровень защиты задает ограничения для подписанных приложений, запрещая использовать небезопасные сетевые функции, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Для неподписанных приложений ограничивается вызов DNS API, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Средний уровень включает в себя настройки «низкого» уровня защищенности.
     - **«Низкий»** уровень защиты задает минимальные ограничения для подписанных приложений, запрещая использовать отладочные API и RAW сокеты. Для неподписанных приложений запрещается все, кроме использования функций межпроцессного взаимодействия, запуска подписанных и неподписанных процессов.
     - **«Выкл»** — отключает контроль приложений. Переводит параметр «Контроль приложений» в состояние «Выкл.».

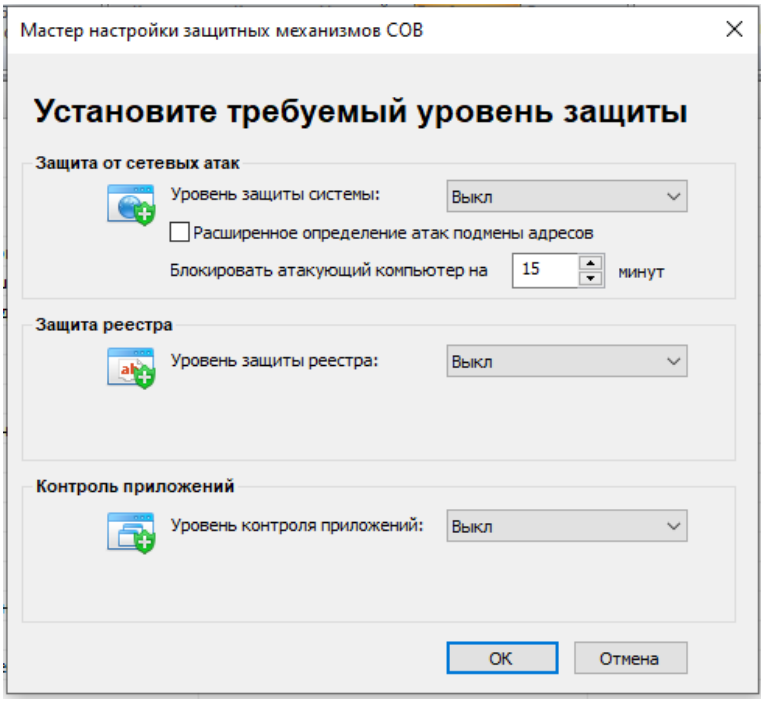


Рис. 298. Мастер настройки защитных механизмов СОВ

16.5.5 Отключить СОВ

Для временного прекращения работы СОВ необходимо нажать кнопку «Отключить СОВ» на панели «Параметры СОВ» и в появившемся окне подтвердить действие (рис. 299).

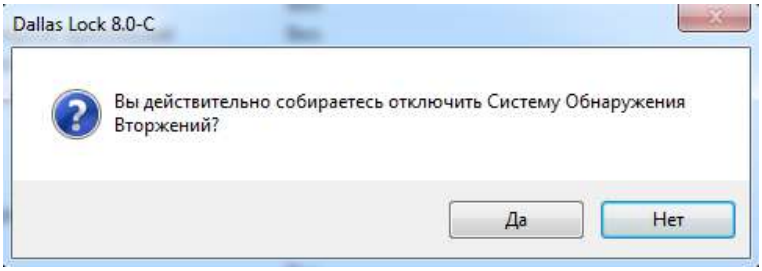


Рис. 299. Отключение СОВ

16.6 Безопасная среда СОВ (песочница)

В СЗИ реализована возможность запускать стороннее ПО в изолированной, безопасной среде — песочнице. В результате запуска стороннего ПО, в песочнице проводится анализ поведения такого приложения в изолированной среде. По результатам анализа реализована возможность автоматического закрытия приложения, в случае обнаружения угроз безопасности и информирование пользователя (администратора) о результатах проверки.

16.6.1 Настройки

Уполномоченному пользователю предоставляется возможность на вкладке СОВ оболочки администрирования СЗИ выбрать категорию «Безопасная среда СОВ», после чего пользователь может произвести настройку безопасной среды в подкатегории «Настройки» (рис. 300).

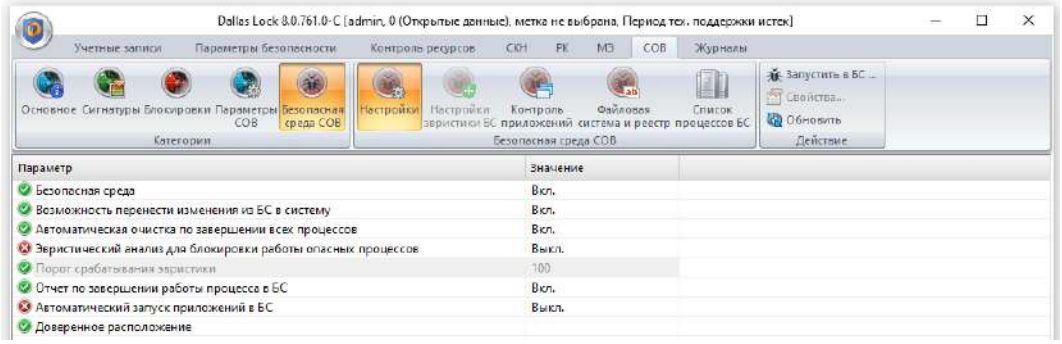


Рис. 300. Панель настройки безопасной среды СОВ

Доступны следующие параметры:

Безопасная среда
Параметр позволяет включать и отключать БС. По умолчанию имеет значение «Вкл.».
Диалог с сохранением изменений после завершения
Параметр позволяет пользователю отключить сохранение результатов работы процесса, запущенного в БС. Если данный параметр включен, перед сохранением пользователю будет выведено диалоговое окно с вопросом на сохранение изменений, выполненных завершенным процессом. По умолчанию имеет значение «Вкл.».
Автоматическая очистка по завершению всех процессов
Данный параметр позволяет пользователю определить будет ли производиться автоматическая очистка временных каталогов от содержимого, созданного процессом или процессами, запущенными в безопасной среде. По умолчанию имеет значение «Вкл.».
Эвристический анализ для блокировки работы опасных процессов
Параметр позволяет разрешить безопасной среде применять эвристический анализ для принудительного завершения работы опасных процессов согласно настройкам эвристического анализа, указанным в категории «Безопасная среда СОВ» → «Настройки эвристики БС» (см. «Настройки эвристики безопасной среды»). Параметру задается значение «Режим ручной настройки», при котором пользователь самостоятельно определяет весовые коэффициенты и значение параметра «Порог срабатывания эвристики», которые в этом режиме доступны для редактирования. При переключении с «Режима ручной настройки» на «Режим с настройками по умолчанию» будет выведено сообщение сбросе настроек на значения по умолчанию (см. «Настройки эвристики безопасной среды»). Параметру может быть задано значение «Режим с настройками по умолчанию» для автоматического определения и завершения потенциально опасных приложений, запущенных в режиме БС, с учетом настроек весов правил эвристического анализа по умолчанию. При этом параметр «Порог срабатывания эвристики» не активен, кнопка «Настройка эвристики БС» активна, но настройки весов недоступны для редактирования. При нажатии на кнопку «Настройки эвристики БС» и при двойном клике на параметре «Порог срабатывания эвристики» выводится сообщение: «Для разрешения редактирования настроек включите «Режим ручной настройки» в «Эвристическом анализе для блокировки работы опасных процессов»». При заданном значении параметра «Выключен» (по умолчанию) параметр «Порог срабатывания эвристики» и кнопка «Настройки эвристики БС» не активны и действия по принудительному завершению процесса со стороны БС предприниматься не будут. Уполномоченный пользователь может запустить приложение в БС и самостоятельно принять решение о его завершении.
Порог срабатывания эвристики
Параметр является накопительным счетчиком весов срабатываний правил эвристики, расположенных в подкатегории «Настройки эвристики БС», по достижению значения (по умолчанию равного «100») которого приложение, запущенное в БС, будет принудительно завершено. Параметр может принимать значения в диапазоне от 0 до 1000 единиц. Если при включенной эвристике значение порога срабатывания указано «0», то любое приложение,

выполнившее любое действие из списка правил настройки эвристического анализа, будет немедленно закрыто. Таким образом возможно блокировать любые потенциально опасные действия подозрительного ПО в БС. При значении от 1 до 1000 происходит накопление счетчиком всех срабатываний указанных настроек эвристического анализа в виде последовательного сложения значений веса первого параметра, если данное действие было выявлено в первый раз, и значения веса последующих срабатываний, если действие было выявлено во второй и последующий разы. Данное действие происходит при срабатывании каждого правила эвристики.

При каждом увеличении счетчика происходит сравнение его значения со значением параметра. В случае, если значение параметра больше значения счетчика, то БС продолжает фиксацию действий приложения с увеличением счетчика согласно значениям весов, указанным в настройках. В случае, если значение порога срабатывания эвристики равно или меньше значения счетчика, то БС завершает работу приложения и предлагает пользователю открыть отчет, а также сохранить данные из БС. При завершении работы приложения в БС по достижению значения параметра в журнале контроля приложений фиксируется последнее действие, добавление веса которого привело к завершению процесса в БС по порогу эвристики. Все остальные действия подлежат записи в отчет.

Отчет по завершению работы процесса в БС

Параметр разрешает СЗИ формировать отчет с результатами контроля ПО, запущенного в БС с уведомлением пользователя. По умолчанию имеет значение «Вкл.».

Автоматический запуск приложений в БС

Параметр позволяет автоматически запускать в безопасной среде исполняемые файлы и приложения, ассоциированные с неисполняемыми файлами, а также файлы, запускаемые из недоверенных источников. Доверенные источники указываются в параметре «Доверенное расположение».

По умолчанию параметр имеет значение «Выкл.».

Доверенное расположение

Параметр содержит пути к доверенным директориям, имеющим сетевое расположение, либо находящимся на съемном носителе. Запуск программ и файлов из этих директорий в автоматическом режиме не производится.

Для добавления и удаления доверенных директорий и носителей информации необходимо открыть окно редактирования свойств параметра, воспользовавшись соответствующей кнопкой в панели «Действия» или в контекстном меню, либо вызвать данное окном двойным кликом мыши на выбранном параметре.

Затем необходимо перейти на соответствующую вкладку и в случае добавления директории указать соответствующий путь, в случае добавления носителя информации — выбрать подключенный носитель из выпадающего списка, затем нажать кнопку «Добавить» (рис. 301).

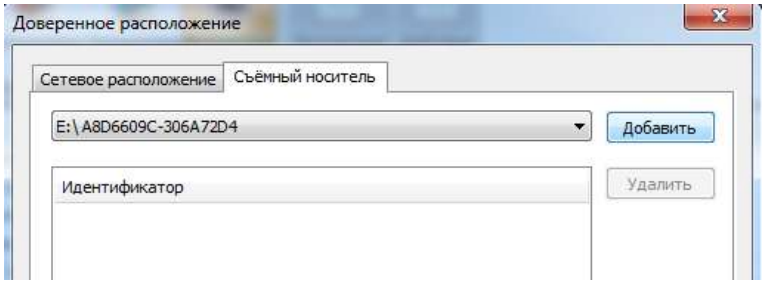


Рис. 301. Добавление доверенного носителя информации

Для удаления директории или съемного носителя из списка доверенных необходимо выбрать их в списке и нажать кнопку «Удалить».

16.6.2 Настройки эвристики безопасной среды

Настройки эвристического анализа в «Безопасной среде» расположены на вкладке СОВ оболочки администрирования СЗИ в категории «Безопасная среда СОВ» в подкатегории «Настройки эвристики БС» и доступны, если для параметра «Эвристический анализ для блокировки работы опасных процессов» установлено значение «Режим ручной настройки». Для удобства пользователя параметр «Порог срабатывания эвристики» вынесен в подкатегорию «Настройки».

Настройки содержат поля «Правило эвристики», «Вес первого срабатывания», «Вес последующих срабатываний» (рис. 302):

- «Правило эвристики» содержит наименование настраиваемого правила;
- «Вес первого срабатывания» определяет то количество единиц, которое прибавляется к значению счетчика в случае первого обнаружения действия из списка настроек, может задаваться в диапазоне от 0 до 1000;
- «Вес последующих срабатываний» определяет то количество единиц, которое прибавляется к значению счетчика в случае второго и последующих обнаружений действия из списка настроек, может задаваться в диапазоне от 0 до 1000.

Рис. 302. Панель «Настройки эвристики БС»

Применение двух весов срабатывания позволяет максимально гибко настроить БС для более безопасного и удобного использования. Настройки эвристики БС имеют предустановленные параметры весов, указанные по умолчанию. Эти правила используются для пользователей, не имеющих прав на настройку параметров СОВ и БС. Для возврата всех настроек к значениям по умолчанию необходимо нажать кнопку «По умолчанию» в блоке «Действие».

Примечание. При включении блокировки межпроцессорного взаимодействия в БС завершаются процессы межпроцессорного взаимодействия в том случае, если превышен порог срабатывания по эвристике для операций, выходящих за рамки БС. При проверке на превышение порога срабатывания по эвристике берется разность между общим счетчиком весов срабатываний и счетчиком весов для процессов внутри БС (не учитывается взаимодействие с процессами, которые находятся внутри БС). В отчет вносится общее число срабатываний.

Доступны следующие настройки эвристики БС:

Модификация памяти ядра с помощью привилегий отладки
Позволяет определять попытки потенциально зловредного ПО проводить модификацию памяти ядра через получения привилегий отладки. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetWinEventHook для внедрения dll в чужой процесс
Позволяет определять функцию системного перехватчика SetWinEventHook для внедрения динамических библиотек в процесс другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetWindowsHook для внедрения dll в чужой процесс
Позволяет определять функцию системного перехватчика SetWindowsHook для внедрения динамических библиотек в процесс другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetThreadContext для внедрения в чужой процесс
Позволяет определять функцию SetThreadContext для внедрения исполняемого кода в процесс другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции для работы с памятью чужого процесса
Позволяет определять функции, с помощью которых потенциально зловредное ПО может произвести внедрение постороннего кода в адресное пространство другого приложения.

Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции DupHandles для работы с объектами чужого процесса
Позволяет определять функцию DupHandles, используемую для работы с объектами чужого процесса. Значения по умолчанию: вес первого срабатывания — 10; вес последующих срабатываний — 1.
Вызов функции для создания потока в чужом процессе
Позволяет определять функции, создающие поток в чужом процессе. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции потока в чужом процессе
Позволяет определять вызов функции потока в чужом процессе. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Управление чужим процессом с помощью отладочного API
Позволяет определять попытки потенциально зловредного ПО управлять чужим процессом с помощью отладочного API. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Инсталляция драйвера
Позволяет определять инсталляцию драйвера потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Запуск драйвера
Позволяет определять запуск драйвера потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Инсталляция службы
Позволяет определять инсталляцию службы потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Запуск службы
Позволяет определять запуск службы потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Взаимодействие с другим процессом посредством отсылки оконных сообщений
Позволяет определять попытки взаимодействия (внедрение динамических библиотек или компонент) потенциально зловредного ПО с другим процессом путем отправки информации в его окно. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Взаимодействие с другим процессом посредством отсылки DDE сообщений
Позволяет отслеживать взаимодействие потенциально опасного ПО с другими приложениями посредством DDE сообщений. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Взаимодействие с другим процессом с помощью OLE объектов
Позволяет отслеживать взаимодействие потенциально опасного ПО с другими

приложениями посредством OLE объектов. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Вызов функции для отправки ICMP сообщения
Позволяет контролировать вызов функции, через которую происходит отправка сообщений по протоколу ICMP. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Вызов DNS API
Позволяет отследить создание ПО DNS-запросов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Запуск доверенных (подписанных) дочерних процессов
Позволяет определять запуск потенциально зловредным ПО доверенных (подписанных) дочерних процессов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Запуск не доверенных (не подписанных) дочерних процессов
Позволяет определять запуск потенциально зловредным ПО не доверенных (не подписанных) дочерних процессов. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Получение контекста десктопа или активного окна (возможность снятия скриншота)
Позволяет определять попытки потенциально зловредным ПО получения контекста рабочего стола пользователя или активного окна в целях получения снимка. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 0.
Перехват нажатия клавиш
Позволяет отследить попытки вредоносного ПО перехватить доступ к нажатию клавиш. Значения по умолчанию: вес первого срабатывания — 50, вес последующих срабатываний — 50.
Право на работу с сетью для дочерних процессов приложения
Позволяет определить попытку получения потенциально зловредным ПО права на работу с сетью для своих дочерних процессов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Использование RAW сокетов
Позволяет определить попытку получения низкоуровневого сетевого доступа потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 0.
Изменение файла HOSTS
Позволяет определить попытку потенциально зловредного ПО произвести изменения в файле HOSTS, содержащий базу данных доменных имен. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Выполнение скриптов PowerShell
Позволяет определить попытку выполнения последовательности действий (сценариев) в оболочке с интерфейсом командной строки PowerShell. Значения по умолчанию: вес первого срабатывания — 10, вес последующих

срабатываний — 1.
Выполнение скриптов через Windows Script Host
Позволяет определить попытку выполнения последовательности действий (сценариев) реализованных на языках JScript и VBScript в среде сервера сценариев Windows. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Запуск cmd (включая пакетные файлы)
Данная настройка позволяет отслеживать запуск консоли, в том числе пакетные файлы. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Перезагрузка системы
Позволяет отслеживать перезагрузку системы. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.

16.6.3 Контроль приложений

Подкатегория «Контроль приложений» предназначена для управления правилами безопасной среды СОВ (рис. 303).

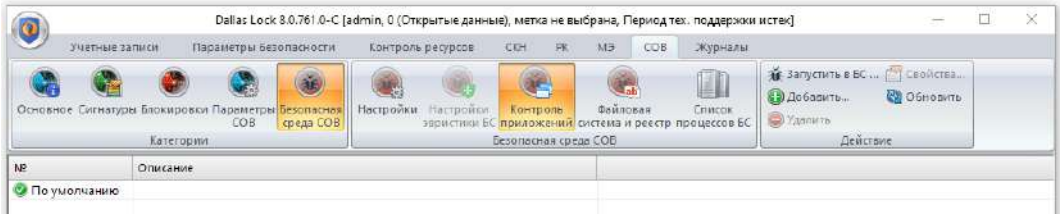


Рис. 303. Панель «Контроль приложений»

По умолчанию «Контроль приложений содержит настройку безопасной среды «По умолчанию», которая содержит в себе набор правил для контроля приложений, запускаемых в «Безопасной среде».

Доступно создание новых и изменение созданных правил. Во вкладке «Общие» для правила безопасности СОВ устанавливается его описание и настраивается список «Правил контроля приложений». Для правила по умолчанию устанавливается вариант доступа «Запрещено» или «Разрешено». При новом правиле устанавливается один из вариантов доступа: «Запрещено», «Разрешено» или «Наследуется» (рис. 304).

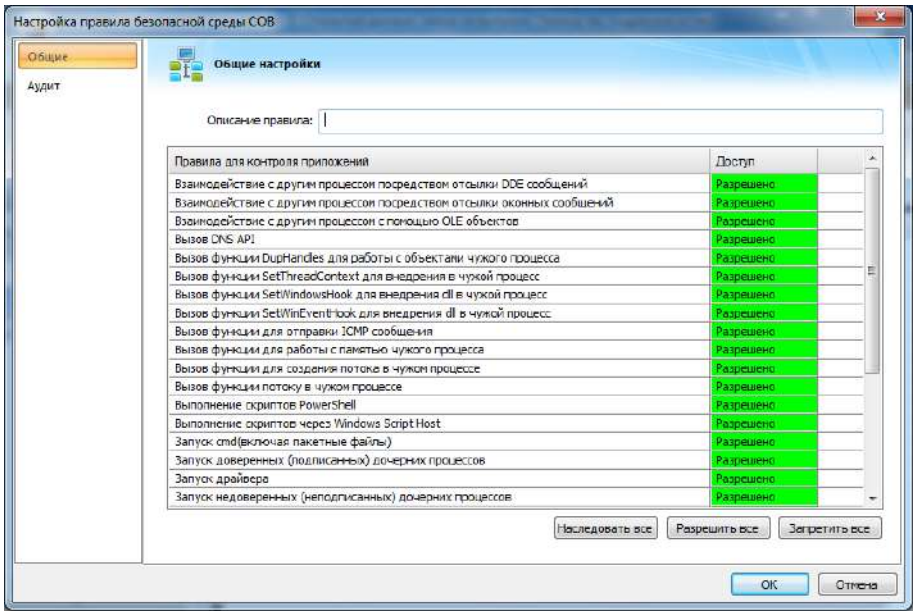


Рис. 304. Общие настройки правила безопасности СОВ

Примечание. Необходимо отметить, что если правило СОВ «Контроль приложений» отмечено как «Запрещено», то общее правило с «Контролем приложений» БС будет так же запрещено и изменению не подлежит. Если в правиле СОВ «Контроль приложений» отмечено как «Разрешено», а в «Контроле приложений» БС запрещено, то будет действовать запрещение этого правила.

На вкладке «Аудит» предлагается настройка уровня журналирования (рис. 305).

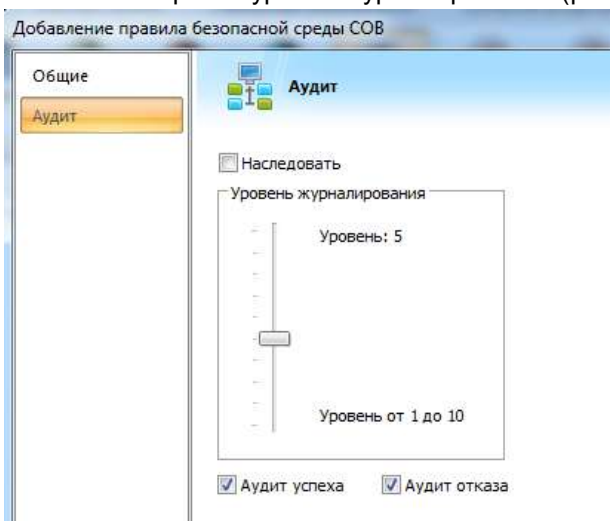


Рис. 305. Настройка аудита правила безопасной среды СОВ

16.6.4 Файловая система и реестр

Подкатегория «Файловая система и реестр» категории «Безопасная среда СОВ» предназначена для указания пользователем тех областей ФС и реестра, которые могут содержать в себе критически важные данные, к которым нельзя предоставлять доступ недоверенным приложениям. При запуске приложения в безопасной среде СЗИ НСД перехватывает вызовы функций от приложения к ОС и отслеживает обращения ПО к системному реестру и критическим объектам операционной системы.

По умолчанию доступ ко всем областям разрешен.

Настройка позволяет указать пути к каталогам и веткам реестра, которые недоступны для чтения и записи, и к каталогам и веткам реестра, к которым разрешен полный доступ (рис. 306).

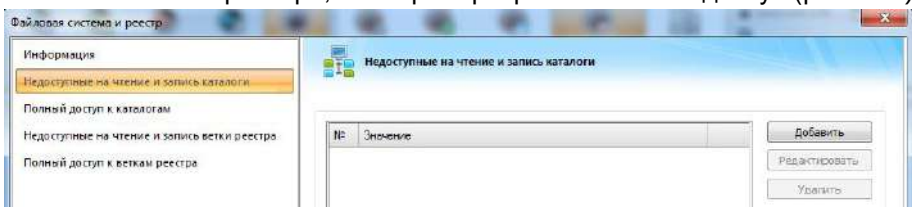


Рис. 306. Настройка доступа приложений к ФС и реестру в режиме БС

16.6.5 Режим безопасной среды

Примечание. Необходимо отметить, что при попытке запуска в БС приложений с расширением .msi такие процессы не запускаются в БС, выводится соответствующее сообщение о невозможности запуска приложения .msi в БС и отмене запуска.

Примечание. Приложения, запускаемые в безопасной среде системы обнаружения вторжений, поддерживают работу как с локальным хранилищем, так и с сетевыми папками и дисками.

Произвести запуск приложения в безопасной среде системы обнаружения вторжений можно следующими способами:

- в консоли администрирования СЗИ перейти на вкладку «СОВ» → «Безопасная среда СОВ» → нажать кнопку «Запустить в БС» на панели «Действия»;
- через пункт «DL8.0: Запустить в безопасной среде …» контекстного меню, отображаемого

при нажатии на нужном файле правой кнопкой мыши;

- через пункт «СОВ» → «Запустить приложение в безопасной среде СОВ» контекстного меню, отображаемого при нажатии на значок на «Панели задач» Windows (рис. 307).

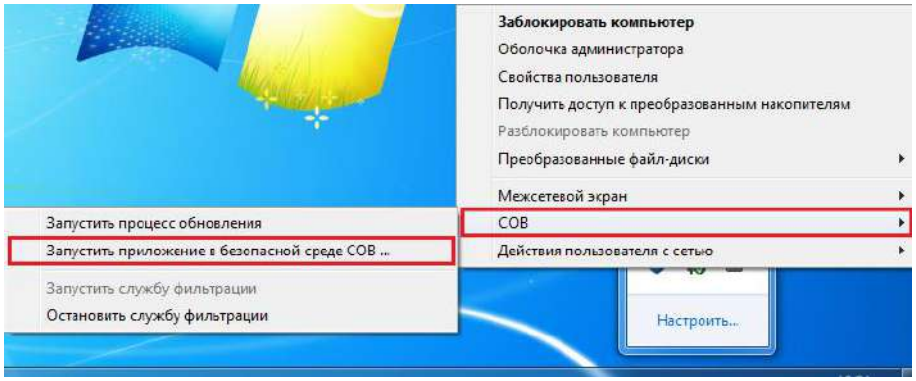


Рис. 307. Запуск приложения в безопасной среде через «Панель задач»

После выполнения одного из этих действий, на экране возникнет диалоговое окно, в котором необходимо в поле «Файл» указать путь к запускаемому приложению, указать параметры, правило и права для запуска приложения (рис. 308).

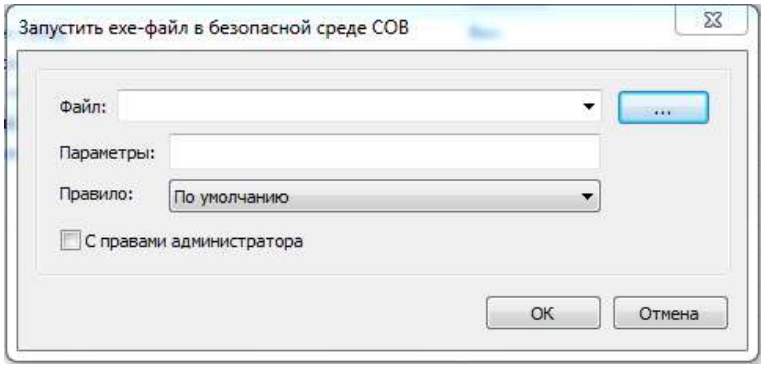


Рис. 308. Запуск приложения в режиме БС

Графическая форма приложения, запущенного в безопасной среде выделяется цветовой рамкой и подписывается (рис. 309).

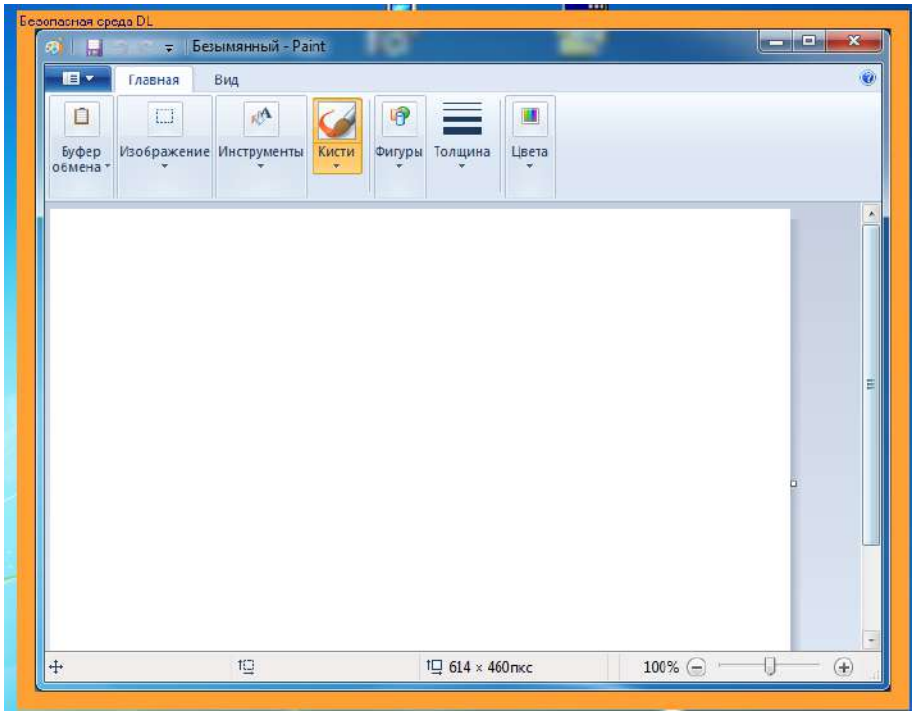


Рис. 309. Безопасная среда

После завершения работы приложения в безопасной среде вручную или в автоматическом режиме, если параметр «Формировать отчет» имеет значение «Вкл.», появляется диалоговое окно с

информацией об отчете.

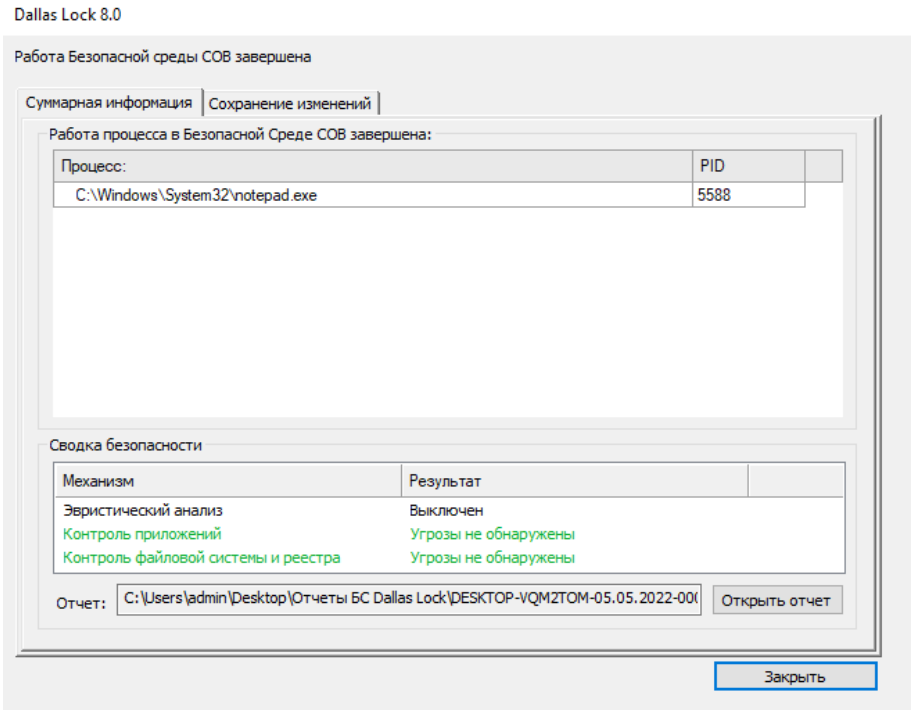


Рис. 310. Завершение работы приложения в безопасной среде

В появившемся окне на вкладке «Суммарная информация» содержится краткая информация о завершении работы процесса в безопасной среде. В строке «Отчет» указан путь, где сохранен отчет. Отчет безопасной среды откроется в браузере при нажатии на кнопку «Открыть отчет» (Рис. 311).

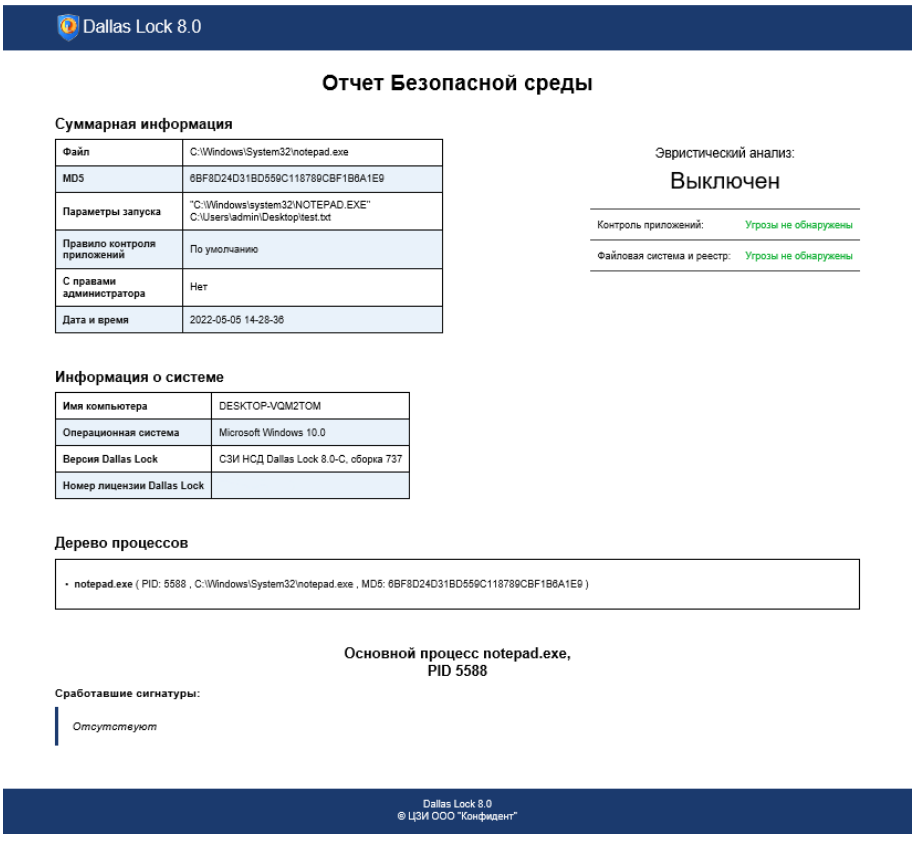


Рис. 311. Отчет безопасной среды

На вкладке «Сохранение изменений» отображены файлы, которые подлежат сохранению из безопасной среды в систему (рис. 312).

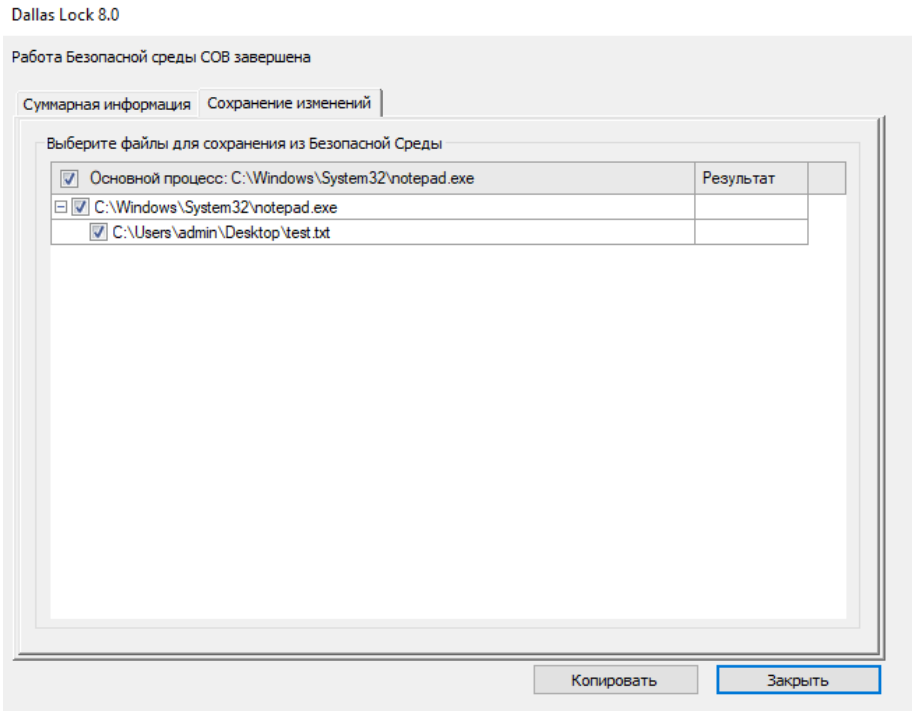


Рис. 312. Сохранение файлов из безопасной среды

Просмотр списка процессов, запущенных в БС доступен в подкатегории «Список процессов БС» (Рис. 313). Для получения списка запущенных процессов необходимо нажать кнопку «Обновить».

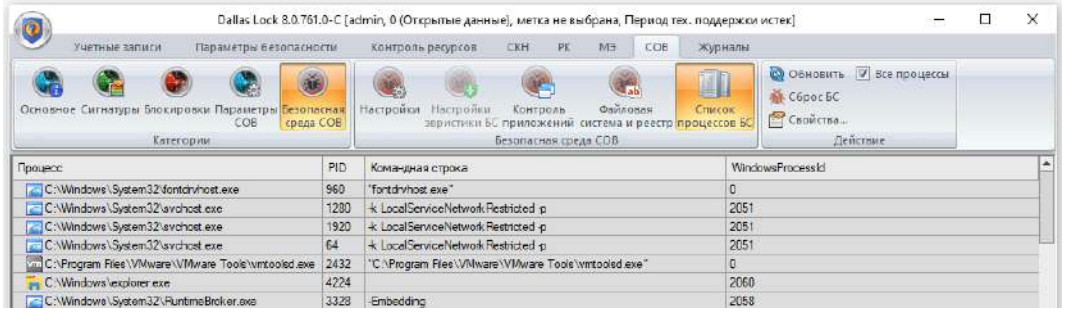


Рис. 313. Список процессов БС

В данной подкатегории есть возможность завершения работы всех процессов в БС и реализации полной очистки данных. Для этого нужно на панели «Действия» нажать кнопку «Сброс БС», обозначенную значком .

При нажатии данной кнопки, пользователю показывается диалоговое окно для подтверждения завершения всех процессов и очистки данных в БС (рис. 314).

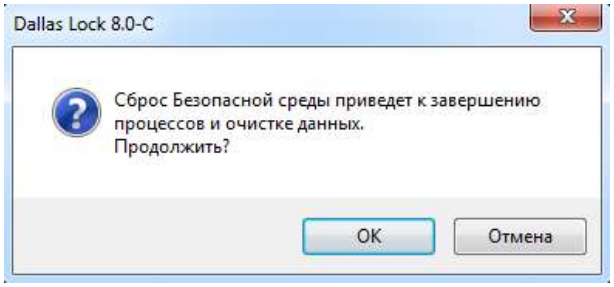


Рис. 314. Сброс СБ

При завершении процесса сброса на экране появляется информационное сообщение об успехе выполнения команды (рис. 315).

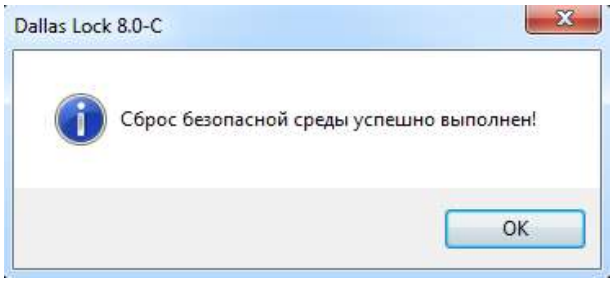


Рис. 315. Успешный сброс безопасной среды

16.7 Журналы СОВ

Основной информацией, фиксируемой в журналах СОВ, является информация о подозрительном сетевом трафике, блокировках сетевых атак, информация о поведении ОС и прикладного ПО.

Для того, чтобы ознакомиться с данной информацией, нужно открыть общую вкладку «Журналы» и выбрать один из трех журналов: «Журнал событий ОС», «Журнал трафика», «Журнал контроля приложений». По умолчанию журналы СОВ включены.

На панели «Действия» расположено три кнопки. При нажатии кнопки «Обновить» отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах СОВ, нужно нажать кнопку «Архивировать». После этого в папке программы появится файл с архивом данных. Для открытия такого файла нужно использовать категорию «Журнал из файла» и в ее окне на панели действий нажать кнопку «Открыть журнал», а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Кнопка «Экспорт» отвечает за сбор и конвертирование информации журналов межсетевого экрана в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку «Экспорт», указать имя файла и выбрать место для его хранения.

Примечание. При открытии «Журнала из файла», в окне выбора файлов возможно выбрать несколько журналов одного типа. При выборе разных типов появится сообщение об ошибке.

В СОВ предусмотрено ведение следующих журналов:

1. Журнал событий ОС — в журнал заносятся сведения о событиях безопасности, генерируемых ОС и прикладным ПО.
2. Журнал трафика — в журнал заносятся события, связанные с проходящим сетевым трафиком через контролируемые сетевые интерфейсы.
3. Журнал контроля приложений — в журнал заносятся сведения об активности приложений, при вызове ими функций, связанных с безопасностью ОС.

Настройки журналов СОВ находятся во вкладке «Параметры безопасности» → «Аудит» и задаются через три параметра (рис. 316).

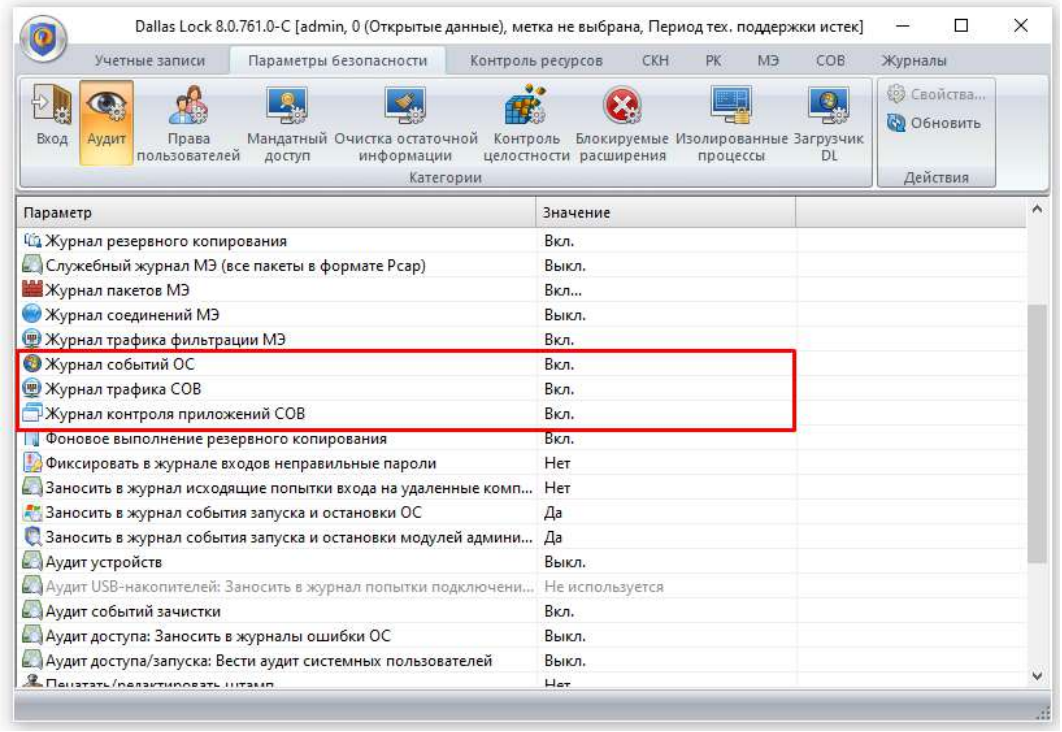


Рис. 316. Основные параметры работы журналов

Чтобы выключить журнал событий ОС необходимо нажать правой кнопкой мыши на параметре «Журнал событий ОС» и в появившемся окне выбрать пункт «Выкл.», после чего нажать кнопку «ОК» (рис. 317). Для остальных журналов СОВ настройка аналогична.

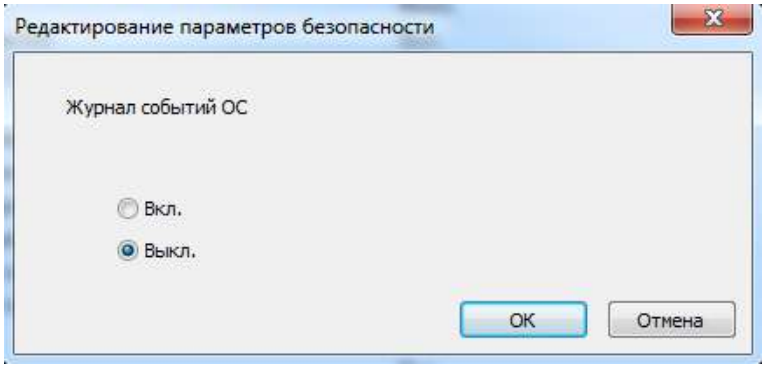


Рис. 317. Отключение ведения журнала событий ОС

В «Журнале управления политиками» СЗИ фиксирует события редактирования параметров и политик СОВ. По умолчанию журнал включен (рис. 318).

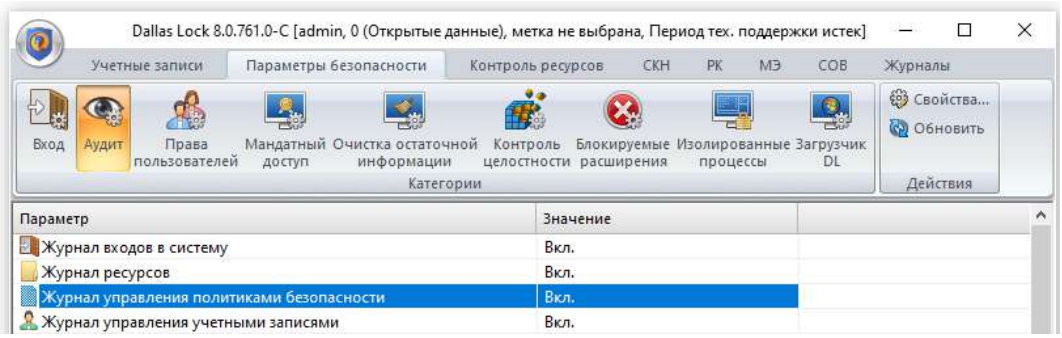


Рис. 318. Журнал управления политиками безопасности

Для просмотра и изменения политик и других параметров «Безопасной среды» пользователь должен быть указан в значении параметров «СОВ: Изменение настроек» и «СОВ: Просмотр настроек» категории «Права пользователей» либо состоять в группе, указанной в данном параметре (рис. 319).

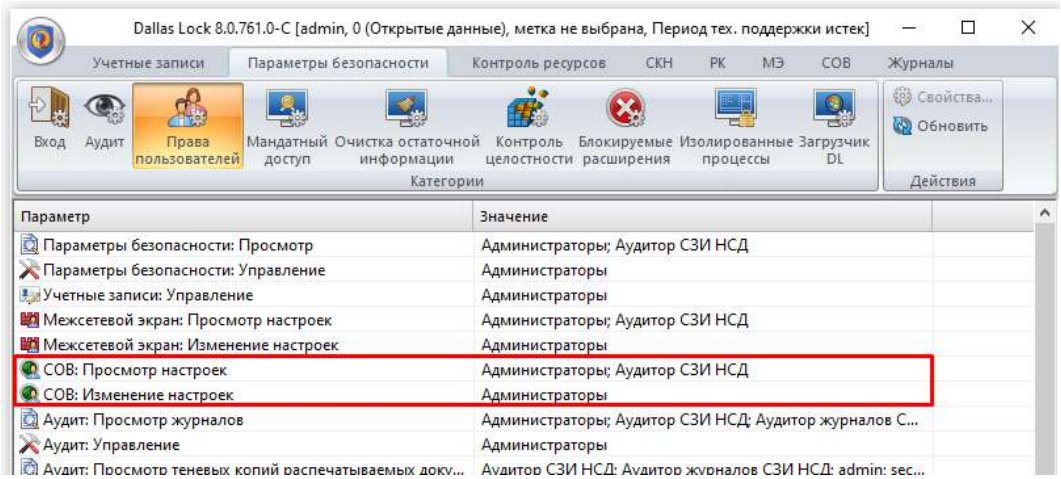


Рис. 319. Настройка аудита настроек СОВ

17 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

17.1 Отчеты

17.1.1 Создание отчета о правах и конфигурации

В системе защиты Dallas Lock 8.0 реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет по правам и конфигурации, который содержит упорядоченные списки пользователей с соответствующими правами на определенные ресурсы.

Для создания отчета по назначенным правам необходимо в оболочке администратора нажать кнопку  основного меню и в появившемся меню выбрать пункт «Отчет о правах и конфигурации» (рис. 320).

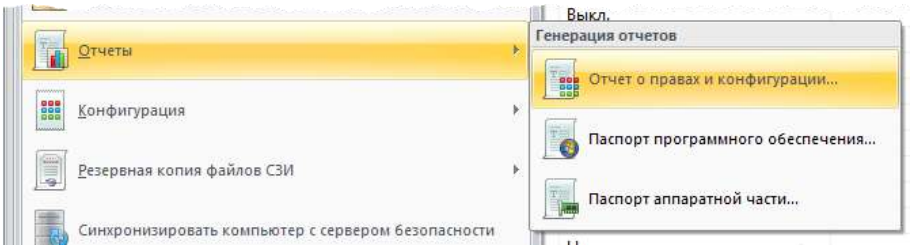


Рис. 320. Меню выбора дополнительных функций системы защиты

Появится окно с выбором параметров для формирования отчета (рис. 321):

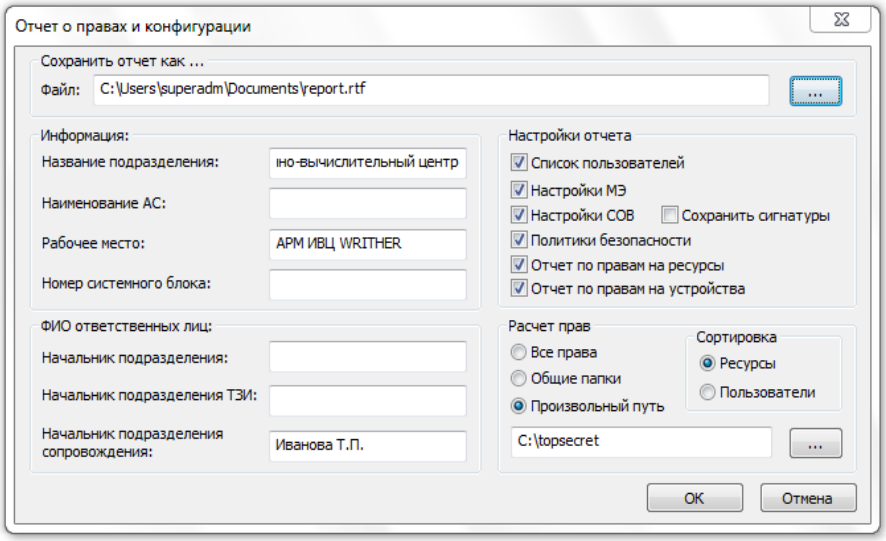


Рис. 321. Создание отчета по назначенным правам и конфигурации

В появившемся окне необходимо ввести следующие данные:

- ввести информацию о реквизитах, которые должны содержаться в документе;
- выбрать настройки отчета: по назначенным правам, список пользователей, политики безопасности;
- если в настройках указан отчет по правам на ресурсы, то необходимо выбрать их параметры: все права, общие папки или конкретный ресурс, указав его размещение (путь) и способ сортировки;
- указать имя отчета и путь для его сохранения.

При нажатии кнопки «ОК» будет создан отчет и открыт в текстовом редакторе. В отчете будет представлена матрица доступа для выбранных ресурсов со следующими значениями:

!R/R — Чтение (запретить/разрешить);
!W/W — Изменение/Запись (запретить/разрешить);
!E/E — Выполнение (запретить/разрешить);
!RA/RA — Чтение разрешений (запретить/разрешить);
!WA/WA — Запись разрешений (запретить/разрешить).

Данная функция может быть удобна для фиксирования настроек матрицы доступа на ФС и для возможности дальнейшей проверки соответствия этих настроек, сравнив с эталонным отчетом.

Событие формирования отчета фиксируется в журнале управления политиками.

17.1.2 Создание паспорта программного обеспечения

В системе защиты Dallas Lock 8.0 реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет со списком программ, установленных на данном компьютере, размером их системных файлов и расчетом контрольных сумм — паспорт ПО автоматизированного рабочего места.

Для создания паспорта ПО необходимо в оболочке администратора нажать кнопку  основного меню и в появившемся меню выбрать пункт «Паспорт программного обеспечения» (рис. 322).

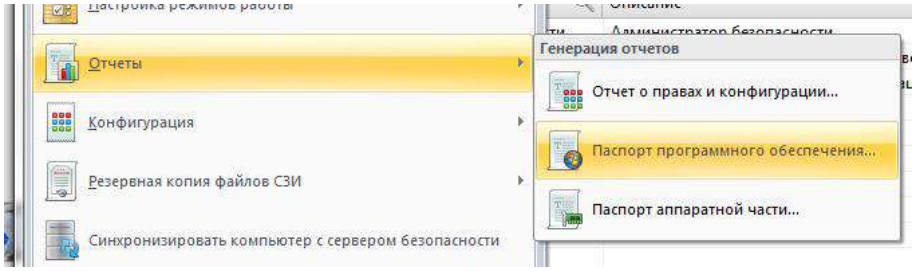


Рис. 322. Меню выбора дополнительных функций системы защиты

Появится окно ввода данных для формирования паспорта ПО, в котором необходимо ввести реквизиты. Нажать «Сохранить как» (рис. 323).

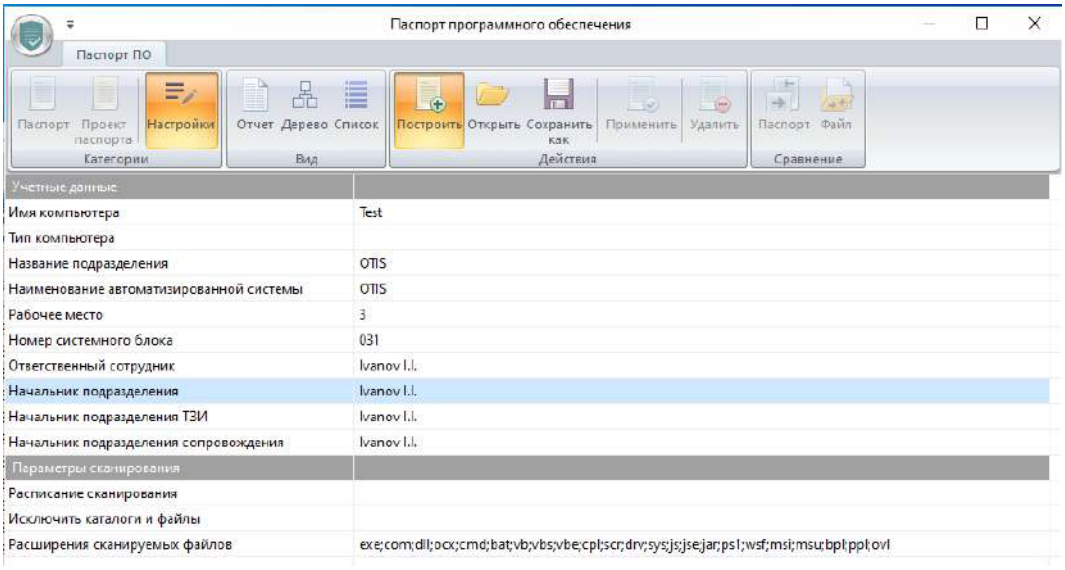


Рис. 323. Создание отчета по назначенным правам и конфигурациям

Откроется окно, в котором необходимо выбрать одну из формы сохранения паспорта ПО: оптимальная для печали, полный (Рис. 324). Нажать «Ок», в появившемся окне выбрать имя и место хранение файла.

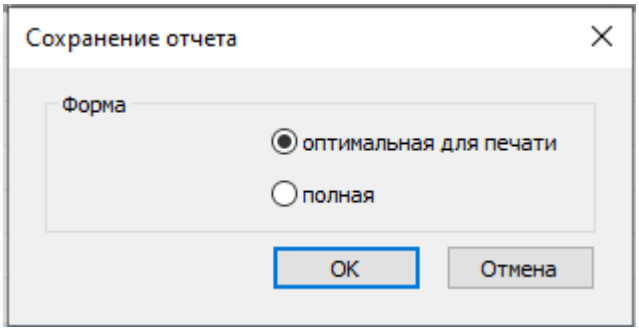


Рис. 324. Сохранение отчета паспорта ПО

Паспорт ПО будет сформирован в текстовом документе в указанном месте и содержать типовой[13] список параметров ПО, установленного на ПК.

Событие формирования паспорта ПО фиксируется в журнале управления политиками.

Расширенные функции по созданию Паспорта ПО

При включенном в состав лицензии СК функции СЗИ Dallas Lock 8.0 по построению Паспортов ПО расширяются. Подробная информация о функциональных возможностях приведена в Инструкции по использованию Сервера конфигураций RU.48957919.501410-02 И4.

17.1.3 Создание паспорта аппаратной части ПК

В системе защиты Dallas Lock 8.0 реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет со списком и характеристиками установленных на данном компьютере устройств.

Для создания паспорта аппаратной части ПК необходимо в оболочке администратора нажать кнопку  основного меню и в появившемся меню выбрать пункт «Паспорт аппаратной части» (рис. 325).

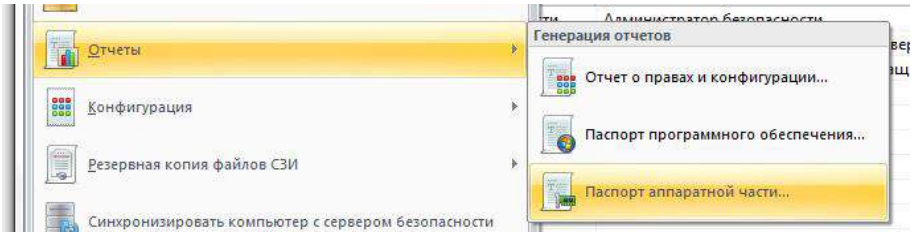


Рис. 325. Меню выбора дополнительных функций системы защиты

Появится окно ввода данных для формирования документа, в котором необходимо ввести реквизиты и указать путь для сохранения сформированного файла (рис. 326).

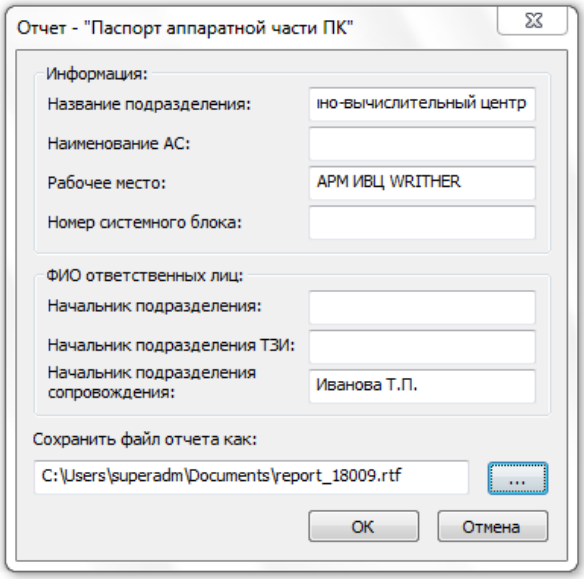


Рис. 326. Создание паспорта аппаратной части ПК

Паспорт аппаратной части будет сформирован в текстовом документе в указанном месте и будет содержать характеристики аппаратной конфигурации ПК.

Событие формирования паспорта аппаратной части ПК фиксируется в журнале управления политиками.

17.2 Автоматическое тестирование функций СЗИ

Данная функция позволяет выполнить автоматическое тестирование основных функциональных

[13] В соответствии с Приложением 3 Приказа ЦБ РФ от 03.03.97 № 02-144.

возможностей системы защиты (создание/удаление пользователя, назначение/снятие параметров доступа к ресурсам и пр.).

Для запуска автоматического тестирования функций СЗИ необходимо в оболочке администратора нажать кнопку  основного меню и в списке функций выбрать пункт «Тестирование функций СЗИ» (рис. 327).

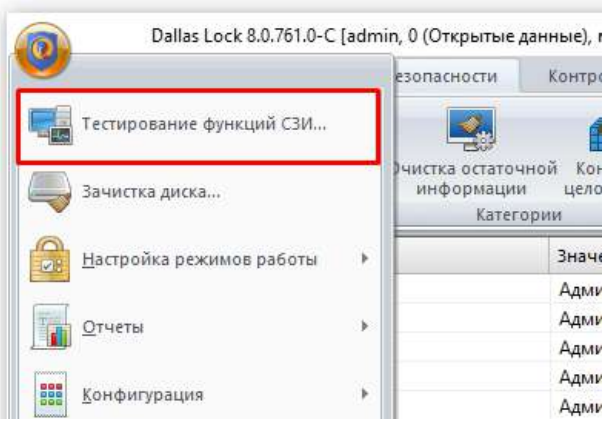


Рис. 327. Меню выбора дополнительных функций системы защиты

В появившемся окне нужно нажать кнопку «Запустить».

По окончании тестирования, при необходимости, можно сохранить отчет, нажав кнопку «Сохранить» (рис. 328).

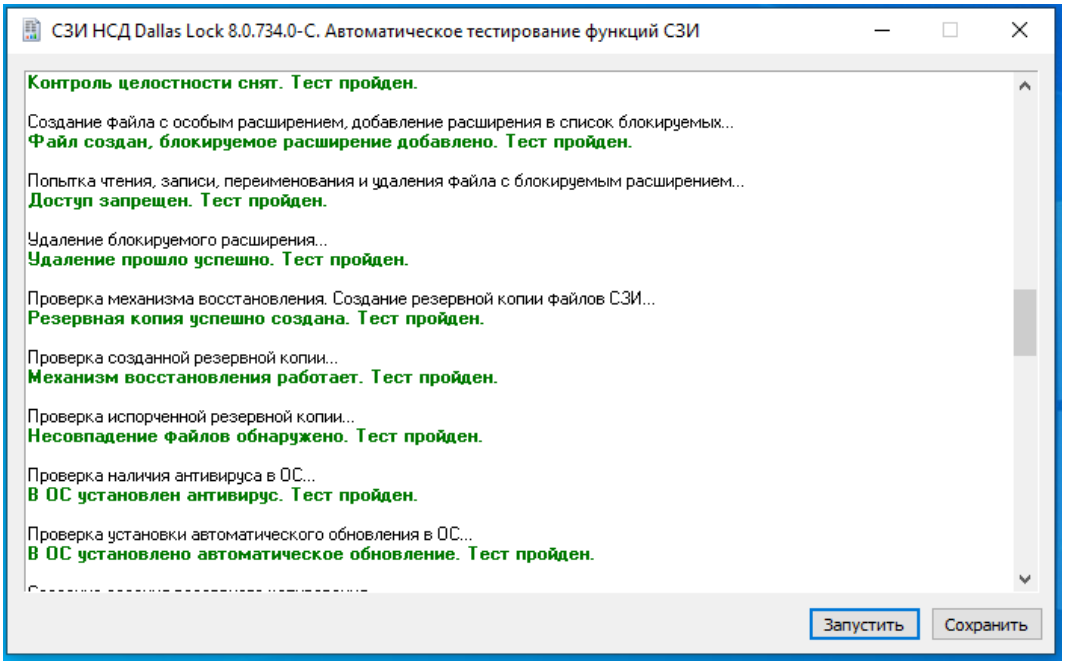


Рис. 328. Автоматическое тестирование функций СЗИ

Для сохранения отчета системой будет предложено выбрать папку для текстового файла. По умолчанию отчет сохранится в формате *.rtf.

Примечание. В Dallas Lock 8.0 редакции «С» функцию «Автоматическое тестирование функций СЗИ» можно запускать, только в случае авторизации под мандатным уровнем 0: «Открытые данные».

17.3 Сохранение резервной копии файлов СЗИ

В СЗИ реализован механизм создания и сохранения резервной копии файлов локально установленной СЗИ Dallas Lock 8.0. Данная функция предназначена для ведения нескольких копий программных компонентов СЗИ, с возможностью последующей сверки с текущими файлами, используемыми в СЗИ, обнаружения несоответствий (проверяется не только совпадение размера,

но и содержимое файлов) и возможностью восстановления.

Чтобы сохранить резервную копию файлов СЗИ, необходимо в оболочке администратора нажать кнопу  основного меню и в появившемся списке дополнительных функций выбрать «Резервная копия файлов СЗИ» → «Сохранить резервную копию файлов СЗИ» (рис. 329).

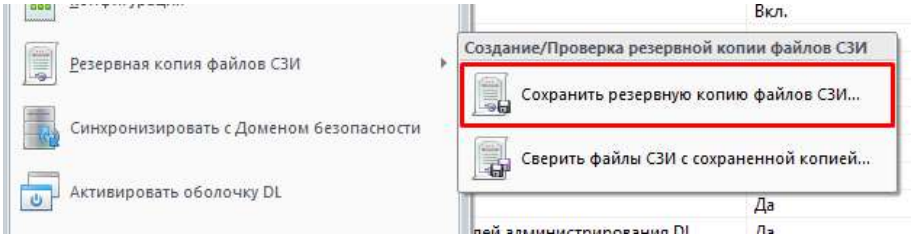


Рис. 329. Меню выбора дополнительных функций системы защиты

После этого выведутся окно проводника, в котором необходимо указать путь и название папки, в которой создастся новая папка, содержащая копии файлов системы защиты. Далее — нажать «Сохранить». В указной папке будет сохранена резервная копия файлов СЗИ, и выведено соответствующее сообщение системы (рис. 330).

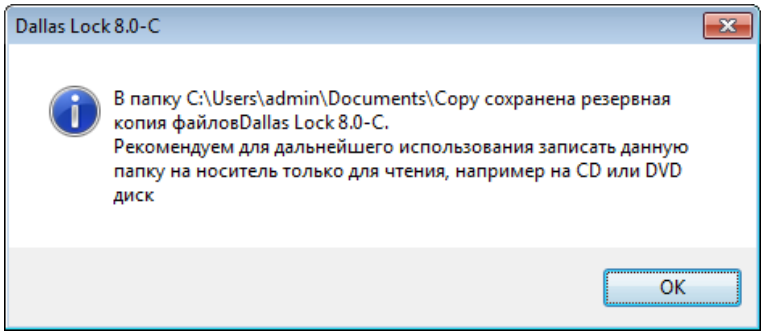


Рис. 330. Сообщение системы о сохранении резервной копии файлов

Для того, чтобы сверить резервную копию файлов СЗИ с файлами, используемыми в системе, необходимо в оболочке администратора выбрать соответствующий пункт (рис. 329).

После этого появится окно, в котором необходимо указать расположение сохраненной копии файлов СЗИ и выбрать файл конфигурации (*.ini). После нажатия кнопки «Открыть» система выполнит проверку и выведет сообщение о результатах сравнения.

Если копии файлов СЗИ и файлов, используемых в системе, совпадают, будет выведено соответствующее сообщение (рис. 331).

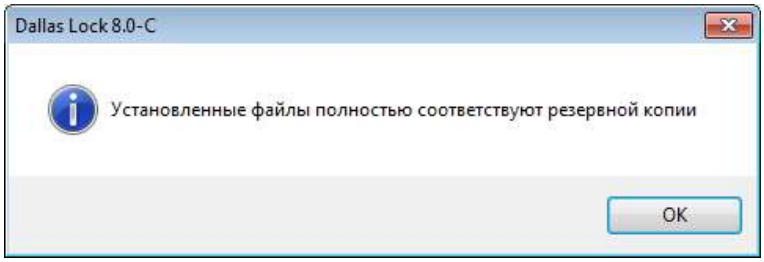


Рис. 331. Сообщение об успешной сверке файлов СЗИ

При обнаружении несоответствий (проверяется не только совпадение размера, но и содержимое файлов) будет выведено предупреждающее сообщение (рис. 332).

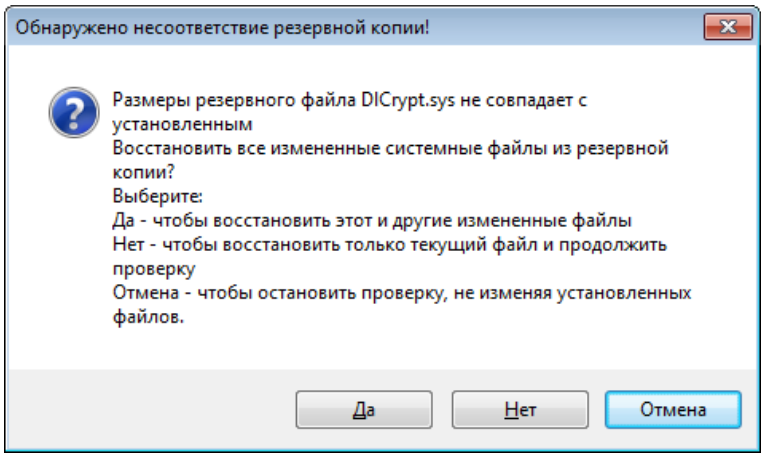


Рис. 332. Несоответствие файлов при сверке

Если выбрать «Да» или «Нет», система восстановит Измененные файлы на основании сохраненной копии файлов и выведет сообщение о том, что файлы полностью соответствуют резервной копии. При нажатии кнопки «Отмена» система продолжит работу с измененными системными файлами, но выведет предупреждение (рис. 333).

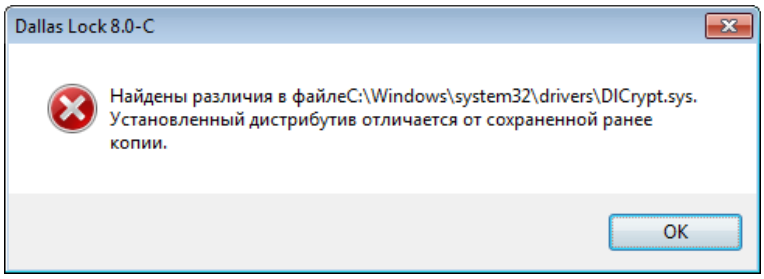


Рис. 333. Сообщение системы о несоответствии файлов при сверке

17.4 Возврат к настройкам по умолчанию

В некоторых случаях бывает необходимо полностью или в большой степени изменить параметры безопасности, установленные в системе защиты. С этой задачей можно справиться, не прибегая к переустановке системы, а вернув системе защиты Dallas Lock 8.0 настройки по умолчанию.

Следует учесть, что помимо возврата всех настроек, в том числе настроек доступа и аудита к изначальным настройкам, учетных записей пользователей, созданных прежде в системе защиты, не окажется. Но так как при создании новых пользователей в СЗИ, их учетная запись создается и в ОС, то при возврате к настройкам по умолчанию, необходимые учетные записи можно снова зарегистрировать, выбрав их из списка локальных.

Для того, чтобы вернуть системе защиты ее исходное состояние, необходимо в списке функций кнопки  основного меню выбрать «Конфигурация» → «Установить настройки по умолчанию» (рис. 334)

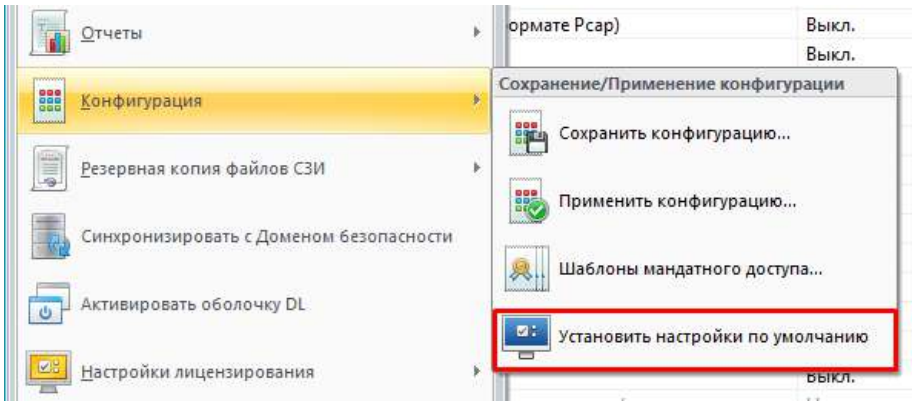


Рис. 334. Выбор установки настроек системы по умолчанию

Появится окно подтверждения установки настроек по умолчанию (рис. 335).

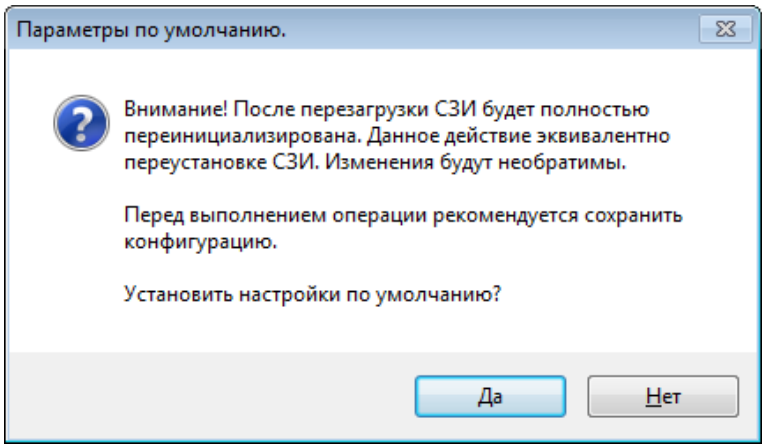


Рис. 335. Подтверждение установки настроек по умолчанию

После подтверждения установки появится сообщение об успешном завершении операции.

Для завершения установки первоначальных настроек системы защиты Dallas Lock 8.0 необходимо самостоятельно перезагрузить компьютер.

Внимание! После применения параметров по умолчанию и до перезагрузки ПК производить преобразование жесткого диска нельзя! Это приведет к невозможности загрузки ОС.

Также следует учесть, что в процессе установок параметров по умолчанию будут удалены ключи преобразования сменных накопителей. Если в СЗИ были преобразованы сменные накопители, то параметры ключей необходимо заранее сохранить.

18 СОХРАНЕНИЕ КОНФИГУРАЦИИ

18.1 Сохранение файла конфигурации Dallas Lock

После того, как была произведена настройка системы защиты Dallas Lock 8.0 согласно требованиям, были зарегистрированы пользователи, и им были предоставлены необходимые права и полномочия, администратор безопасности может сохранить все или определенные настройки системы защиты в специальном файле конфигурации.

Для сохранения настроек системы защиты необходимо в списке функций кнопки основного меню выбрать «Конфигурация» → «Сохранить конфигурацию» (рис. 336).

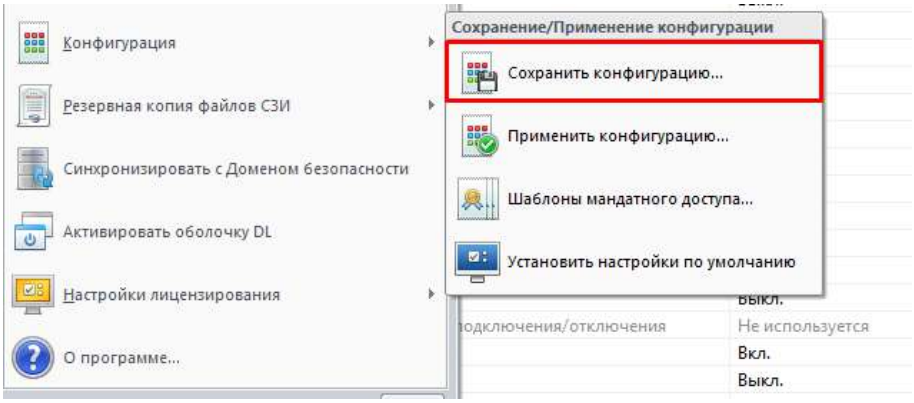


Рис. 336. Выбор сохранения конфигурации

Появится окно с выбором параметров системы защиты для их сохранения (рис. 337).

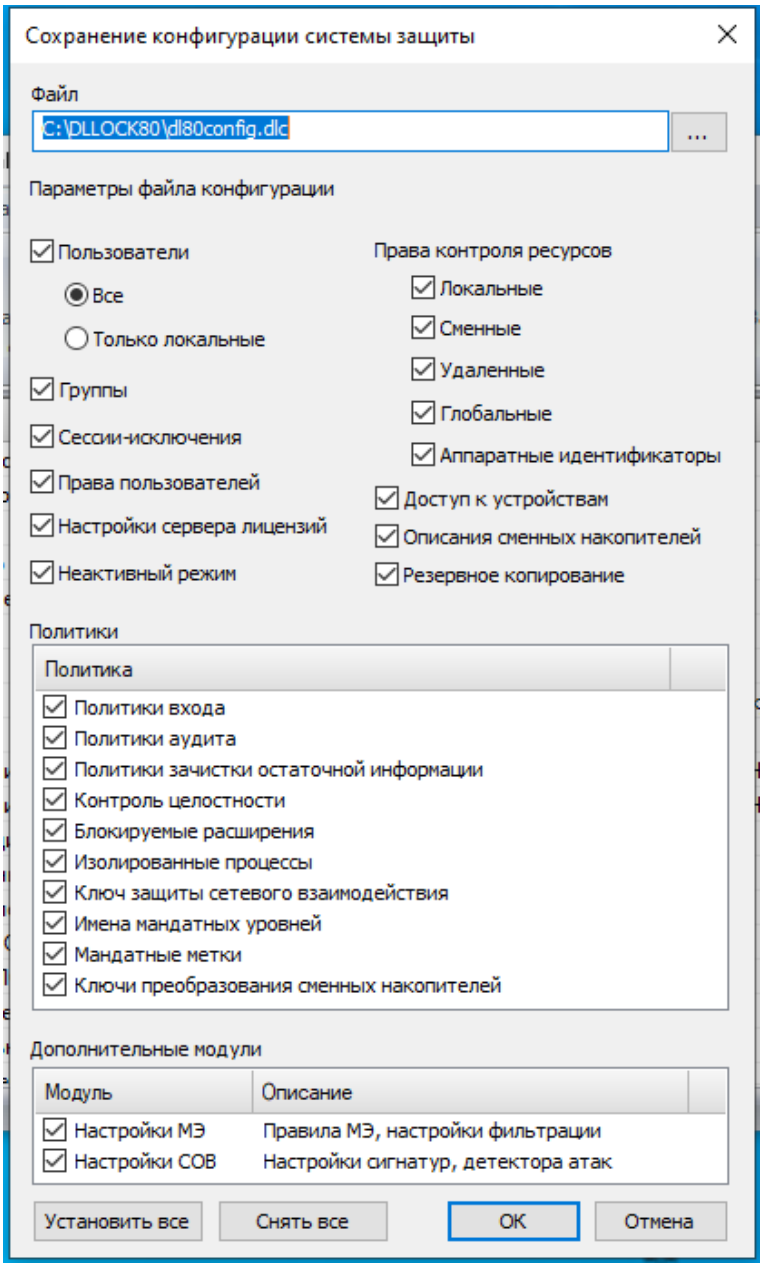


Рис. 337. Окно для выбора параметров при сохранении их в файле конфигурации

В данном окне необходимо отметить названия параметров, выбрать расположение и имя файла, в котором будет сохранена конфигурация (по умолчанию это системная папка DLLOCK80). После нажатия кнопки «ОК» файл конфигурации будет сформирован и сохранен. Появится подтверждение операции. Сохраненный файл конфигурации будет иметь расширение *.dlc.

Примечание. Если на клиенте системы защиты Dallas Lock 8.0, находящемся в одном домене AD, зарегистрированы учетные записи из другого домена AD, и эти домены не связаны, то сохранение конфигурации с параметром «Пользователи» → «Все» приведет к ошибке.

18.2 Применение файла конфигурации Dallas Lock

Файл конфигурации может быть использован в следующих случаях:

1. При установке системы защиты. В этом случае рекомендуется сохранять файл конфигурации со всеми параметрами.

   Применение файлов конфигурации в процессе установки может быть полезно, если, например, необходимо защитить с помощью Dallas Lock несколько автономных компьютеров, но на настройку политик безопасности на каждом компьютере по отдельности тратить время нет возможности или желания. В этом случае можно настроить СЗИ на одном компьютере, сохранить

его полную конфигурацию и при установке на остальные компьютеры, использовать полученный файл конфигурации.

2. В произвольный момент времени на локально установленной СЗИ.

   Для этого в списке функций кнопки  основного меню оболочки администратора необходимо кликнуть пункт «Применить конфигурацию» (рис. 336).
   Откроется окно проводника для поиска файла конфигурации. Требуется выбрать данный файл и нажать кнопку «Открыть». После этого система защиты применит данный файл, изменив свои параметры безопасности. На экране появится окно-отчет с информацией об операции.

3. В произвольный момент времени с помощью СБ для компьютеров, объединенных в ДБ (подробнее в главе «Сервер безопасности»).

Примечание. Стоит отметить, что Dallas Lock 8.0 позволяет применять файлы конфигурации от СЗИ Dallas Lock 7.7, что может быть полезно при миграции.

Примечание. Если клиентские компьютеры входят в ДБ, то использовать файлы конфигурации нет смысла, так как при следующей синхронизации все настройки политик, пользователей и т. п. будут взяты с СБ. В этом случае могут быть полезны только файлы конфигурации с настройками прав доступа к ресурсам ФС.

Помимо сохранения конфигурации клиентской части СЗИ имеется возможность сохранения и применения конфигурации СБ (см. «Сохранение конфигурации СБ»).

19 СЕРВЕР БЕЗОПАСНОСТИ

При использовании в ЛВС нескольких компьютеров, защищенных СЗИ Dallas Lock 8.0, возможно централизованное управление ими. Оно осуществляется с помощью Сервера безопасности Dallas Lock. Этот модуль должен быть установлен на отдельный компьютер, защищенный СЗИ Dallas Lock 8.0.

Остальные компьютеры, введенные под контроль данного СБ, становятся его клиентами и образуют ДБ.

СБ Dallas Lock 8.0 предоставляет следующие возможности:

- централизованное управление пользователями и группами пользователей на клиентах,
- централизованное управление политиками безопасности клиентов,
- централизованный сбор журналов с клиентов,
- управление доступом к ресурсам ФС и к устройствам на клиентах,
- просмотр состояния отдельных клиентов,
- объединение клиентов в группы.

Некоторые параметры безопасности могут быть настроены сразу для всего ДБ, некоторые — для групп клиентов, и некоторые — для отдельных клиентов.

СБ Dallas Lock 8.0 редакции «С» позволяет объединять клиентские рабочие станции, защищенные Dallas Lock 8.0 редакций «К» и «С». СБ Dallas Lock 8.0 редакции «К» — только ПК с Dallas Lock 8.0 редакции «К». Также следует обратить внимание, что управление клиентскими рабочими станциями, защищенными Dallas Lock 8.0 с активированными модулями МЭ, СОВ и СКН, возможно только при наличии СБ Dallas Lock 8.0 с активированными модуля МЭ, СОВ и СКН.

Централизованное управление осуществляется также с помощью ЕЦУ Dallas Lock (см. «Единый центр управления Dallas Lock»).

19.1 Общие принципы работы СБ

СБ реализован в виде службы, которая при загрузке ОС автоматически запускается при подключении к ПК лицензионного ключа СБ, запрограммированного в аппаратном идентификаторе (eToken или Рутокен (Rutoken)). Если ОС уже запущена, то при подключении лицензионного ключа СБ, запрограммированного в аппаратном идентификаторе, необходимо инициировать запуск службы СБ вручную.

Управление СБ осуществляется КСБ. Так как КСБ — это самостоятельная программа, то ее установка на рабочую станцию, защищенную Dallas Lock 8.0, может осуществляться независимо от того, установлен на ней СБ или нет. Таким образом, возможна работа в КСБ, расположенной на одном компьютере, с СБ, расположенном на другом компьютере.

Совместно с установкой СБ происходит автоматическая установка КСБ. Поэтому при установке на компьютер модуля СБ дополнительной установки программы КСБ не требуется.

КСБ представляет собой пользовательский интерфейс для отображения на экране информации о работе службы СБ. Пользователь может вызвать ее, нажав ярлык программы.

Если КСБ и СБ расположены на разных компьютерах, то запуск КСБ будет осуществляться при условии, что компьютер, на котором расположен СБ, включен.

Если при запуске КСБ появляется сообщение об ошибке, то необходимо проверить, предъявлен ли аппаратный идентификатор с ключом СБ, и запущена ли служба «Dallas Lock 8.0 Сервер безопасности» («Панель управления» → «Администрирование» → «Службы»).

19.1.1 Синхронизация

Синхронизация — это ключевое понятие в идеологии СБ. Под синхронизацией понимается процесс сверки соответствия параметров безопасности клиента с внутренней базой данных СБ и, при обнаружении несоответствия, модификация параметров безопасности клиента.

Что бы ни происходило на клиенте, какие бы настройки параметров умышленные или злоумышленные ни производились, при синхронизации все настраивается согласно записям СБ. Если параметры оставались без изменения (например, список пользователей), синхронизация этих параметров не происходит. Факты и результаты синхронизации отображаются в журнале СБ. Но если в процессе синхронизации на клиенте не было изменений, то запись в журнал СБ не заносится.

Синхронизация клиентов СДЗ происходит при каждом включении клиента СДЗ до момента авторизации пользователя.

Синхронизировать клиентов Windows и Linux с СБ можно следующими способами:

1. Из КСБ. Необходимо настроить периодичность синхронизации для всего ДБ.
2. Из КСБ (кнопки «Синхронизировать» на панели инструментов для объектов дерева КСБ) по команде администратора СБ.
3. Из оболочки администратора Dallas Lock 8.0 на клиентском ПК. Необходимо выбрать пункт «Синхронизировать компьютер с доменом безопасности» в меню кнопки  основного меню.
4. Из оболочки администратора Dallas Lock 8.0 на ПК, подключившись к целевому клиенту через оболочку сетевого администратора (см. «Сетевое администрирование»). Необходимо выбрать пункт «Синхронизировать компьютер с доменом безопасности» в меню кнопки  основного меню.

19.2 Установка и удаление СБ

19.2.1 Установка СБ

Для установки СБ необходимо выполнение ряда условий:

1. Компьютер должен быть защищен СЗИ Dallas Lock 8.0 (соответственно в редакции «К» или «С»).
2. Текущий пользователь должен иметь права администратора ОС СБ.
3. Компьютер не должен быть контроллером домена.
4. Должны быть открыты TCP/IP порты, используемые СБ для обмена данными с клиентами (17491, 17492, 17493, 17494, 17496, 17501, 17502).
5. Должен быть установлен драйвер аппаратного идентификатора.
6. К компьютеру должен быть подключен аппаратный идентификатор, содержащий информацию о лицензии на СБ и количестве поддерживаемых клиентов СБ.

Примечание. Если в ЛВС совместно с СБ планируется использование доменных пользователей, то необходимо также включить ПК, на котором расположен СБ, в соответствующий домен AD.

Примечание. При установке СБ полномочным для администрирования сервера пользователем становится суперадминистратор уже установленного клиента.

Чтобы установить СБ необходимо:

1. Запустить установочный файл «DL80-C.SecServer.msi» («DL80-K.SecServer.msi») и дождаться завершения копирования файлов (рис. 338). СБ всегда по умолчанию устанавливается в папку «C:\DLLOCK80\DlSecServer».

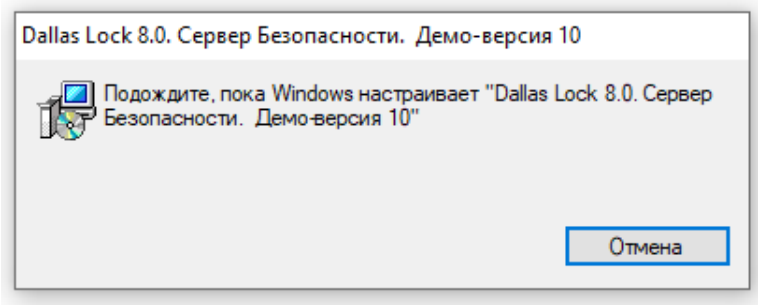


Рис. 338. Подготовка ОС к установке СБ

2. После завершения копирования файлов запустится окно установки СБ (рис. 339). В программе установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность отмены установки с возвратом сделанных изменений. Для этого служит кнопка «Назад». Для выполнения следующего шага установки нажать кнопку «Далее».

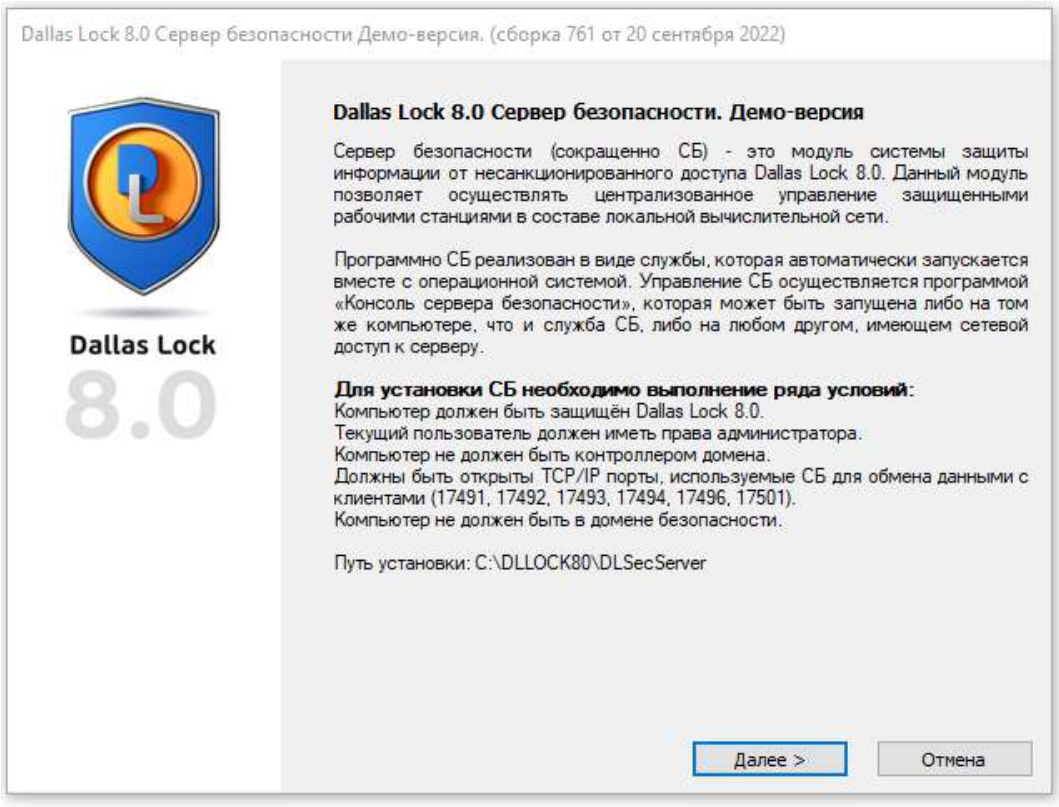


Рис. 339. Окно приглашения установки СБ

3. Опционально поставить флаг и заполнить поля подключения для ввода СБ в уже существующий ДБ (рис. 340) (см. «Репликация»). Для продолжения установки нажать кнопку «Далее».

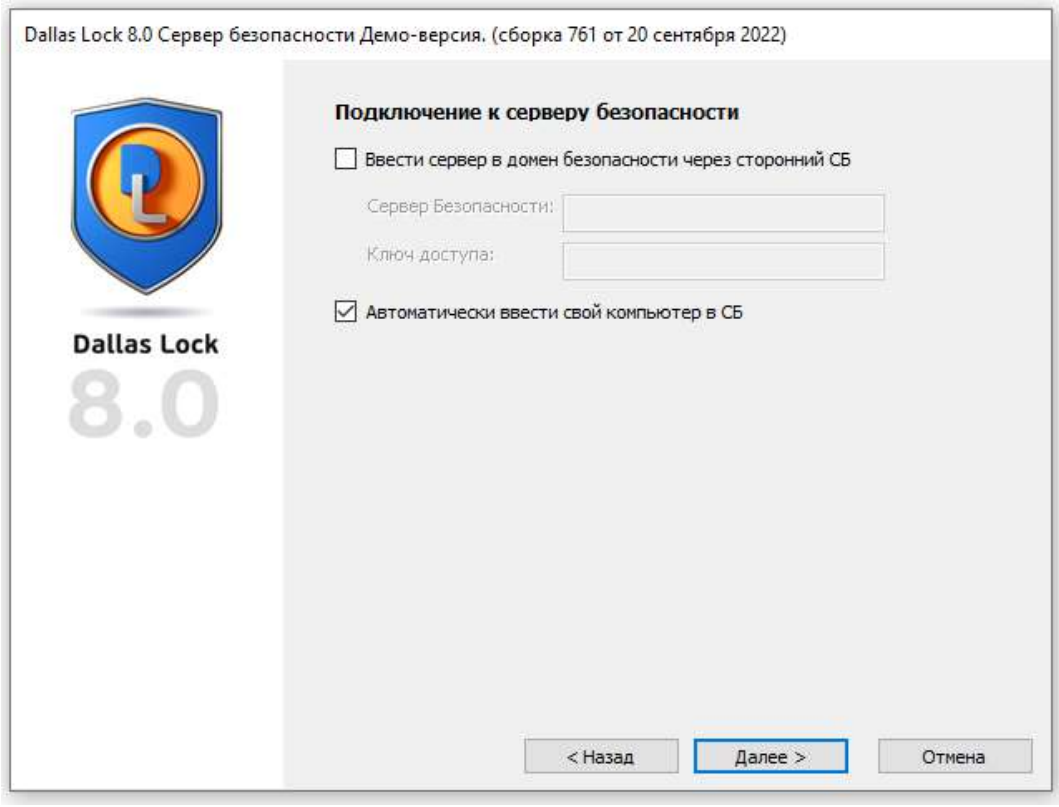


Рис. 340. Установка СБ

4. Опционально поставить флаг и заполнить поля подключения к системе хранения данных MS SQL Server (рис. 341) (подробнее см. в документе «Инструкция по использованию SQL-сервера для СБ» RU.48957919.501410-02 И3). Для продолжения установки нажать кнопку «Далее».

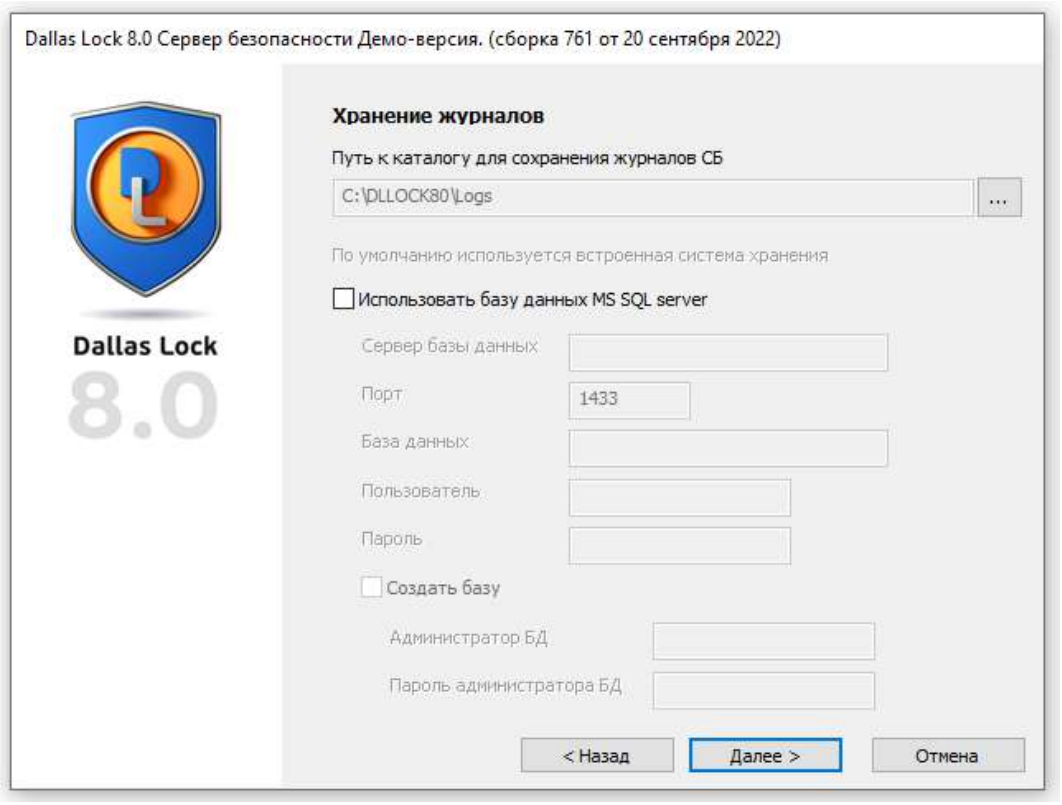


Рис. 341. Установка СБ

5. Опционально поставить флаг и заполнить поля подключения к СЛ (рис. 342) (подробнее об использовании СЛ см. в документе «Инструкция по использованию сервера лицензий» RU.48957919.501410-02 И2). Для продолжения установки нажать кнопку «Установить».

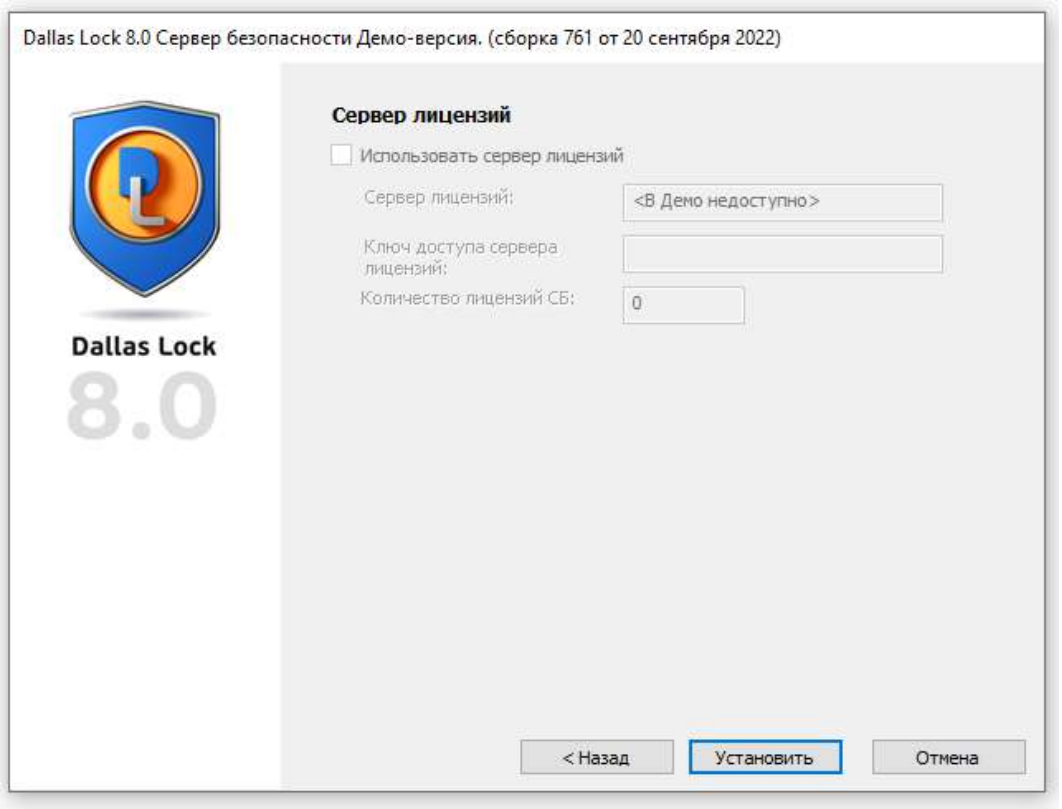


Рис. 342. Установка СБ

6. Далее происходит процесс установки. Если процесс прошел без ошибок, то появится сообщение «Установка успешно завершена!». При этом перезагрузка ПК не требуется (рис. 343).

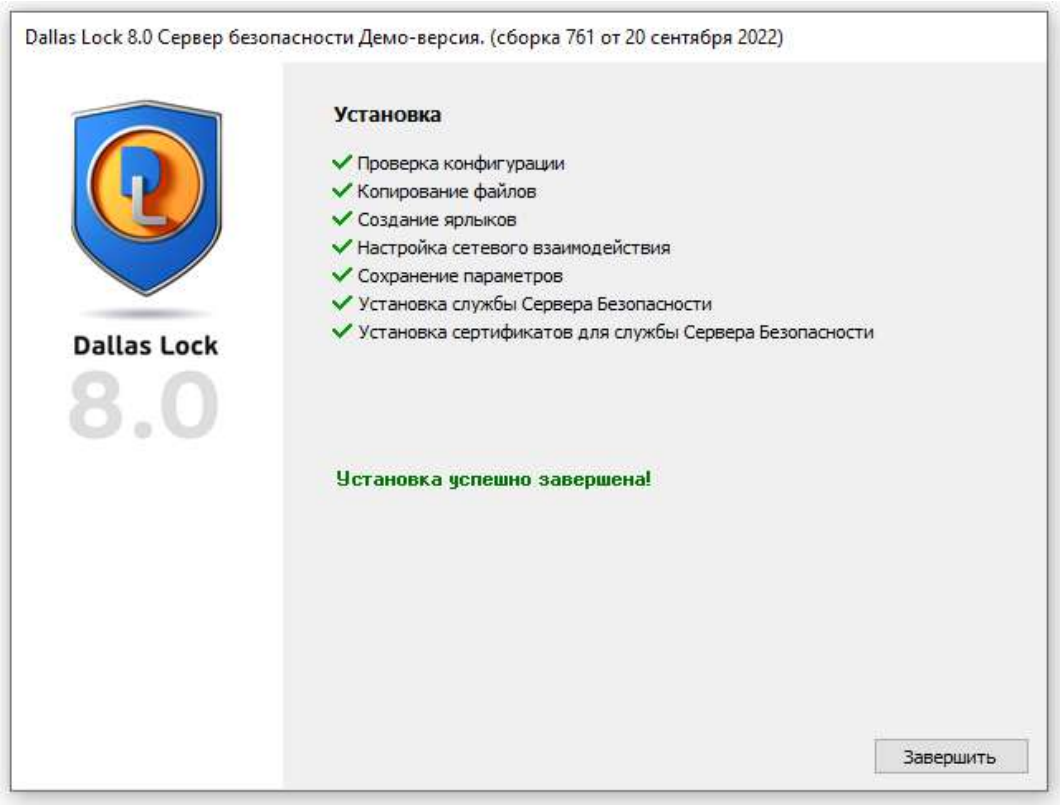


Рис. 343. Состояние установки СБ

После этого в меню «Пуск» и на рабочем столе появится ярлык для запуска КСБ (рис. 344).

Рис. 344. Ярлык КСБ на рабочем столе

19.2.2 Удаление СБ

Удаление СБ производится с помощью Мастера установок. В разных операционных системах запуск Мастера установок может осуществляться по-разному.

Перед удалением СБ рекомендуется сохранить его конфигурацию (см. «Сохранение конфигурации СБ»).

В ОС Windows 10 необходимо вызвать пункт «Параметры», выбрать пункт «Приложения». В появившемся окне два раза нажать на СБ и выбрать действие «Удалить», подтвердить удаление (рис. 345).

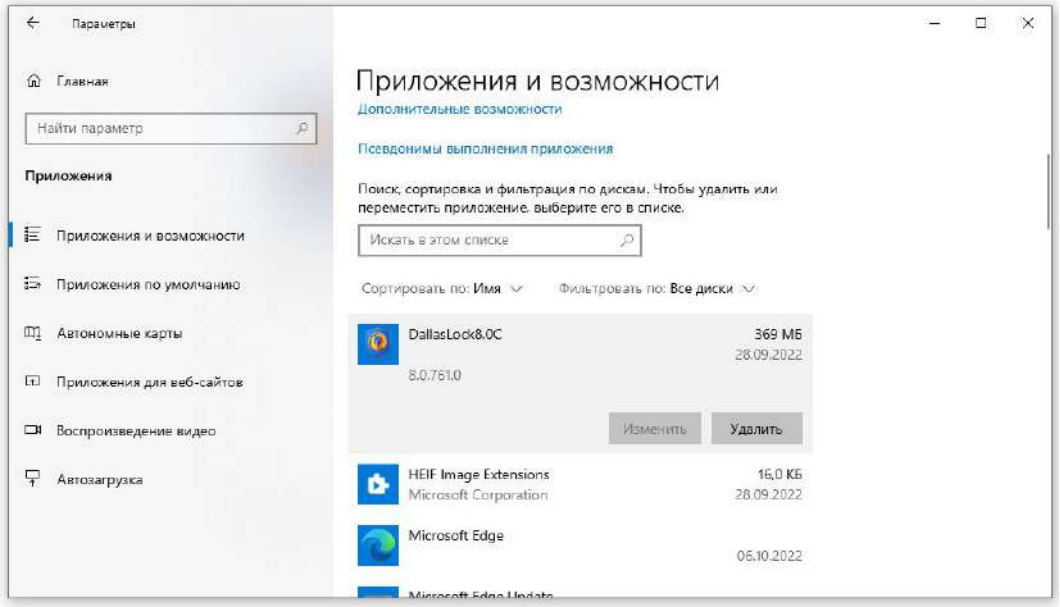


Рис. 345. Удаление программы СБ

После удаления СБ перезагрузки компьютера не требуется.

Если использовался механизм лицензирования через СЛ, при удалении СБ зарезервированная квота на управление клиентами возвращается на СЛ.

19.3 Администрирование СБ

Управление СБ осуществляется с помощью КСБ.

Примечание. Стоит отметить, что возможно одновременное подключение нескольких КСБ к ДБ при наличии нескольких серверов безопасности в таком домене. Одномоментно возможно подключение неограниченного числа КСБ к одному Серверу безопасности.

Так как СБ может быть установлен на один ПК, а КСБ на другой, то вход на КСБ с указанием подключенного СБ может осуществляться под той учетной записью, которая зарегистрирована в оболочке администратора Dallas Lock 8.0 на СБ.

Также для учетной записи, под которой осуществляется подключение КСБ, должны быть определены следующие разрешающие права на СБ (учетная запись должна быть установлена для параметров доступа Dallas Lock 8.0):

Для возможности пользователя осуществлять полную настройку и установку параметров безопасности на СБ	Для возможности пользователя осуществлять только аудит (просмотр) настроенных параметров безопасности на СБ
• «Параметры безопасности: Управление»; • «Учетные записи: Управление»; • «Межсетевой экран: Изменение настроек»; • «СОВ МЭ: Изменение настроек»; • «Аудит: Просмотр журналов»; • «Аудит: Управление»; • «Ресурсы: Управление дискреционным доступом»; • «Ресурсы: Управление мандатным доступом» (только для Dallas Lock 8.0 редакции «С»); • «Ресурсы: Управление контролем целостности»; • «Администрирование на СБ»	• «Параметры безопасности: Просмотр»; • «Межсетевой экран: Просмотр настроек»; • «СОВ МЭ: Просмотр настроек». • «Аудит: Просмотр журналов»; • «Аудит: Просмотр теневых копий распечатываемых документов»; • «Аудит: Просмотр теневых копий файлов».

Примечание. Для администрирования СБ доменным пользователем его учетная запись должна быть зарегистрирована в системе защиты отдельно, а не с помощью маски «*/*» (см. «Регистрация доменных пользователей»).

После входа на КСБ под учетной записью пользователя с правами только на просмотр параметры безопасности будут отображены, но не будет возможности их редактировать, производить настройки и действия; кнопки, отвечающие за настройки, будут недоступны.

19.4 КСБ

Ярлык КСБ появляется на рабочем столе после установки СБ. Вызвать КСБ можно двойным кликом мыши.

В окне подключения к СБ требуется ввести следующие данные (рис. 346):

- имя ПК, на котором установлен СБ (автоматически отображается имя локального);
- имя учетной записи (подставляется автоматически при выборе аппаратного идентификатора с записанными данными);
- домен (если это доменная учетная запись);
- предъявить и выбрать аппаратный идентификатор;
- пароль учетной записи пользователя.

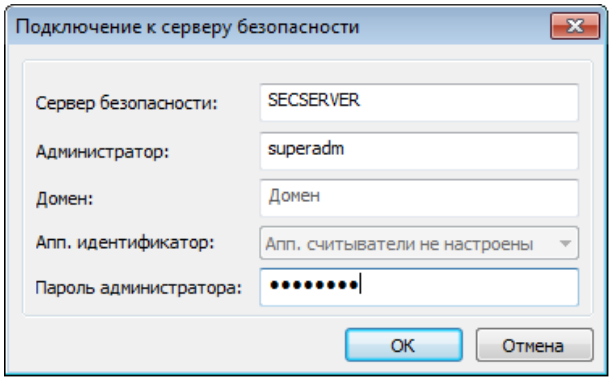


Рис. 346. Ввод пароля учетной записи для входа в КСБ

Главное окно КСБ содержит следующие рабочие области (рис. 347):

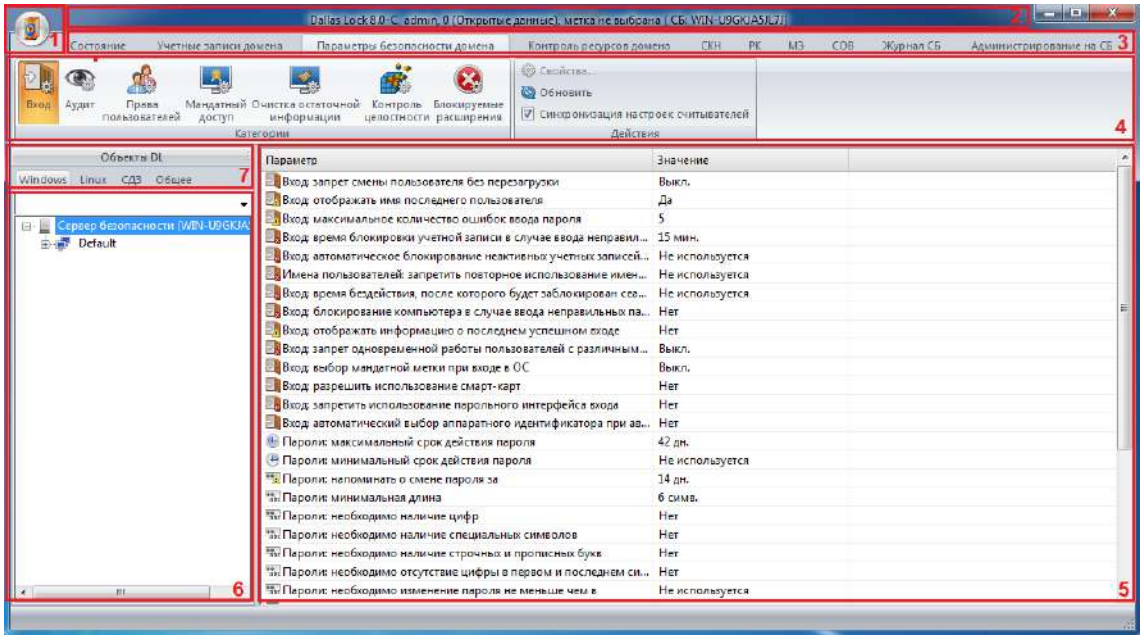


Рис. 347. Окно КСБ

1. Кнопка основного меню, раскрывающая дополнительное меню.
2. Заголовок окна (верхняя строка), содержащий название версии системы защиты, имя СБ (по имени компьютера) и уровень доступа текущего пользователя.
3. Основное меню с набором основных вкладок. Это меню меняется в зависимости от выбора объекта в проводнике (пункт 5).

4. Категории параметров основного меню и панель действий.
5. Информационная панель, содержащая списки параметров или объектов текущей категории.
6. Проводник в виде дерева объектов, отображающий список клиентов и групп клиентов или объектов СБ, входящих в ДБ.
7. Вкладки выбора клиентов Windows, Linux, СДЗ и Общее.

С помощью КСБ можно настроить параметры безопасности для следующих объектов ДБ:

- для всего ДБ, определив настройки при выборе объекта, обозначающего СБ в дереве объектов КСБ;
- для группы клиентов, определив настройки при выборе объекта, обозначающего группу в дереве объектов КСБ;
- для индивидуального клиента, выбрав его в дереве объектов КСБ.

Для каждого из объектов в основном меню КСБ формируется свой список вкладок. При выборе вкладки, в рабочей области открывается страница с соответствующими параметрами и меню.

Значки объектов, обозначающие клиентов СБ, в зависимости от состояния клиента могут принимать следующий вид:

 — клиент Default;

 — клиент выключен;

 — связь с клиентом отсутствует свыше заданного на СБ времени, которое определяется параметром «Оповещение при отсутствии связи с клиентом» (при условии, что настроено оповещение об отсутствии связи с клиентом);

 — на клиенте не отвечает Dallas Lock 8.0/Dallas Lock Linux;

 — клиент включен;

 — СБ собирает журналы с клиента Dallas Lock 8.0;

 — на клиенте установлена более старая версия Dallas Lock 8.0. Для таких клиентов не доступно ОУ и не работает синхронизация;

 — на клиенте установлена более старая версия Dallas Lock 8.0, при этом клиент работает в «неактивном режиме СЗИ»;

 — клиент работает в «неактивном режиме СЗИ».

Контекстное меню объектов дерева КСБ позволяет добавлять/удалять/переименовывать группы клиентов, перемещать клиентов из группы в группу, синхронизировать клиентов по команде администратора СБ Dallas Lock и производить другие операции.

19.5 Сохранение конфигурации СБ

Для сохранения настроек СБ необходимо открыть дополнительное меню КСБ  → «Сохранить конфигурацию».

Появится окно, в котором необходимо выбрать расположение и имя файла, в котором будет сохранена конфигурация (по умолчанию предварительно задан путь «C:\DLLOCK80» и частота сохранения файла конфигурации). После нажатия кнопки «ОК» файл конфигурации СБ будет сформирован и сохранен. Сохраненный файл конфигурации будет иметь расширение *.dlsc2.

Применяется данный файл конфигурации на уже установленный СБ с помощью пункта «Применить конфигурацию» кнопки дополнительного меню КСБ.

Примечание. Сохранение и применение файла конфигурации СБ осуществляется только на соответствующем СБ (на котором данная конфигурация была сформирована). В случае, если СБ находится в кластере серверов, данные функциональные возможности для него недоступны.

Для синхронизации конфигурации необходимо открыть дополнительное меню КСБ  → «Синхронизировать конфигурацию» (будет неактивно в случае, если в ДБ не введены другие сервера) → выбрать определенный сервер или произвольный сервер (в этом случае выбор будет произведен автоматически) для синхронизации (рис. 348).

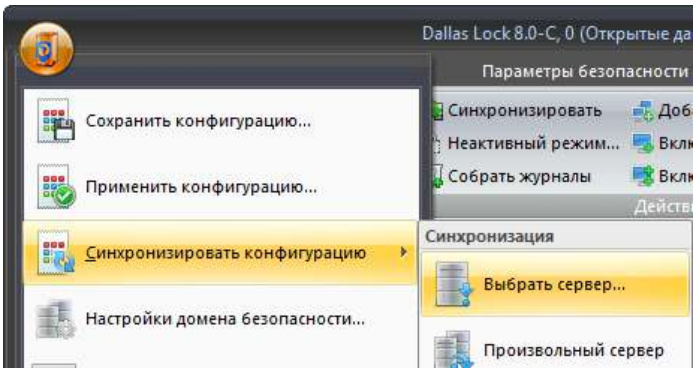


Рис. 348. Синхронизация конфигурации СБ

19.6 Ключ доступа к СБ

КСБ позволяет установить ключ доступа к СБ, который нужен для ввода клиентов в ДБ. По умолчанию ключ доступа — пустой.

Для изменения ключа доступа к СБ необходимо открыть дополнительное меню КСБ → «Ключ доступа к СБ…».

Появится окно «Ключ доступа к СБ», где необходимо заполнить требуемые поля (рис. 349).

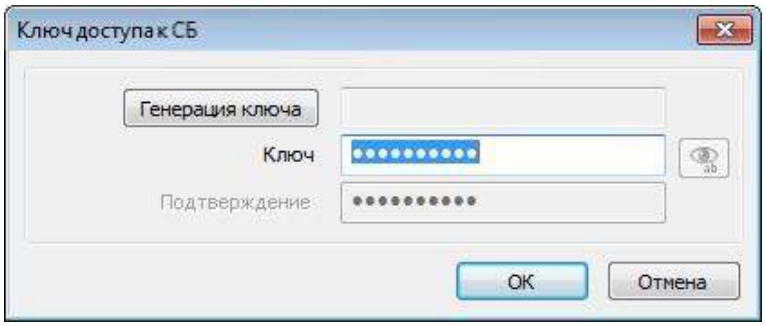


Рис. 349. Ключ доступа СБ

Примечание. Политики сложности паролей в оболочке администратора СБ распространяются на установку значений для ключа доступа к СБ. Чтобы была возможность задать пустое значение ключа доступа к СБ, необходимо, чтобы в оболочке администратора СБ параметр «Пароли: минимальная длина» имел значение «Не используется».

19.7 Настройки лицензирования

СЛ позволяет централизовать и упростить управление лицензиями на терминальные подключения и на клиентов в нескольких доменах безопасности (подробнее см. в документе «Инструкция по использованию сервера лицензий» RU.48957919.501410-02 И2).

Для изменения параметров СЛ для СБ необходимо открыть дополнительное меню КСБ → «Настройки лицензирования…».

Появится окно «Настройки сервера лицензии для Сервера безопасности». Для использования СЛ необходимо поставить флаг «Использовать сервер лицензий», заполнить параметры подключения к СЛ и ввести количество лицензий (рис. 350).

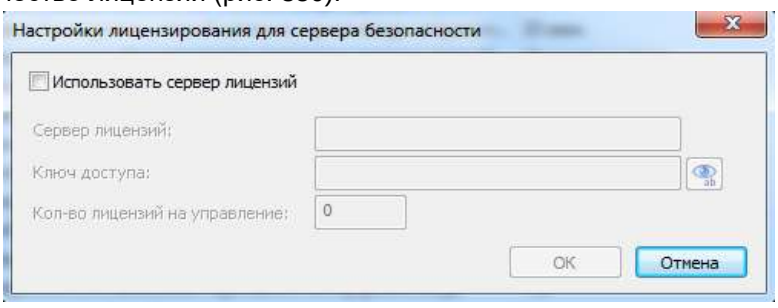


Рис. 350. Настройка СЛ для СБ

Примечание. На момент установки СБ допускается отсутствие СЛ в сети. В таком случае при установке СБ можно в параметрах подключения к СЛ указать данные пока не доступной машины (т. е. не выполняется валидация путем подключения). СЛ должен быть доступен при запуске СБ, в противном случае СБ будет запущен с нулевой квотой на централизованное управление.

19.8 Параметры хранения журналов

Существует возможность выгружать журналы всех клиентов ДБ во внешнюю MS SQL базу данных.

Для использования внешней MS SQL базы данных в СБ необходимо выполнение ряд требований (подробнее см. в документе «Инструкция по использованию SQL-сервера для СБ» RU.48957919.501410-02 И3).

Для изменения параметров хранения журналов, необходимо открыть дополнительное меню КСБ → «Параметры хранения журналов».

Появится окно «Параметры хранения журналов». Для сохранения журналов в существующую БД, необходимо поставить флаг «Использовать базу данных MS SQL Server» и заполнить параметры подключения к БД (рис. 351).

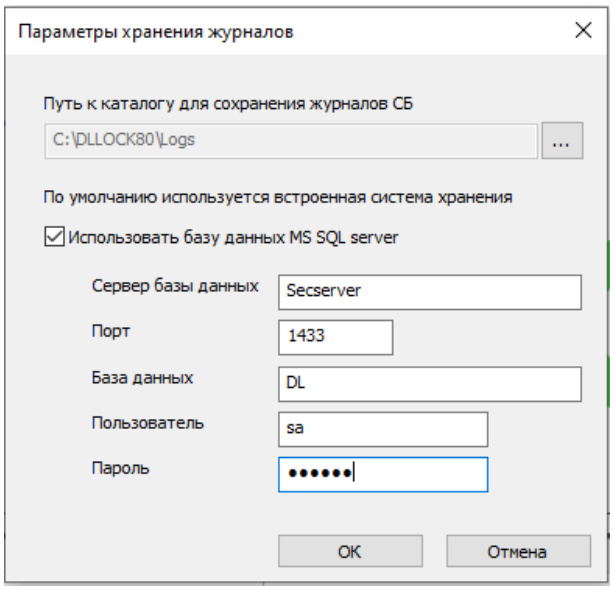


Рис. 351. Параметры хранения журналов

Хранение журналов осуществляется в каталоге, который был указан при установке СБ. Путь к этому каталогу отображен в поле «Путь к каталогу для сохранения журналов СБ», также его можно изменить нажав кнопку ....

Для сохранения журналов в файлы на СБ требуется снять флаг с параметра «Использовать базу данных MS SQL Server».

19.9 Ролевая модель учетных записей СБ

Настройки по правам администрирования на СБ осуществляются в рабочей области для вкладки

«Администрирование на СБ», находящейся в правом верхнем углу (рис. 352).

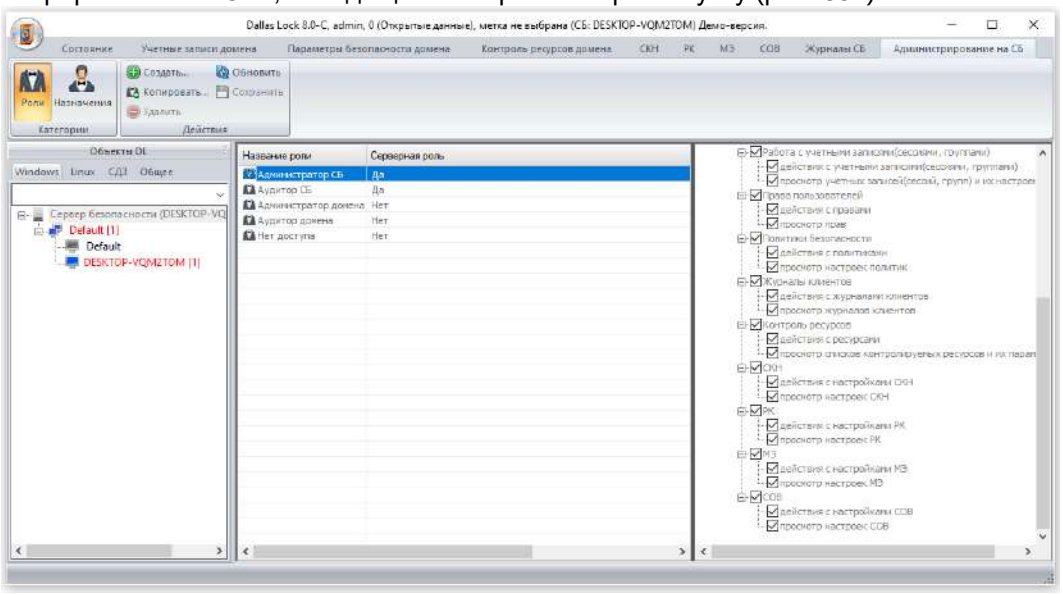


Рис. 352. Администрирование на СБ

Роль представляет собой совокупность привилегий — полномочий по выполнению действий в части администрирования СБ и ДБ. Для удобства привилегии группируются в несколько категорий в зависимости от области применения.

Различным учетным записям (или группам пользователей) ДБ ставится в соответствие роль, отображающая права данного пользователя (группы) в части администрирования средствами СБ.

Рабочая область категории «Роли» состоит из трех разделов: «Название роли», «Серверная роль» и «Привилегии».

Привилегии разделены на два раздела: «Управление СБ» и «Управление ДБ». Каждая привилегия дает пользователю права на совершение определенных операций, например, привилегия «управление СБ» позволяет пользователю, имеющему роль с данной привилегией, осуществлять централизованную смену лицензий, а привилегия «управление режимами работы» в разделе «Управление ДБ» дает право пользователю осуществлять через КСБ смену лицензий непосредственно на клиентах.

Ролевая модель учетных записей подразумевает наличие двух типов ролей: серверной и доменной. Особенность серверной роли заключается в том, что пользователь, которому назначена серверная роль, может пользоваться привилегиями как на управление СБ, так и на управление ДБ. Серверная роль назначается только на уровне СБ. Доменная же роль наделяется привилегиями на управление только ДБ и может быть назначена как на уровне СБ, так и на уровне группы клиентов. Для доменной и серверной ролей осуществляется автоматическое наследование назначения на более низкоуровневых узлах. Изменения на нижних узлах не влияют на настройки верхних, что позволяет создавать отдельные назначения для групп и подгрупп клиентов. Например, если пользователю назначена серверная роль с привилегиями только на управление СБ, она может быть переопределена как доменная на уровне группы или подгруппы, при этом на уровне СБ роль назначения не изменится, поменяется только имя владельца назначения.

Также на уровнях ниже уровня СБ нельзя переопределить роль назначения на серверную, это возможно только на уровне СБ.

При удалении назначения, роль которого была переопределена на уровне группы или подгруппы с серверной на доменную, оно не исчезнет из списка назначений, а вернется в исходное состояние, заданное на СБ. При удалении назначений и ролей на уровне СБ они удаляются также на всех уровнях.

Пример 1

1. На уровне СБ был создан пользователь «*user1*» и в категории «Назначения» на вкладке «Администрирование на СБ» ему была назначена доменная роль «Аудитор домена» (рис. 353).

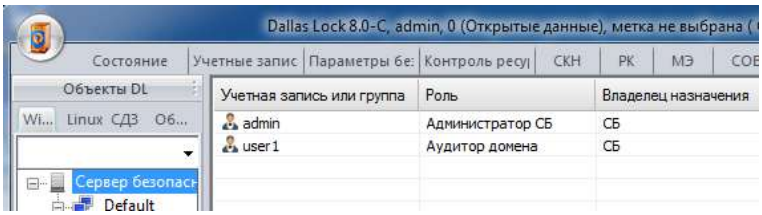


Рис. 353. Назначена доменная роль

2. На уровне группы назначенная роль была изменена на роль «Администратор домена» (рис. 354). На уровне СБ в категории «Назначения» список назначений остался прежним (рис. 353).

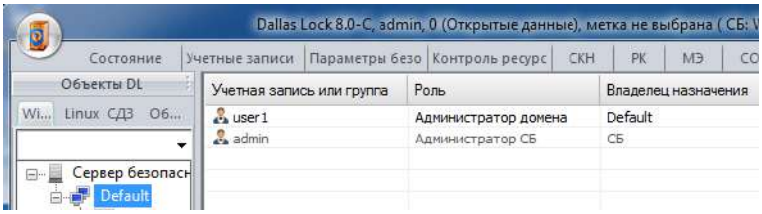


Рис. 354. Роль переопределена на уровне группы

3. На уровне группы удалили назначение роли «Администратор домена» пользователю «*user1*». После сохранения внесенных изменений назначение пользователя «*user1*» вернулось к изначально заданному на СБ (рис. 355).

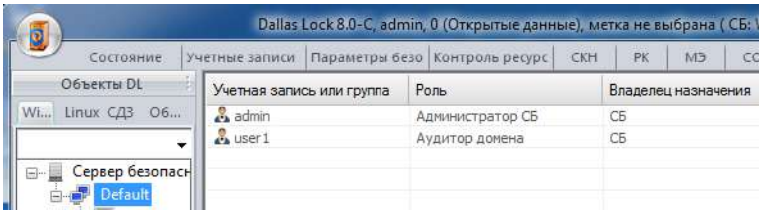


Рис. 355. Удаление назначения на уровне группы

4. После удаления на уровне СБ назначения для пользователя «*user1*», назначение также удаляется и на нижестоящих узлах (рис. 356).

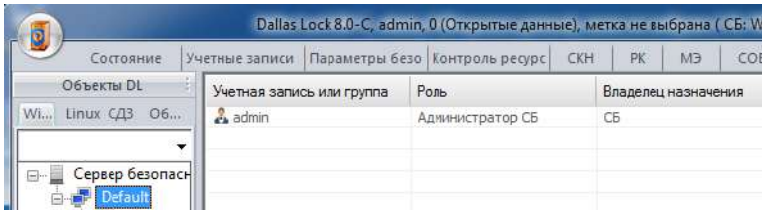


Рис. 356. Удаление назначения на уровне СБ

Пример 2

1. На уровне СБ был создан пользователь «*user2*» и в категории «Назначения» на вкладке «Администрирование на СБ» ему была назначена созданная серверная роль «Аудитор СБ» (рис. 357).

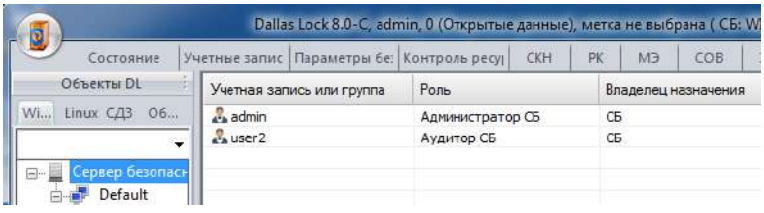


Рис. 357. Назначена серверная роль

2. На уровне группы назначенная роль была изменена на роль «Администратор домена» (рис. 354, рис. 358). На уровне СБ в категории «Назначения» список назначений остался прежним (рис. 357).

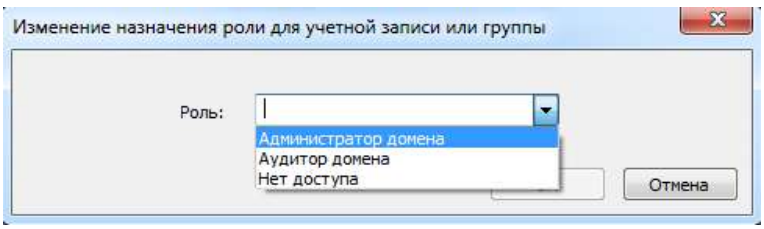


Рис. 358. Доступные на уровне группы назначения

3. На уровне группы удалили назначение роли «Администратор домена» пользователю «*user2*». После сохранения внесенных изменений назначение пользователя «*user2*» вернулось к изначально заданному на СБ (рис. 359).

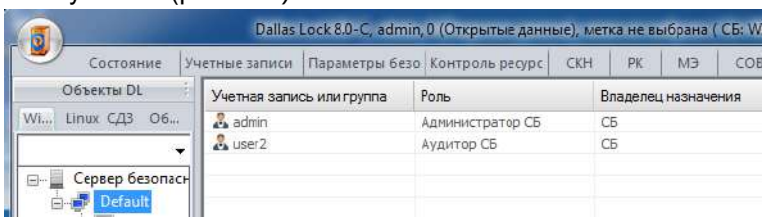


Рис. 359. Удаление назначения на уровне группы

4. После удаления на уровне СБ назначения для пользователя «*user2*», назначение также удаляется и на нижестоящих узлах (рис. 360).

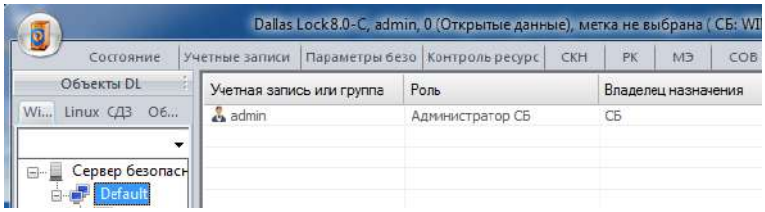


Рис. 360. Удаление назначения на уровне СБ

Процедуры создания, изменения и удаления ролей, а также управления назначениями подробнее описаны ниже.

В СБ существуют роли по умолчанию, которые невозможно отредактировать или удалить.

Роли типа «Серверная роль» по умолчанию:

- «Администратор СБ»;
- «Аудитор СБ».

Роли типа «Доменная роль» по умолчанию:

- «Администратор домена»;
- «Аудитор домена»;
- «Нет доступа».

Роли по умолчанию имеют следующие настройки:

Роль пользователя по умолчанию	Настройки
Администратор СБ	Все привилегии
Аудитор СБ	Все привилегии на просмотр
Администратор домена	Все привилегии из раздела «Управление ДБ»
Аудитор домена	Все привилегии на просмотр из раздела «Управление ДБ»
Нет доступа	Все привилегии отключены

Пользователь с правами на настройку и назначение ролей может осуществлять назначение и настройку ролей только в рамках своих привилегий (невозможно задать для роли права, которыми не обладает учетная запись, от имени которой осуществляется администрирование; невозможно назначение роли субъектом, если он не обладает хотя бы одной привилегией роли). При этом считается, что в привилегию действий входят все возможности аудита.

Примечание. Для пользователя или группы может быть назначена только одна роль на объект, однако, разрешения для пользователя могут складываться, если он является членом нескольких групп, для которых назначены разные роли на объект. При этом если роль явно назначается учетной записи пользователя, она перекрывает все права, полученные от групп.

Однако если пользователь состоит хотя бы в одной группе, которой явно была назначена роль «Нет доступа», все привилегии считаются снятыми.

19.9.1 Описание привилегий ролевой модели СБ

Привелегии ролевой модели СБ предоставляют следующие полномочия по выполнению действий в части администрирования СБ и ДБ:

Привилегия	Описание
Управление СБ	
Управление СБ	Включает в себя все действия основного меню СБ
Аудит СБ	Включает в себя возможность просмотра информации основного меню СБ
Архивирование и экспорт журнала СБ	Включает в себя возможность производить архивирование и экспорт журнала СБ
Аудит журнала СБ	Включает в себя работу с фильтрами, просмотр журнала, открытие журнала, настройка параметров СБ в части сбора журналов и оповещений о событиях на клиенте
Настройка и назначение ролей	Включает в себя возможность управления ролями, в том числе создание ролей и их назначение учетным записям и группам
Аудит настройки и назначения ролей	Включает в себя возможность просмотра ролей и назначений ролей
Управление ДБ	
Изменение состава ДБ	Позволяет осуществлять ввод/вывод клиента в ДБ (для СДЗ только вывод из ДБ), управление деревом клиентов, установку, обновление и удаление СЗИ клиентов, подготовку дистрибутива для AD. Учетная запись с данной привилегией всегда видит группу и клиента Default
Общие настройки клиентов	
Управление общими настройками клиентов	Включает в себя привилегии работы с вкладкой и блоком «Состояние», установку описания клиента, установку ключа доступа СБ
Аудит общих настроек клиентов	Включает в себя привилегии на просмотр информации вкладки «Состояние», просмотр информации блока «Состояние»
Действия над клиентами	Включает в себя привилегии на подключение/отключение к клиенту, завершение работы, перезагрузку клиента, Wake-on-lan
Управление режимами работы	Включает в себя привилегии на изменение номера лицензий, управление неактивным режимом, работу с файлами конфигурации (в том числе через задания), работу с отчетами (в том числе через задания)
Аудит режима работы	Включает в себя работу с отчетами (в том числе через задания), просмотр списка заданий, просмотр списка лицензий при назначении на СБ
Работа с учетными записями (сессиями, группами)	
Действия с учетными записями (сессиями, группами)	Включает в себя возможность создания и удаления учетных записей и групп, редактирования их свойств. Доступен просмотр списка учетных записей и групп, а также просмотр свойств учетных записей и групп
Просмотр учетных записей (сессий, групп) и их настроек	Включает в себя возможность просмотра списка ученых записей, групп, а также их свойств без полномочий на их изменение
Права пользователей	
Действия с правами	Включает в себя возможность просмотра и назначения прав пользователей для пользователей и групп
Просмотр прав	Включает в себя возможность только просмотра прав пользователей и их назначений
Политики безопасности	
Действия с политиками	Включает в себя возможность просмотра и изменения политик безопасности для ДБ
Просмотр настроек политик	Включает в себя возможность только просмотра политик безопасности для ДБ
Журналы клиентов	
Действия с журналами клиентов	Включает в себя возможности сбора журналов клиентов, их просмотр, экспорт, удаление, настройку параметров фильтра журналов

Привилегия	Описание
Просмотр журнала клиентов	Включает в себя возможность только сбора и просмотра журналов клиентов
Контроль ресурсов	
Действия с ресурсами	Включает в себя возможность просмотра списка ресурсов ДБ и назначенных на них прав доступа, возможность назначения, изменения и удаления прав доступа для ресурсов ДБ
Просмотр списков контролируемых ресурсов и их параметров	Включает в себя возможность только просмотра списка ресурсов ДБ и выполненных настроек доступа для ресурсов ДБ
СКН	
Действия с настройками СКН	Включает в себя возможность регистрации СКН, назначения, изменения и удаления прав доступа для СКН, задания, редактирования и удаления описания для СКН, создания, редактирования и удаления ключей преобразования
Просмотр настроек СКН	Включает в себя возможность просмотра списка зарегистрированных СКН, их описаний, назначенных на них прав доступа, возможность просмотра списка ключей преобразования
РК	
Действия с настройками РК	Включает в себя возможность изменения настроек РК для ДБ
Просмотр настроек РК	Включает в себя возможность просмотра настроек РК для ДБ, управление настройками РК при этом запрещено
МЭ	
Действия с настройками МЭ	Включает в себя возможность изменения настроек МЭ для ДБ, в том числе создание, изменение и удаление правил МЭ
Просмотр настроек МЭ	Включает в себя возможность просмотра настроек МЭ для ДБ, управление настройками МЭ при этом запрещено
СОВ	
Действия с настройками СОВ	Включает в себя возможность изменения настроек СОВ для ДБ
Просмотр настроек СОВ	Включает в себя возможность просмотра настроек СОВ для ДБ, управление настройками СОВ при этом запрещено

19.9.2 Создание и изменение ролей

Создать новую роль можно нажатием одной из кнопок: «Создать» или «Копировать» в блоке «Действия». После нажатия в списке ролей появляется новое редактируемое поле, в котором необходимо задать имя для роли. Для подтверждения операции нужно нажать «Enter» или в любую другую рабочую область. Далее произойдет проверка допустимости введенного имени (имя не может быть пустым или совпадать с уже существующим).

Примечание. Настройка ролей для пользователей и групп пользователей осуществляется только при выбранном СБ в дереве клиентов.

По умолчанию все новые роли создаются типа «Доменная роль» и все привилегии для них отключены. Для назначения привилегий необходимо корректно заполнить поле с привилегиями и нажать кнопку «Сохранить» на панели сверху.

При копировании роли все атрибуты роли, копия которой создается, сохраняются.

Для всех ролей, кроме ролей по умолчанию, доступно изменение значений параметра «Серверная роль». Для изменения необходимо дважды кликнуть левой кнопкой мыши в поле «Серверная роль» для выбранной роли. При этом появится одно из двух возможных типов предупреждений об изменении (рис. 361, рис. 362).

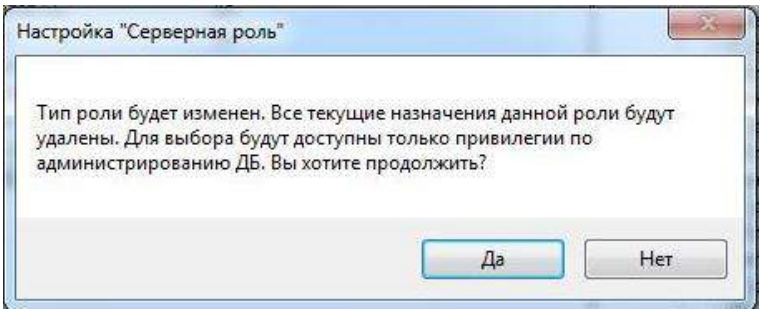


Рис. 361. Изменение параметра «Серверная роль» с северной на доменную

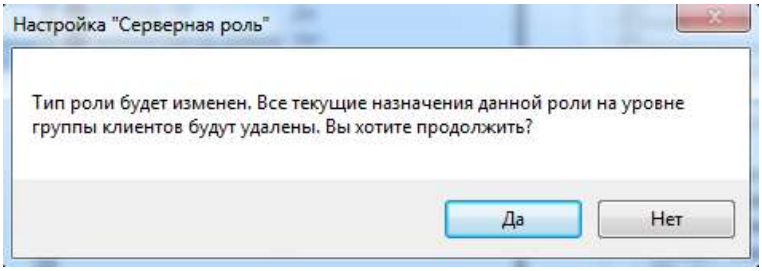


Рис. 362. Изменение параметра «Серверная роль» с доменной на серверную

В случае продолжения действий все назначения данной роли на уровне группы клиентов удаляются.

Все роли за исключением ролей по умолчанию, можно переименовывать.

После внесения всех необходимых изменений следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия».

19.9.3 Удаление ролей

Для удаления роли необходимо выделить удаляемую роль и нажать кнопку «Удалить» в блоке «Действия». При этом на экране появится предупреждение (рис. 363).

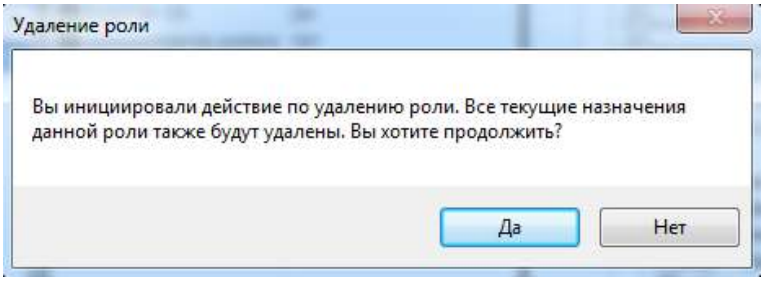


Рис. 363. Удаление роли

После удаления назначенной роли все назначения данной роли удаляются.

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия».

19.9.4 Управление назначениями ролей

Назначение ролей может осуществляться на уровне СБ или группы дерева клиентов вкладки «Общие», при этом настройки на более низкоуровневом узле имеют приоритет выше по сравнению с настройками на более высокоуровневом узле.

Примечание. Назначения ролей могут осуществляться только на учетные записи и группы ДБ СЗИ.

Примечание. Серверную роль можно назначить только на уровне СБ. Порядок наследования назначений описан выше.

Примечание. При назначении на СБ доменной роли, она считается назначенной на всех узлах дерева клиентов. Если назначить роль на уровне группы, она считается назначенной на всех клиентах группы.

Для перехода в режим назначения учетных записей и групп на роли на уровне СБ, необходимо на верхней панели выбрать категорию «Назначения». Рабочая область данной категории состоит из таблицы с полями «Учетная запись или группа», «Роль» и «Владелец назначения».

Категория «Назначения» на уровне группы доступна по умолчанию и имеет аналогичную структуру.

Для назначения новой роли для пользователя или группы необходимо нажать на кнопку «Создать» в блоке «Действия» (рис. 364).

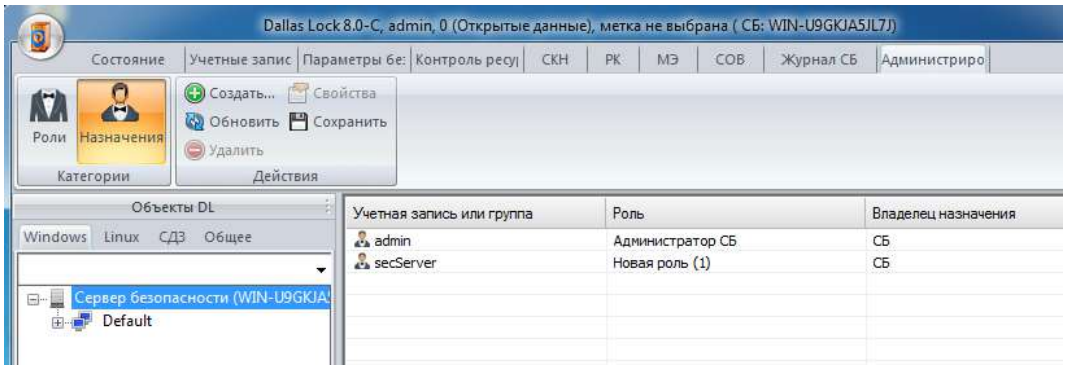


Рис. 364. Назначение ролей

После этого появляется окно, в котором можно выбрать учетные записи пользователя или группы, и в выпадающем списке внизу выбрать назначаемую им роль администрирования на СБ (рис. 365).

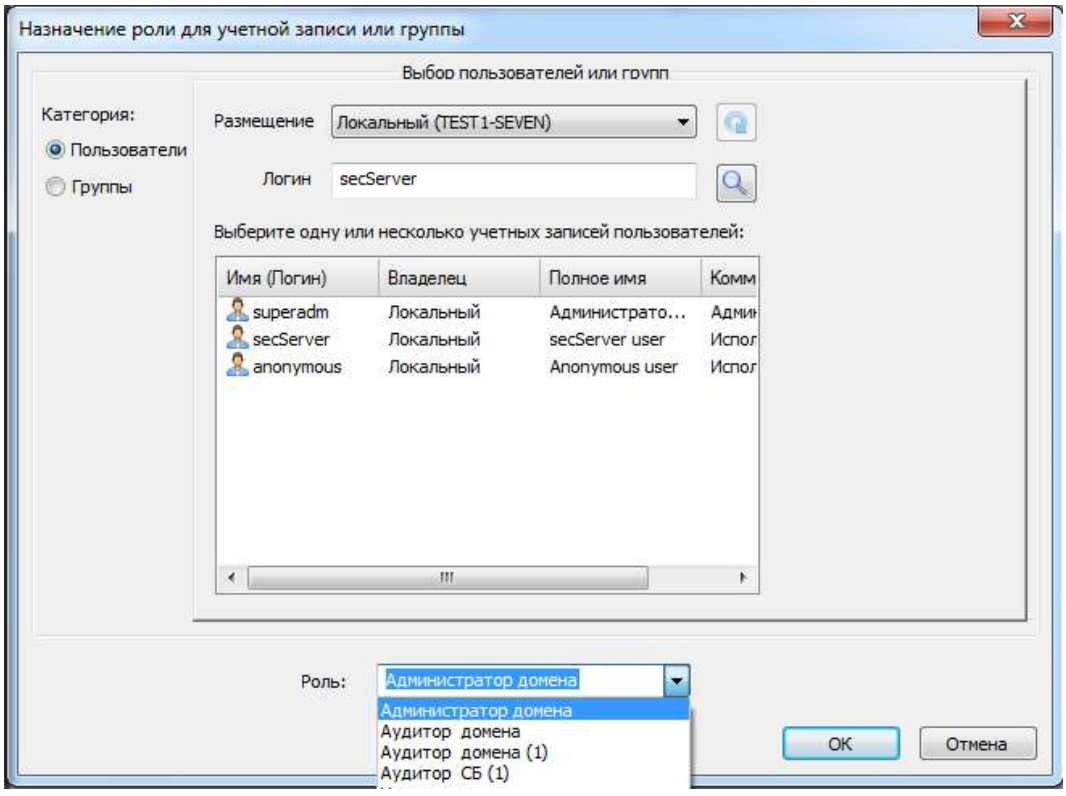


Рис. 365. Назначение роли для учетной записи или группы

Смена роли для учетной записи или группы осуществляется при помощи выделения ее в таблице и нажатия кнопки «Свойства» в блоке «Действия». При этом открывается диалоговое окно с выпадающим списком для выбора назначаемой роли (рис. 366).

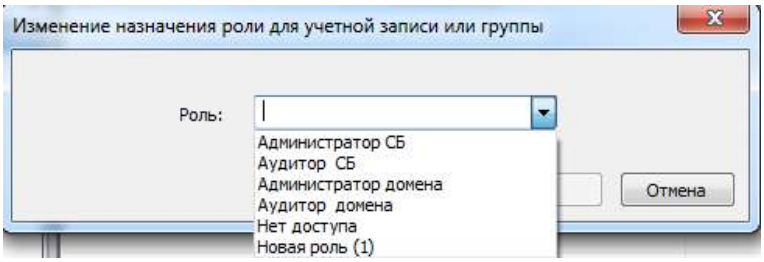


Рис. 366. Изменение назначения роли для учетной записи или группы

Примечание. При назначении роли для учетной записи или группы, для которых назначение уже было создано, происходит переназначение данной роли.

Для удаления назначения необходимо выделить удаляемую роль, на панели сверху нажать кнопку «Удалить» в блоке «Действия» и подтвердить действие в появившемся диалогом окне (рис. 367).

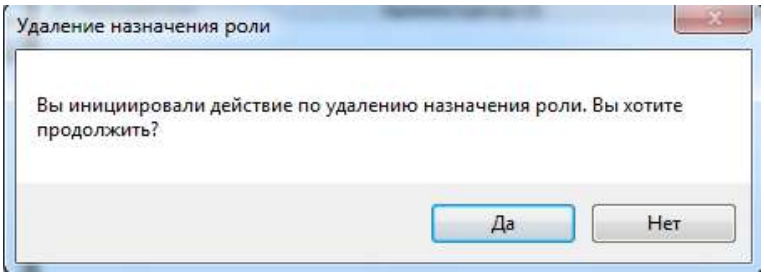


Рис. 367. Удаление назначения роли для учетной записи или группы

После внесения всех необходимых изменений в таблицу следует выполнить сохранение путем нажатия кнопки «Сохранить» в блоке «Действия».

19.10 Клиенты Windows

Для управления Windows клиентами необходимо в списке клиентов ДБ выбрать вкладку «Windows» (рис. 368).

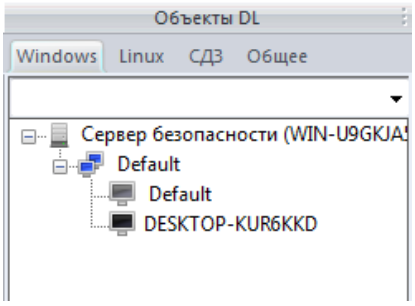


Рис. 368. Windows клиенты

19.10.1 Ввод клиента в ДБ

Для ввода компьютера в ДБ должен быть соблюден ряд условий:

1. В ЛВС должен быть работающий СБ.
2. Между клиентом и СБ должен быть свободный обмен пакетами по TCP/IP портам 17490, 17491, 17492.
3. Должна правильно выполняться операция преобразования имени компьютера в его IP-адрес.

Ввести компьютер в ДБ можно либо в процессе установки СЗИ Dallas Lock 8.0, либо, когда СЗИ Dallas Lock 8.0 уже установлено.

Ввод клиента в ДБ в процессе установки Dallas Lock 8.0

В процессе установки Dallas Lock 8.0 в окне ввода параметров присутствуют поля для ввода компьютера в ДБ на данном этапе (рис. 369).

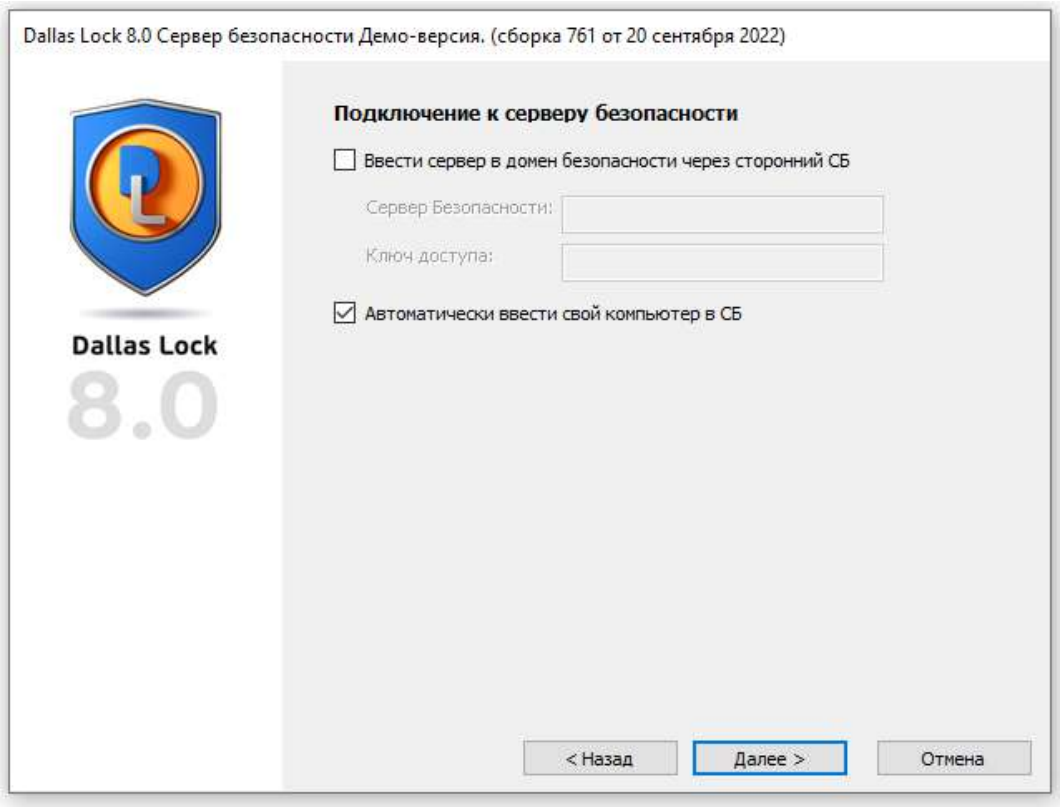


Рис. 369. Параметры установки системы защиты

Необходимо поставить флаг «Ввести сервер в домен безопасности через сторонний СБ». В соответствующие поля необходимо ввести имя СБ и его ключ доступа и нажать кнопку «Далее». Если имя СБ введено неверно, то появится сообщение «Указанное имя не найдено в сети или не установлен Dallas Lock». Если такой компьютер в сети есть, но на нем не установлен СБ, то появится сообщение «Удаленная машина найдена. Но она отклоняет подключение по данному порту». Если указан неправильный ключ доступа к СБ, то появится сообщение «Неправильный код доступа Сервера безопасности». Если же все указано правильно, появится сообщение «Машина успешно введена в домен безопасности».

Примечание. Ключ доступа СБ нужен для ввода компьютеров в ДБ в процессе активации СЗИ. По умолчанию ключ доступа СБ имеет пустое значение. Его можно изменить через дополнительное меню в КСБ (см. «Ключ доступа СБ»). Значение ключа доступа к СБ подчиняется установленным политикам сложности паролей.

Затем необходимо оставить или убрать флаг в поле «Автоматически ввести свой компьютер в СБ», нажать кнопку «Далее» и установка продолжится.

Ввод защищенного компьютера в ДБ

Ввод в ДБ через оболочку администратора

Для ввода клиента в ДБ через оболочку администратора необходимо:

1. Убедиться, что СБ доступен по сети.
2. Запустить оболочку администратора Dallas Lock 8.0 на клиенте.
3. Открыть категорию «Параметры безопасности» → «Вход». Выбрать параметр «Домен безопасности» и нажать действие «Свойства». Откроется окно «Настройки домена безопасности» (рис. 370).

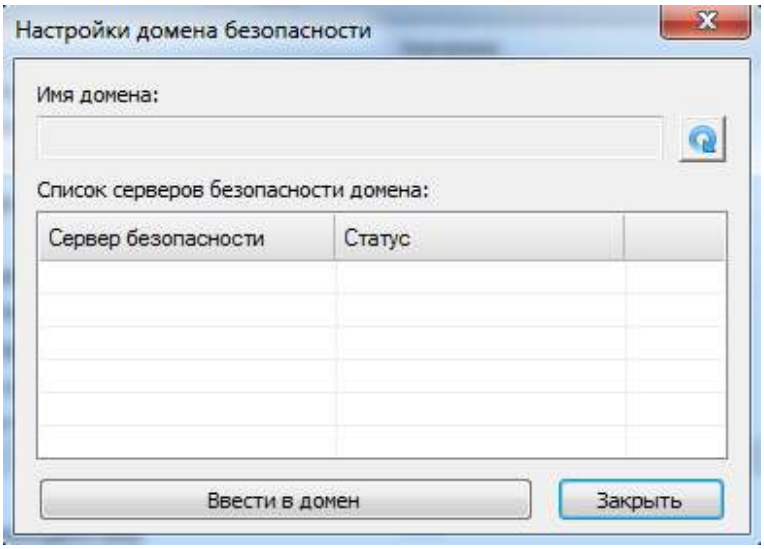


Рис. 370. Настройки ДБ

4. Выбрать СБ из списка или нажать кнопку «Ввести в домен». Откроется окно ввода клиента в ДБ где необходимо ввести (рис. 371):
   - имя компьютера, на котором установлен СБ;
   - ключ доступа, зарегистрированный на СБ (по умолчанию ключ доступа имеет пустое значение).

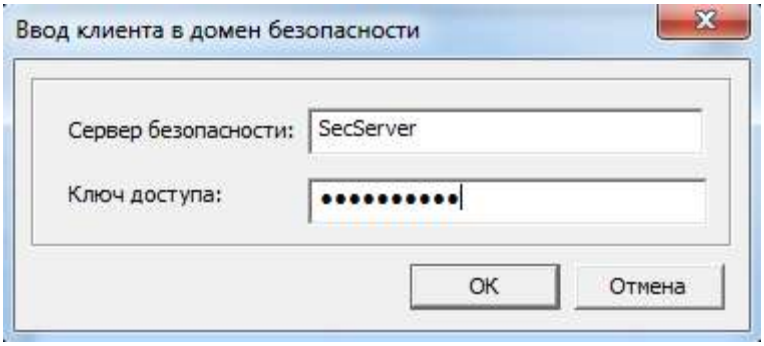


Рис. 371. Ввод компьютера в ДБ

Далее необходимо нажать «ОК», и, в случае успеха, через некоторое время появится сообщение о том, что клиент успешно введен в ДБ.

5. Перезагрузить ПК для подключения и синхронизации клиента с СБ.

   В дереве списка клиентов СБ в группе Default появится новый значок объекта с именем компьютера.

Ввод в ДБ с КСБ

Для ввода одного клиента Dallas Lock 8.0 в ДБ с помощью КСБ необходимо:

1. Убедиться, что целевой клиент включен и доступен по сети для СБ.
2. Открыть вкладку «Состояние» на уровне СБ и на панели «Действия с доменом» нажать кнопку «Включить клиента в домен безопасности…».
3. В появившемся диалоговом окне «Ввод клиента в домен безопасности» необходимо указать имя ПК, на котором установлен клиент СЗИ, и учетные данные администратора данного клиента. Если клиент не введен в AD, соответствующее поле остается пустым (рис. 372). Нажать кнопку «ОК».

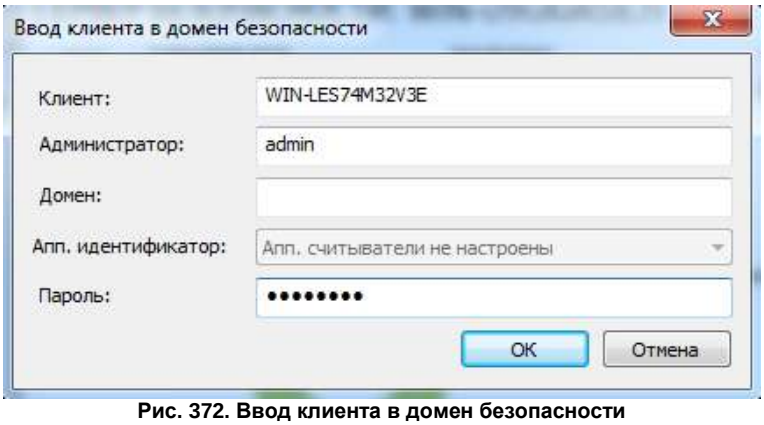


Рис. 372. Ввод клиента в домен безопасности

4. Если все данные введены корректно и клиент доступен по сети, появится информационное сообщение о том, что клиент успешно добавлен в домен безопасности.

Для ввода нескольких клиентов Dallas Lock 8.0 в ДБ с помощью КСБ необходимо:

1. Убедиться, что целевые клиенты включены и доступны по сети для СБ.
2. Открыть вкладку «Состояние» на уровне СБ и на панели «Действия с доменом» нажать кнопку «Включить клиентов в домен безопасности…».
3. С помощью открывшегося окна мастера установки/обновления СЗИ клиентов сервера безопасности добавить клиентов для удаленных операций. Для этого доступны следующие операции:

— добавить имя или IP-адрес клиента;

— удалить имя или IP-адрес клиента;

— добавить список клиентов из файла;

— сохранить список клиентов в файл;

— сканировать сеть;

— удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 373). Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном диапазоне возможно выводить адреса в числовом виде и проверять установленные версии Dallas Lock.

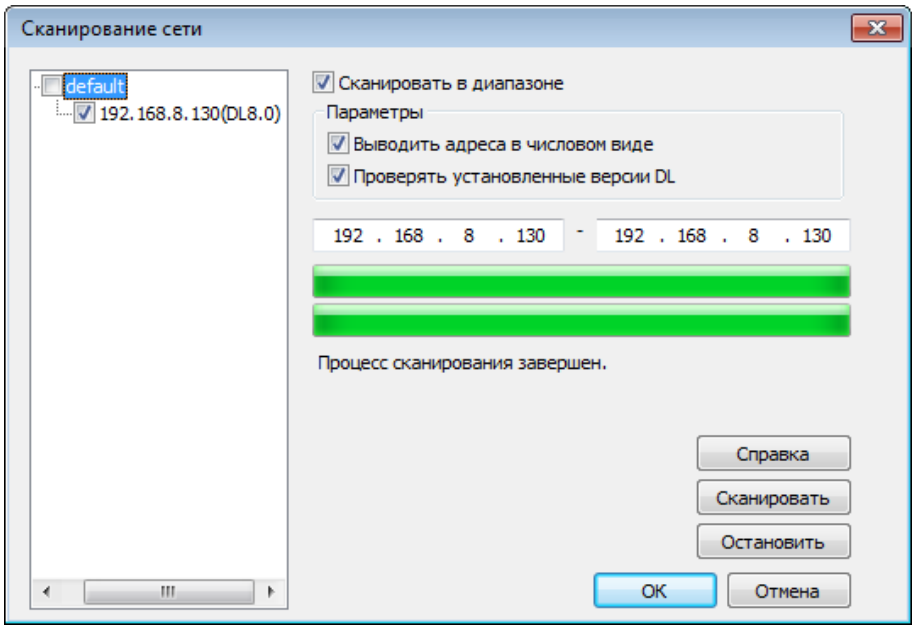


Рис. 373. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить»;

4. Ввести логин и пароль суперадминистратора Dallas Lock 8.0 на целевых клиентах. Для продолжения установки нажать кнопку «Продолжить».
5. Клиенты из списка будут введены в ДБ, сообщения об успешной операции появятся в списке (рис. 374).

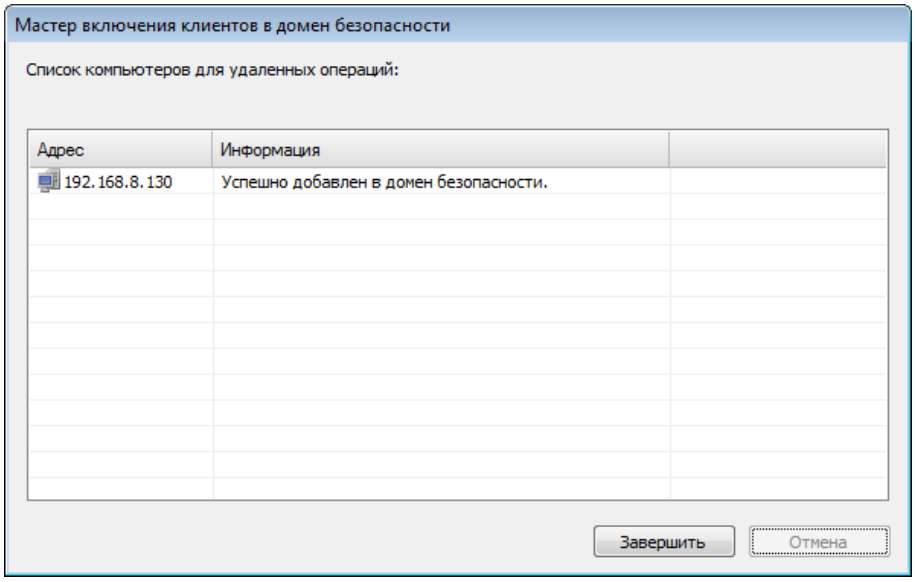


Рис. 374. Добавление клиента в ДБ

В дереве объектов КСБ появятся значки новых клиентов ДБ. На клиентах, введенных в ДБ, после запуска оболочки администратора в параметрах безопасности значение параметра «Сервер безопасности» изменится с «не задан» на имя сервера.

Примечание. В процессе ввода компьютеров в ДБ пароли локальных пользователей с одинаковыми логинами (именами) не синхронизируются. Если на СБ создана такая же учетная запись и включена для работы на клиентах, то после синхронизации клиентов с СБ пароль данной учетной записи на разных клиентах поменяется на тот, который указан на СБ. Но после смены пароля данной учетной записи на любом из клиентов (самим пользователем или администратором Dallas Lock 8.0) при следующей синхронизации на всех ПК с данным пользователем, пароль изменится на тот, который был изменен на одном из клиентов.

19.10.2 Вывод клиента из ДБ

Для вывода клиента через КСБ необходимо выбрать клиента в дереве объектов КСБ и на вкладке «Состояние» нажать кнопку «Удалить из ДБ» или выбрать соответствующую кнопку из контекстного меню, нажав правой кнопкой мыши на клиента (рис. 375).

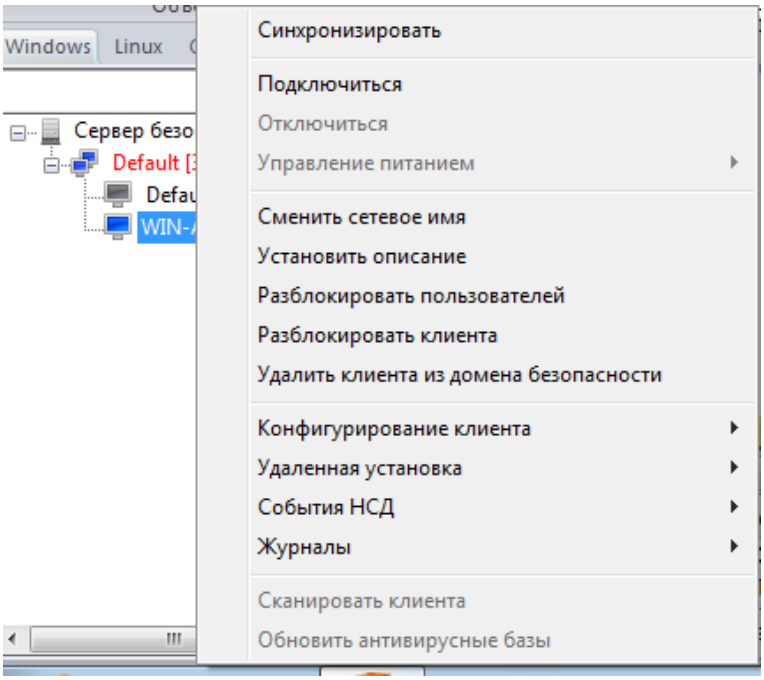


Рис. 375. Удаление клиента из ДБ в КСБ

Для вывода клиента из ДБ через оболочку администратора необходимо:

1. Запустить оболочку администратора Dallas Lock 8.0 на клиенте.
2. Открыть категорию «Параметры безопасности» → «Вход». Выбрать параметр «Домен безопасности» и нажать действие «Свойства». Откроется окно «Настройки домена безопасности» (рис. 376).

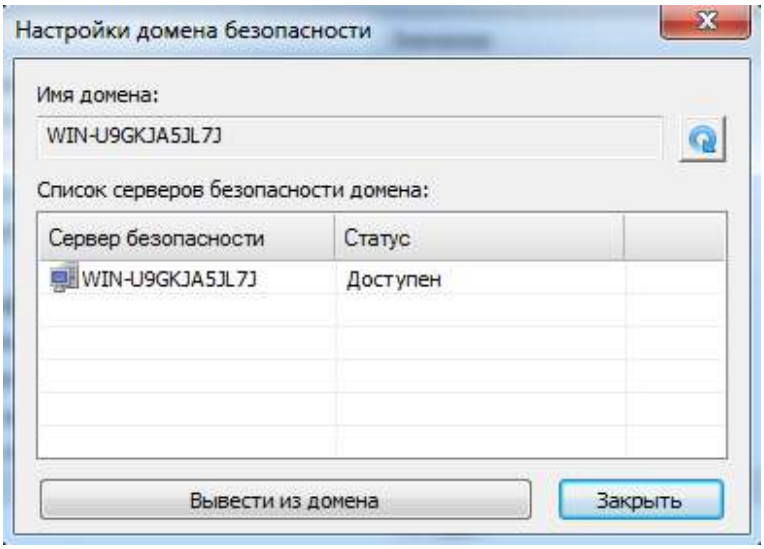


Рис. 376. Настройки ДБ

3. Выбрать СБ из списка или нажать кнопку «Вывести из домена». Откроется окно вывода клиента из ДБ где необходимо ввести (рис. 377):
   - имя компьютера, на котором установлен СБ;
   - ключ доступа, зарегистрированный на СБ (по умолчанию ключ доступа имеет пустое значение).

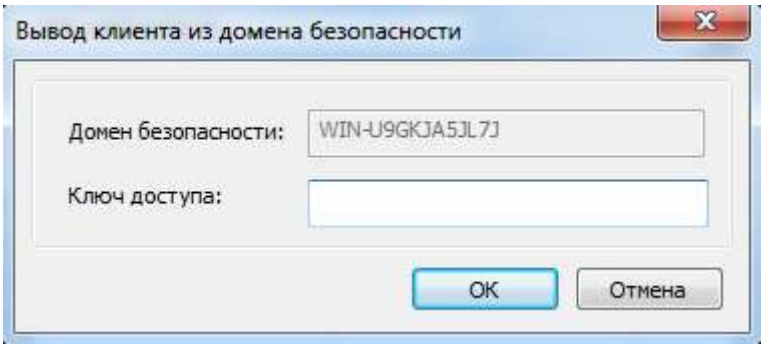


Рис. 377. Вывод клиента из ДБ

Далее необходимо нажать «ОК» и, в случае успеха, через некоторое время появится сообщение о том, что клиент успешно выведен из ДБ.

19.10.3 Централизованная установка Dallas Lock 8.0

Существует возможность выполнить установку или удаление Dallas Lock 8.0 на один или несколько компьютеров, расположенных в одной ЛВС, централизованно, без предварительной подготовки целевых компьютеров.

Централизованная установка Dallas Lock 8.0 средствами СБ

Для централизованной установки необходимо знать пароль администратора ОС ЗАРМ на целевых компьютерах, который в дальнейшем станет паролем суперадминистратора ЗАРМ Dallas Lock 8.0 в случае, когда параметрами установки не определено создание иной учетной записи, выступающей в роли суперадминистратора ЗАРМ Dallas Lock 8.0.

Внимание! На текущий момент не допускается наличие пробела в имени администратора ОС, под которым выполняется установка.

Внимание! На текущий момент на клиенте СЗИ НСД Dallas Lock не поддерживаются полные имена домена — не допускается наличие точки в имени домена. При наличии точки в имени домена мастер установки не сможет продолжить работу.

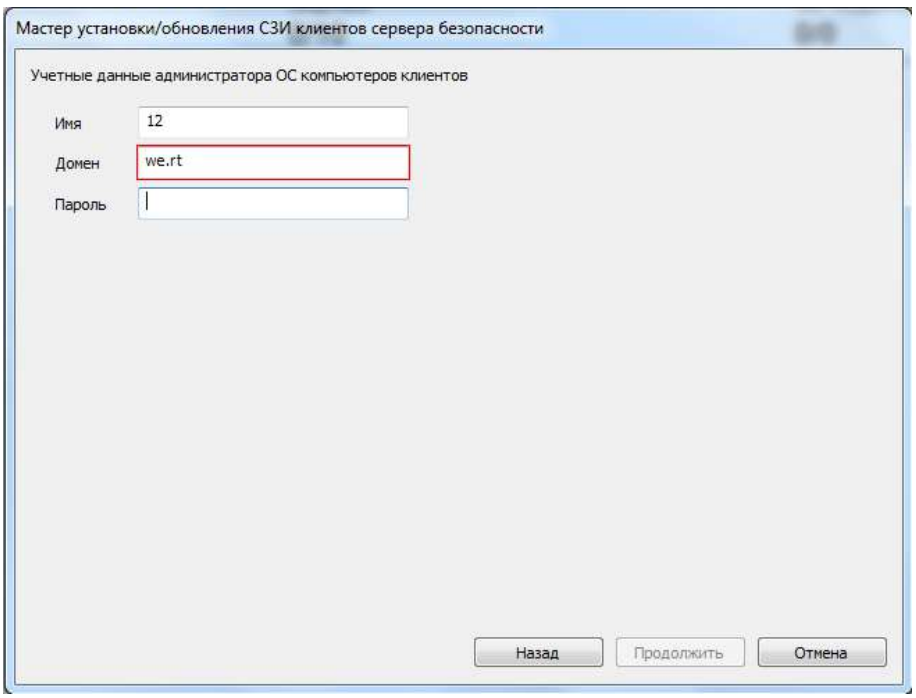


Рис. 378. Недопустимое имя домена

Централизованная установка возможна в следующих вариантах:

1. Для группы компьютеров, входящих в один домен AD. Имя администратора ОС ЗАРМ и пароль будут одинаковыми, и, соответственно, будет возможна групповая централизованная установка системы защиты.
2. Для компьютеров, не входящих в домен AD, следует использовать имя и пароль администратора локальной ОС ЗАРМ и выполнять централизованную установку для группы компьютеров, имеющих одинаковые пароли администратора ОС ЗАРМ.
3. Для компьютеров, имеющих индивидуальные имя и пароль администратора ОС ЗАРМ, централизованную установку следует выполнять отдельно от других.

Необходимо выполнение следующих требований перед проведением централизованной установки:

1. Настройки межсетевого экрана должны разрешать подключение СБ к целевым компьютерам по протоколу «общий доступ к файлам и принтерам» Windows. Это достигается отключением штатного/внешнего межсетевого экрана, либо разрешением соответствующего исключения в его настройках.
2. На целевом компьютере должен быть отключен пункт «Использовать простой общий доступ к файлам». В Windows 7 данная настройка задается через «Панель управления» → «Оформление и персонализация» → «Параметры папок» → «Вид» → отключить пункт «Использовать мастер общего доступа (рекомендуется)» → «Применить» → «Ок».
3. При наличии модуля СОВ на СБ, на время централизованной установки рекомендуется выставить настройки уровней тревожности детекторов сетевых атак в значения по умолчанию или временно отключить модуль СОВ на СБ.

Требования 1-2 можно выполнить централизованно средствами групповой политики Windows, если целевые компьютеры входят в домен AD.

Примечание. По умолчанию в операционных системах начиная с Windows 7 доступ к удаленному компьютеру под локальной учетной записью запрещен. Подробную информацию об этом ограничении можно найти на официальном сайте Справки и поддержки компании Microsoft по адресу https://support.microsoft.com/kb/951016 (на английском языке).

Для разрешения удаленного подключения под локальной учетной записью необходимо в редакторе реестра по пути HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System создать ключ типа dword с именем LocalAccountTokenFilterPolicy со значением «1» («LocalAccountTokenFilterPolicy»=dword:00000001) и перезагрузить компьютер. В крупных сетях с AD данное значение можно распространить через политики.

Для централизованной установки Dallas Lock 8.0, необходимо выполнить следующие шаги:

1. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена КСБ, дистрибутив Dallas Lock 8.0.
2. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Установить/Обновить СЗИ клиентов…».
3. Добавить клиентов для удаленных операций. Для этого доступны следующие операции:

— добавить имя или IP-адрес клиента;

— удалить имя или IP-адрес клиента;

— добавить список клиентов из файла;

— сохранить список клиентов в файл;

— сканировать сеть;

— удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 379). Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном диапазоне возможно выводить адреса в числовом виде и проверять установленные версии Dallas Lock.

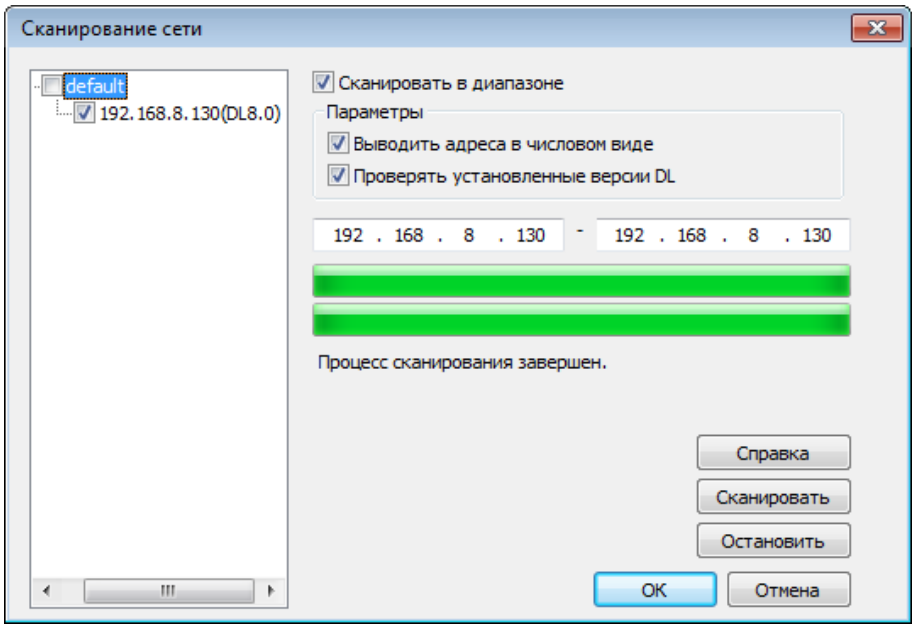


Рис. 379. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить».

4. Ввести логин и пароль будущего суперадминистратора Dallas Lock 8.0 на целевых клиентах. Для продолжения установки нажать кнопку «Продолжить».
5. Есть возможность принудительно создать учетную запись пользователя (рис. 380), которая будет выступать в роли суперадминистратора после установки (обновления) Dallas Lock 8.0. Для этого необходимо поставить флаг «Создать нового пользователя в качестве АИБ», далее указать логин и пароль для учетной записи.

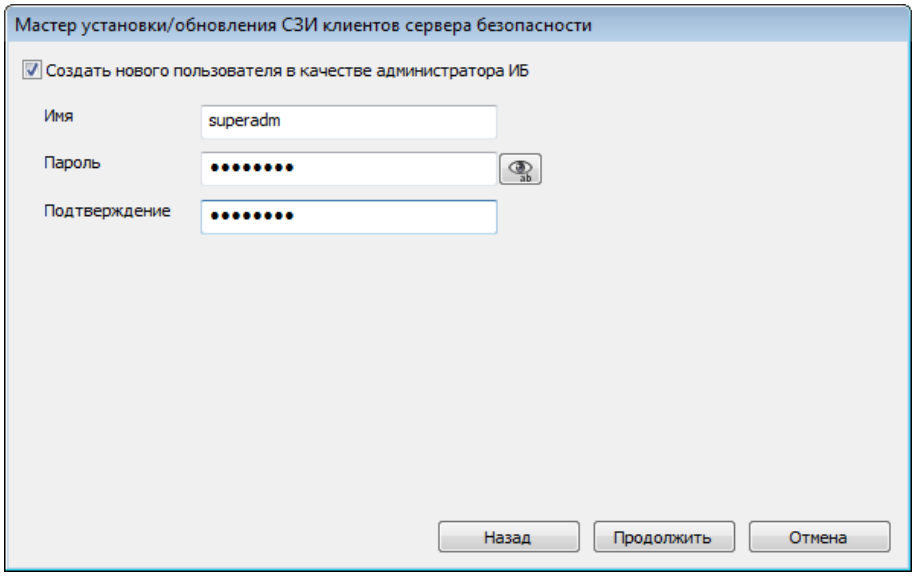


Рис. 380. Окно создания администратора ИБ

Для продолжения установки нажать кнопку «Продолжить».

6. Заполнить параметры установки, которые будут применены к клиентам в процессе активации Dallas Lock 8.0 (рис. 381):
   - Номер лицензии и код технической поддержки, которые указаны на обложке футляра.
   - Путь к дистрибутиву Dallas Lock 8.0.
   - Поставленный флаг «Сохранять настройки от предыдущей установки» позволит сохранять и устанавливать существующую конфигурацию клиента. Если поле не отметить, применится файл конфигурации «По умолчанию», что имеет смысл только при обновлении.
   - Имя и ключ доступа СБ (по умолчанию ключ имеет пустое значение).
   - Поставленный флаг «Перезагрузить удаленный компьютер после установки» позволяет автоматически перезагрузить клиент после завершения установки, иначе клиент должен быть перезагружен пользователем самостоятельно.

- Время до перезагрузки удаленного компьютера после установки/обновления СЗИ в минутах.
- Произвольное сообщение и интервал, через который оно будет повторяться, для пользователей, на чьих компьютерах производится установка/удаление СЗИ.

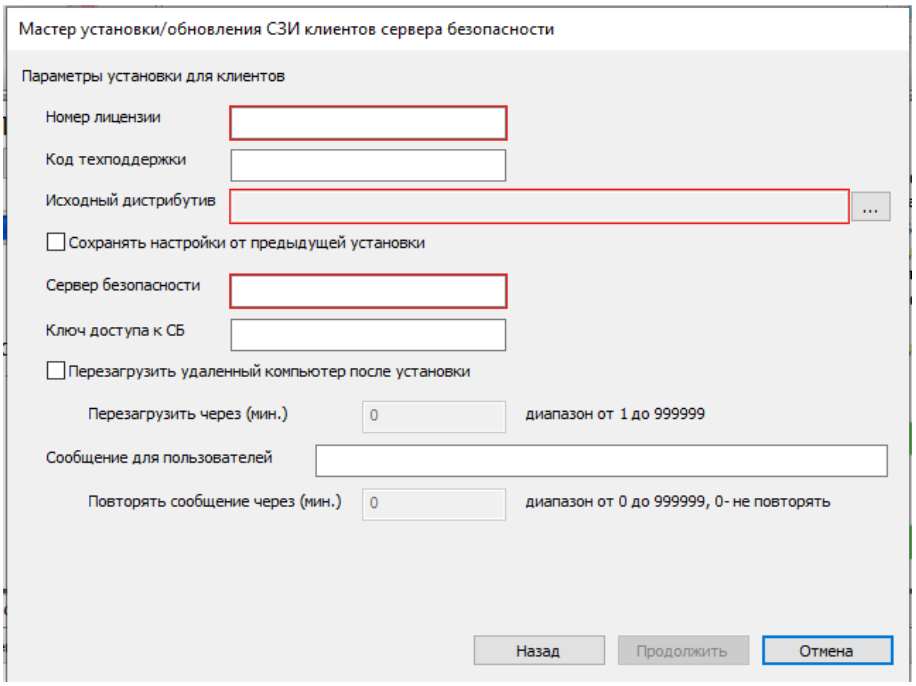


Рис. 381. Поля параметров для централизованной установки

Для продолжения установки нажать кнопку «Продолжить».

7. Далее можно просматривать состояние процесса установки для каждого клиента. Здесь же после централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции (рис. 382).

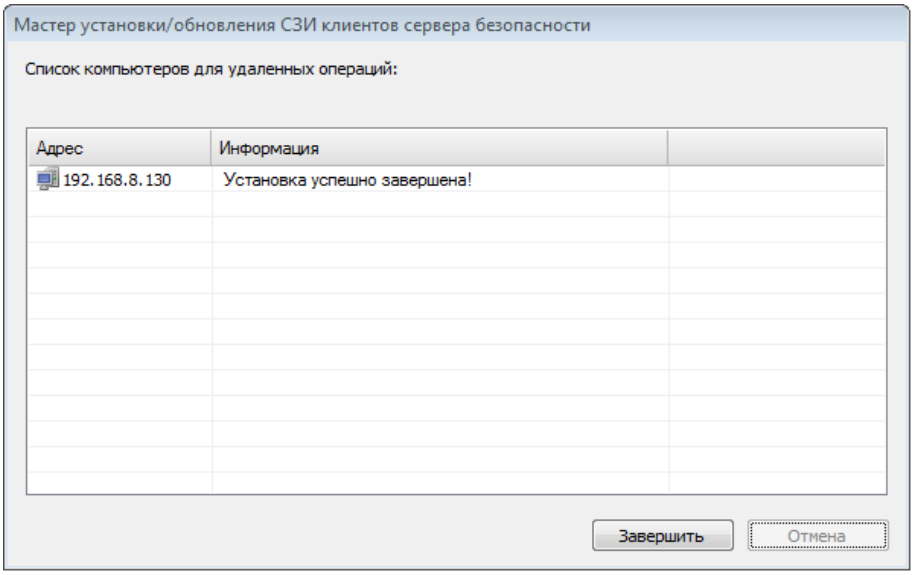


Рис. 382. Информация о ходе централизованной установки средствами СБ

При выборе поля с комментарием в отдельном диалоге откроется список с историей событий в результате операции (рис. 383).

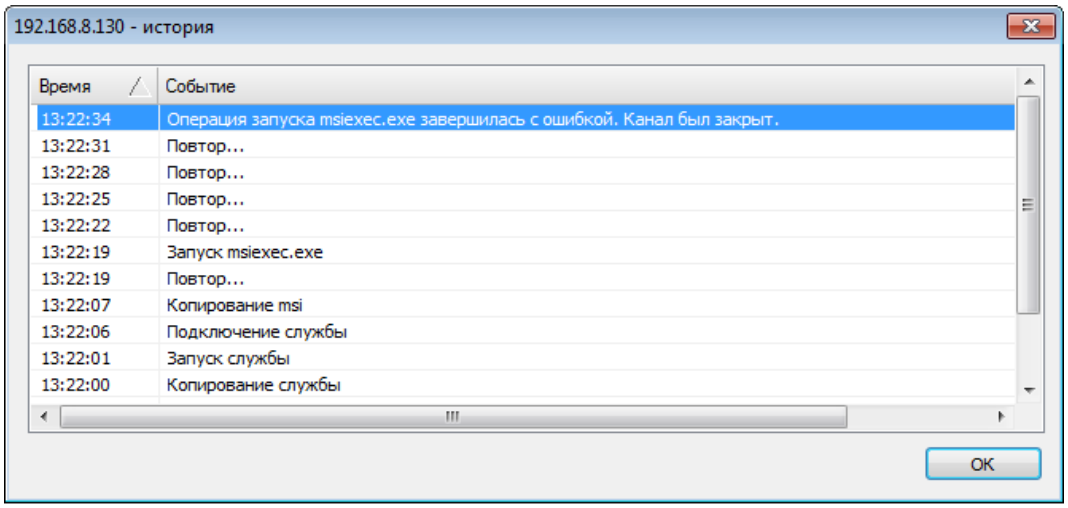


Рис. 383. Список событий в ходе централизованной установки

После удачного завершения установки Dallas Lock 8.0 на выбранных клиентах появится подтверждающее сообщение, а в дереве объектов КСБ появится значок клиента.

Ошибка при централизованной установке

Если во время централизованной установки операция завершилась ошибкой (рис. 384), то возможной ее причиной может быть отключение важного параметра в ОС компьютера с СБ.

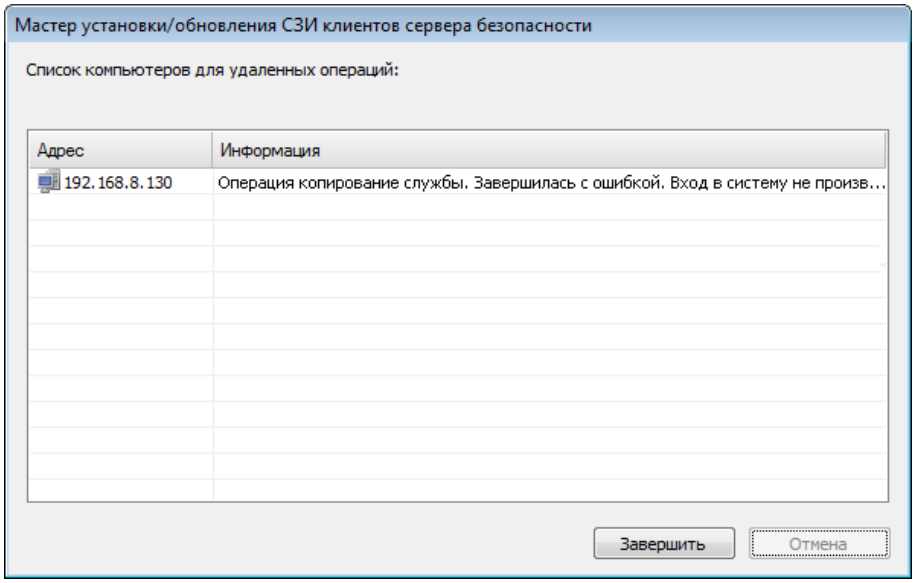


Рис. 384. Ошибка при централизованной установке

Условием централизованной установки является значение параметра локальной политики ОС «Сетевая безопасность: уровень проверки подлинности LAN Manager» → «Отправлять LM и NTLM → использовать сеансовую безопасность» (рис. 385).

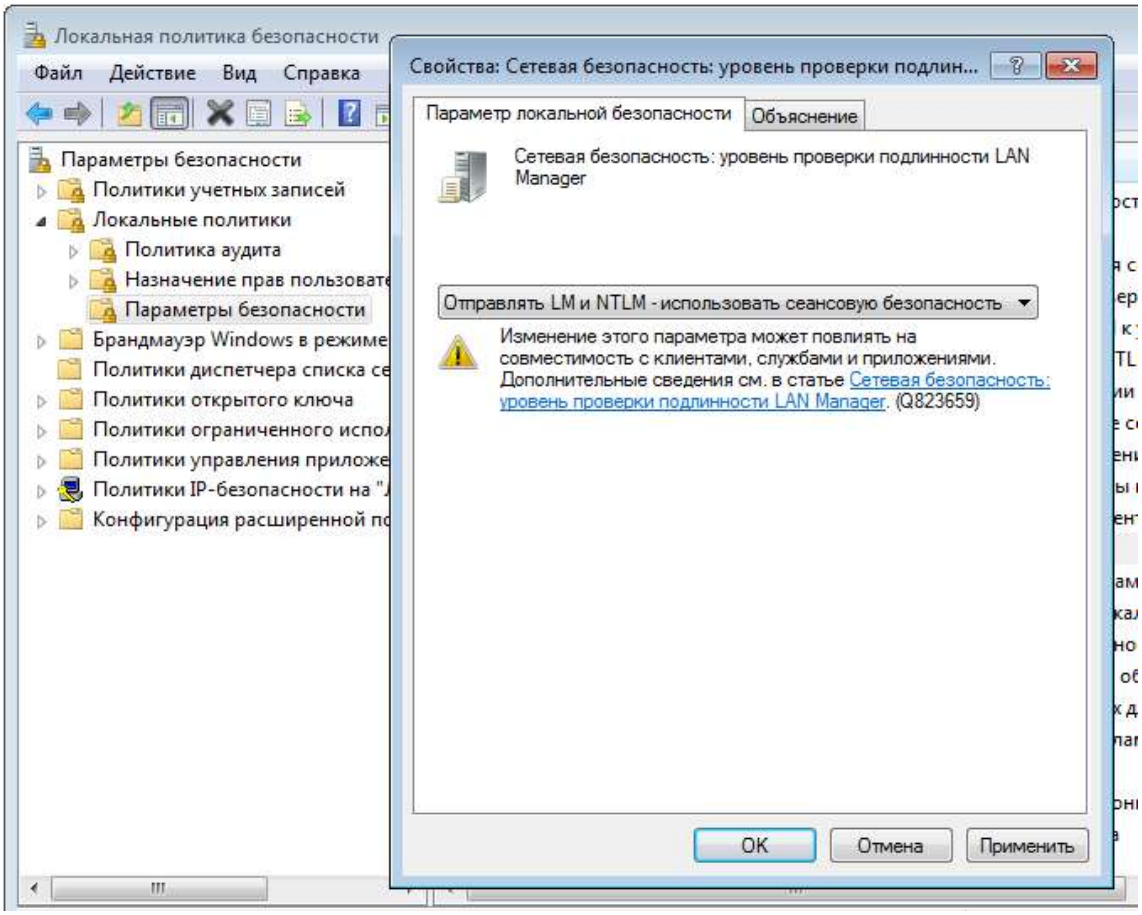


Рис. 385. Локальные политики безопасности для централизованной установки DL

Обновление версий Dallas Lock 8.0 средствами СБ

Средствами Dallas Lock возможно обновление оригинальных версий «8.0» до актуальных «8.0», прошедших испытания с привлечением испытательной лаборатории, а также предыдущих версий «7.5» и «7.7» до версии «8.0» последней актуальной сборки.

Перед обновлением системы защиты средствами СБ следует заранее обновить СЗИ Dallas Lock 8.0 на СБ и версию самого СБ:

1. Для того, чтобы выполнить обновление СЗИ Dallas Lock 8.0, необходимо запустить файл обновленного дистрибутива с указанием файла конфигурации. Так как процесс обновления автоматически сохраняет и применяет конфигурацию уже установленной версии, то путь к файлу можно оставить без изменений.

   Примечание. Обновление Dallas Lock 8.0 на СБ можно произвести под учетной записью, для которой выполняются следующие условия:

   1) Учетная запись, из-под которой производится обновление, должна быть в группе Администраторы ОС СБ.
   2) Учетная запись, из-под которой производится обновление, должна иметь права на удаление Dallas Lock. Это настраивается в правах пользователей, оболочки администратора Dallas Lock 8.0, параметр «Деактивация системы защиты». В значение данного параметра прописывается учетная запись, имеющая право на удаление системы защиты (по умолчанию это суперадминистратор СБ Dallas Lock).

2. Обновление СБ необходимо произвести путем удаления предыдущей версии и установки новой штатными средствами (с помощью мастера установок Windows). При этом необходимо заранее сохранить файл конфигурации СБ и применить его в последующем. Системную папку с оставшимися файлами «C:\DLLOCK80\DlSecServer» необходимо удалить.

В дереве объектов КСБ клиенты, на которых установлена версия Dallas Lock 8.0, отличная от версии на самом СБ, будут отмечены особым образом . Для таких клиентов недоступно ОУ и не работает синхронизация, но имеется возможность обновления версии Dallas Lock 8.0 с помощью СБ.

Для централизованного обновления Dallas Lock 8.0 необходимо нажать на кнопку

«Установить/Обновить СЗИ клиентов…» расположенную на вкладке «Состояние» СБ.

Ряд предварительных настроек и порядок действий для централизованного обновления, аналогичны тем, что и в процессе централизованной установки (см. «Централизованная установка Dallas Lock 8.0 средствами СБ»).

Примечание. При обновлении с версии Dallas Lock 7.7 выбрать клиентов для обновления можно, присоединив список из сохраненного файла «ClientList.txt», сформированного на СБ Dallas Lock 7.7.

Примечание. В процессе разработки Dallas Lock 8.0 идеология и архитектура системы защиты были значительно переработаны. Были оптимизированы параметры политик безопасности и права доступа, поэтому при обновлении СЗИ версий Dallas Lock 7.7 и 7.5 до версии Dallas Lock 8.0, необходимо учесть следующее:

1. Параметры, которые появились только в Dallas Lock 8.0, при обновлении остаются в значениях по умолчанию (как при установке).
2. Параметры, которые исчезли в Dallas Lock 8.0, перестают учитываться.
3. Значение параметра «Аудит: просмотр» берется из значения параметра «Аудит: просмотр журналов входов».
4. Значение параметра «Учетные записи: управление» берется из значения параметра «Учетные записи: создание».
5. Имена мандатных уровней используются только для первых 8-ми, остальные не используются (только для Dallas Lock 8.0 редакции «С»).
6. Права доступа, которые исчезли в Dallas Lock 8.0, перестают учитываться.
7. Значение права доступа «Запись разрешений» берется из значения права «Изменение разрешений».
8. Значения права доступа «Изменение содержимого» берется из значения права «Запись данных».

Централизованное обновление также возможно средствами групповых политик контроллера домена, аналогично установке (см. «Централизованная установка Dallas Lock 8.0 средствами Active Directory»).

Централизованная установка Dallas Lock 8.0 средствами Active Directory

Средствами Microsoft Windows возможна централизованная установка Dallas Lock 8.0 на рабочие станции, входящие в состав Контроллера домена. Необходимые для установки действия включают в себя:

1. Формирование файла установки на СБ.
2. Создание точки распространения на Контроллере домена.
3. Создание объекта групповой политики для централизованной установки средствами AD.
4. Конфигурация и применение групповой политики.

Процесс создания групповой политики будет рассмотрен на примере **Windows Server 2008 R2**.

Подготовка msi-файла

Необходимо подготовить msi-файл для централизованной установки с контроллера домена при помощи СБ Dallas Lock 8.0. Для этого в КСБ необходимо выполнить следующие шаги:

1. Перед удаленной установкой необходимо разместить на компьютере, на котором запущена КСБ, дистрибутив Dallas Lock 8.0.
2. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Подготовить дистрибутив для AD…».

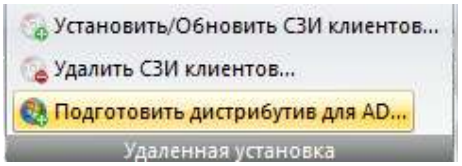


Рис. 386. Подготовить дистрибутив для AD

3. Ввести логин и пароль будущего суперадминистратора Dallas Lock 8.0 на целевых клиентах. Для продолжения подготовки нажать кнопку «Продолжить».

   Возможно принудительно создать учетную запись пользователя, которая будет выступать в роли суперадминистратора после установки (обновления) Dallas Lock 8.0. Для этого необходимо поставить флаг «Создать нового пользователя в качестве администратора ИБ», далее указать

логин и пароль для учетной записи. Для продолжения подготовки нажать кнопку «Продолжить».

4. Заполнить параметры удаленной установки, которые будут применены к клиентам в процессе активации Dallas Lock 8.0 (рис. 387):
   - Номер лицензии и код технической поддержки, которые указаны на обложке футляра;
   - Путь к дистрибутиву Dallas Lock 8.0.
   - Поставленный флаг «Сохранять настройки от предыдущей установки» позволит сохранять и устанавливать существующую конфигурацию клиента. Если поле не отметить, применится файл конфигурации «По умолчанию», что имеет смысл только при обновлении.
   - Имя и ключ доступа СБ (по умолчанию ключ имеет пустое значение).
   - Поставленный флаг «Перезагрузить удаленный компьютер после установки» позволяет автоматически перезагрузить клиент после завершения установки, иначе клиент должен быть перезагружен пользователем самостоятельно.
   - Время до перезагрузки удаленного компьютера после установки/обновления СЗИ в минутах.
   - Произвольное сообщение и интервал, через который оно будет повторяться, для пользователей, на чьих компьютерах производится установка/удаление СЗИ.

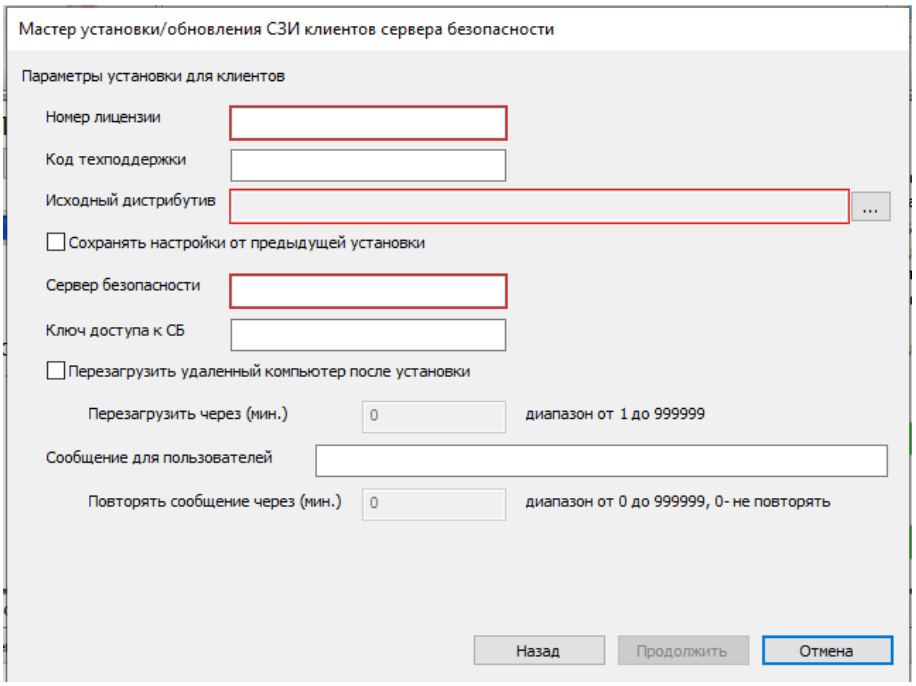


Рис. 387. Поля параметров для удаленной установки

Для продолжения подготовки нажать кнопку «Продолжить».

5. Появится окно с сообщением об успешном обновлении дистрибутива для установки средствами AD. Дистрибутив будет расположен по следующему пути: «C:\DLLOCK80\DlSecServer\DallasLock8.0C-AD.msi».

Этот пакет необходимо перенести на контроллер домена Windows Server, с которого будет происходить удаленная установка (см. ниже).

Далее необходимо приступить к настройкам непосредственно на контроллере домена в службах AD.

Создание объекта групповой политики

На контроллере домена необходимо создать объект групповой политики для развертывания Dallas Lock 8.0.

1. Для этого в службах AD необходимо открыть оснастку «Active Directory — пользователи и компьютеры». Далее найти или создать подразделение, которое будет содержать компьютеры, на которые требуется установить систему защиты (рис. 388, рис. 389).

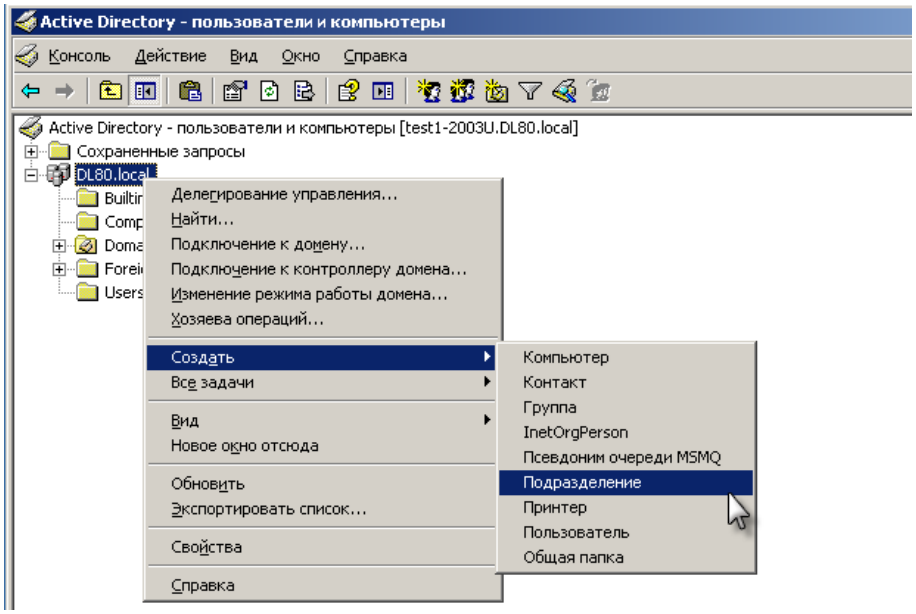


Рис. 388. Создание подразделения в AD

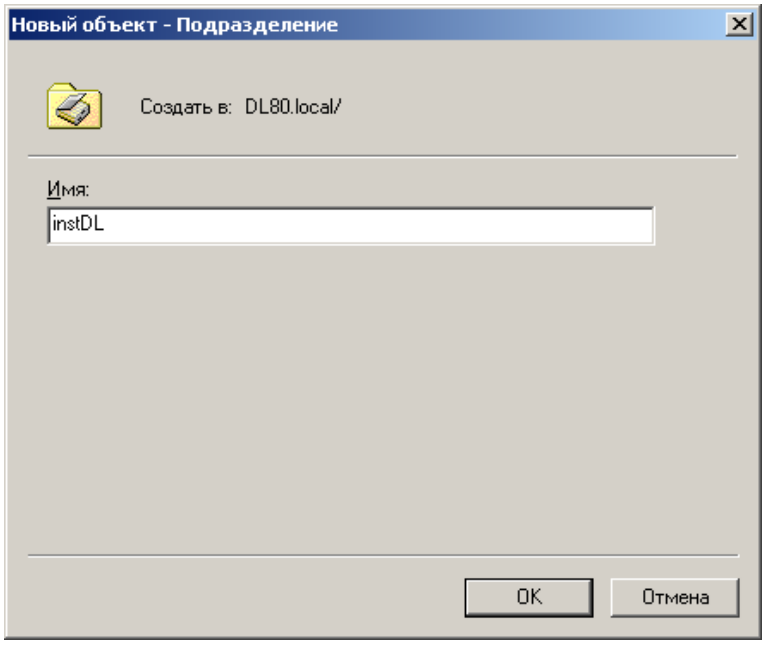


Рис. 389. Имя нового подразделения в AD

2. В это подразделение перенести необходимые компьютеры с помощью функции из контекстного меню «переместить» (рис. 390).

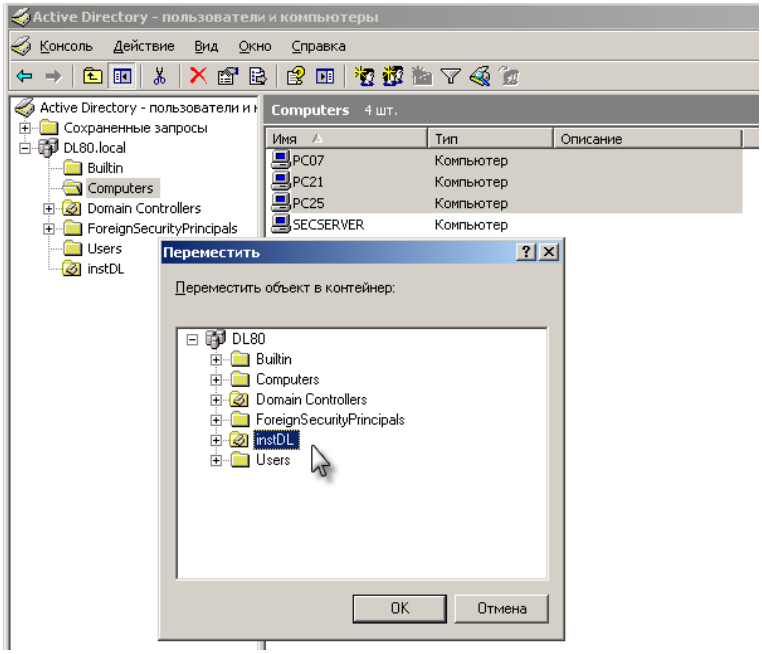


Рис. 390. Перенос рабочих станций в подразделение

В созданном подразделении появится список с необходимыми компьютерами.
Таким образом, создан объект групповой политики для развертывания ПО.

Внимание! Для корректной удаленной установки msi-файла Dallas Lock 8.0, подразделение следует создавать именно для компьютеров, а не для пользователей.

Создание групповой политики

Теперь для выбранного подразделения необходимо создать групповую политику, с помощью которой и будет происходить удаленная установка системы защиты.

Создание и редактирование групповых политик объектов AD в Windows Server управление групповыми политиками осуществляется из отдельной консоли.

Для создания групповой политики в Windows Server необходимо открыть оснастку (или консоль) «Управление групповой политикой». В дереве консоли необходимо развернуть узел необходимого домена и, выбрав созданное подразделение правой кнопкой мыши, нажать пункт меню «Создать объект GPO» (рис. 391).

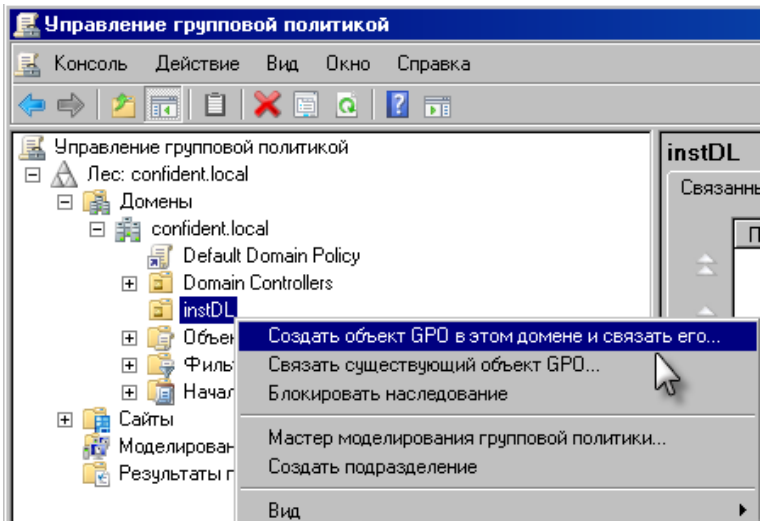


Рис. 391. Консоль управления групповой политикой на Windows Server

В появившемся окне необходимо ввести имя новой групповой политики. В поле с исходным объектом групповой политики ничего выбирать не следует. В списке объектов появится созданная групповая политика.

Таким образом создана групповая политика для подразделения компьютеров использующих Windows Server.

Создание источника установки

Теперь необходимо определить так называемый источник распространения пакета или установки сформированного msi-файла на сервере Windows. Это должна быть общая сетевая папка, к которой разрешен доступ следующим группам пользователей:

- администраторы,
- прошедшие проверку,
- пользователи домена.

Рекомендуется использовать в качестве точки распространения контейнер местонахождения самой групповой политики. Определить путь к папке со скриптами групповой политики можно различными способами.

1. Вначале необходимо определить уникальное имя групповой политики.

   В Windows Server определить уникальное имя (уникальный код) групповой политики можно через **консоль управления групповыми политиками**, выделив необходимую политику и открыв вкладку свойств «Таблица» (рис. 392).

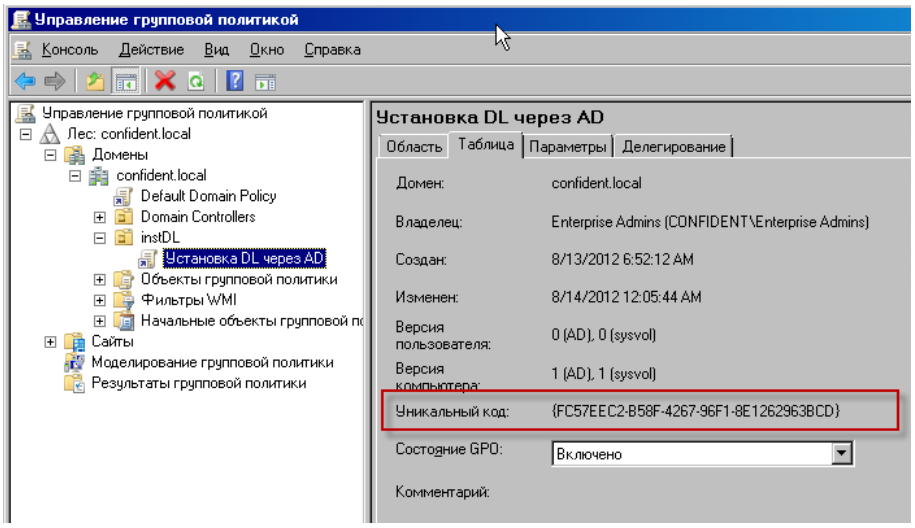


Рис. 392. Свойства политики в консоли управления групповой политикой

   Папки — контейнеры групповых политик располагаются в системной папке «SYSVOL». Эта папка является общей папкой в составе одного домена службы каталогов AD. Поэтому ее свойства соответствуют единой точки распространения.

2. Далее необходимо определить сетевую папку с созданной соответствующей групповой политикой для удаленной установки системы защиты (рис. 393).

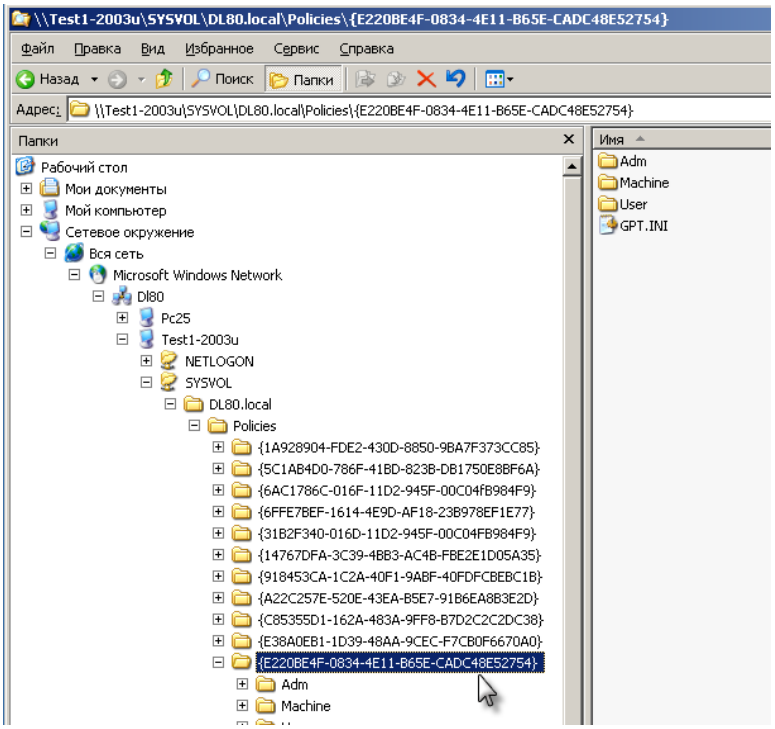


Рис. 393. Расположение папки-контейнера групповой политики

В папках групповых политик располагается каталог Adm, содержащий шаблоны *.ADM, используемые в объектах групповой политики, а также папки MACHINE и USER, включающие в себя файлы со специальными параметрами.

3. В папке MACHINE необходимо расположить созданный на СБ Dallas Lock 8.0 msi–файл (рис. 394).

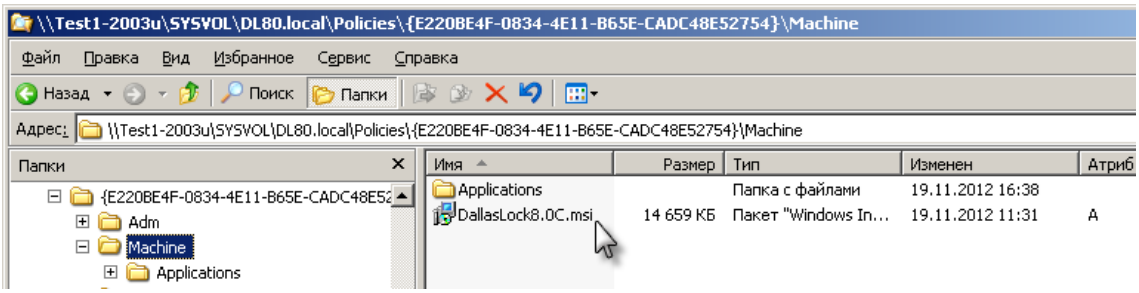


Рис. 394. Перенос msi-файла в папку групповой политики

Таким образом, был создан источник удаленной установки системы защиты Dallas Lock 8.0, который в контексте Microsoft имеет название «Точка распространения».

Настройка групповой политики

Теперь необходимо изменить созданный объект групповой политики для развертывания ПО.

1. В Windows Server редактор объектов групповой политики открывается в консоли управления групповыми политиками. Необходимо выбрать созданную политику правым щелчком мыши и нажать в появившемся контекстном меню «Изменить» (рис. 395).

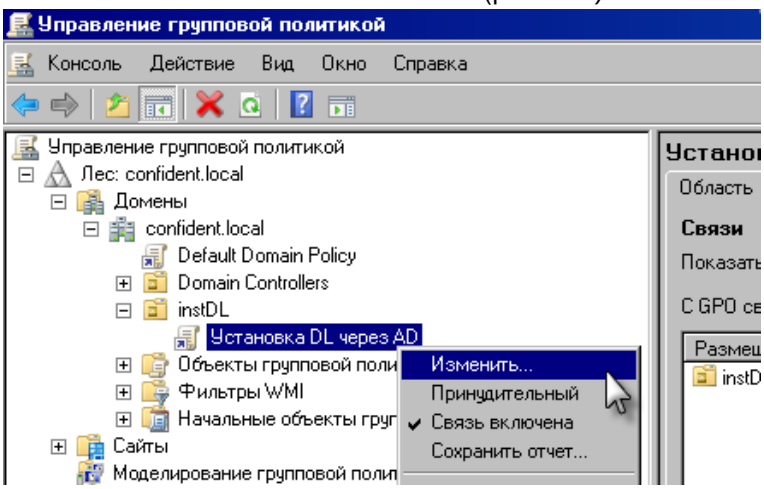


Рис. 395. Вызов контекстного меню в Консоли управления групповой политикой

Откроется необходимое окно редактора. В данном окне в дереве параметров требуется выбрать «Установка программ» (рис. 396).

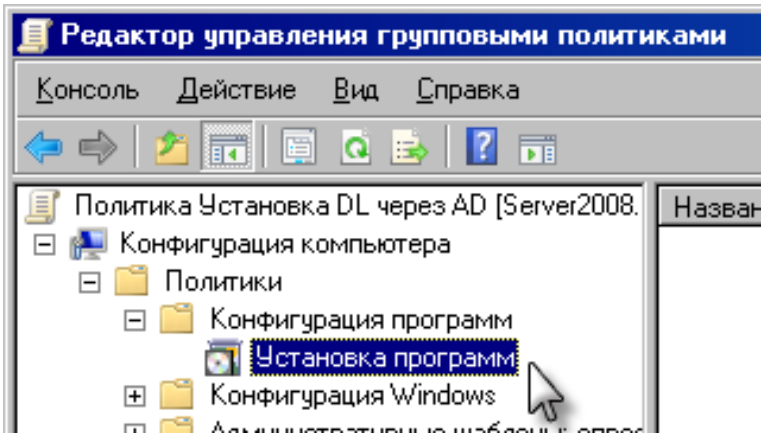


Рис. 396. Окно редактора групповой политики

2. Далее в правом поле окна установки программ с помощью контекстного меню создать пакет установки: нажать последовательно «Создать», «Пакет» (рис. 397).

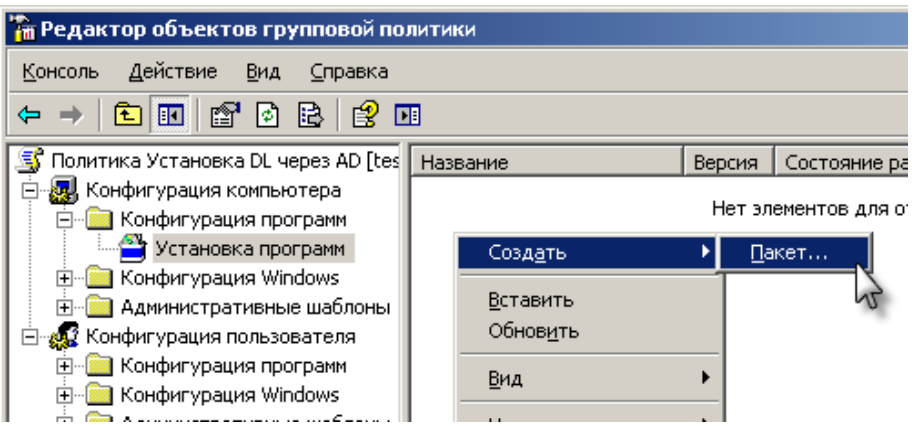


Рис. 397. Создание пакета конфигурации

3. С помощью проводника Windows добавить сетевой путь к распространяемому установочному пакету в общей папке (пакету установщика в точке распространения), который был расположен там ранее (рис. 398).

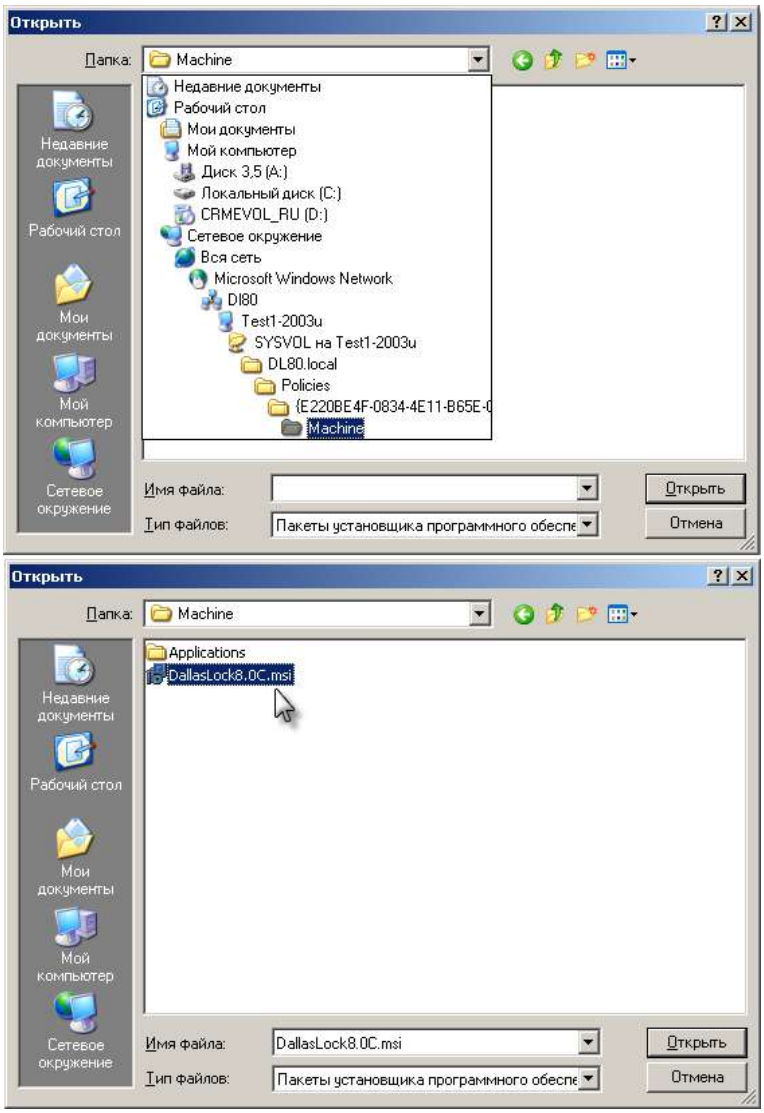


Рис. 398. Выбор расположения пакета установки

4. Выбрать msi-пакет и нажать кнопку «Открыть».
5. В диалоговом окне выбора параметра развертывания программ необходимо выбрать вариант «назначенный» и нажать «OK» (рис. 399).

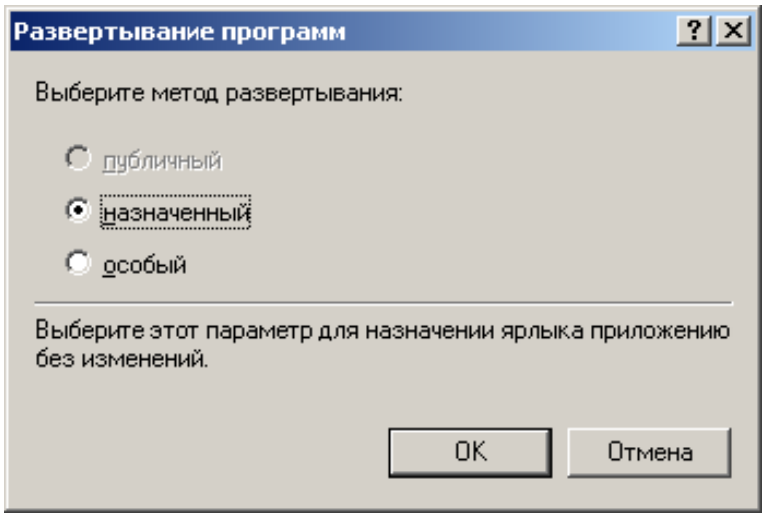


Рис. 399. Определение типа развертывания программы

Система развернет сформированный файл установки. Выбранный общий установочный пакет появится на правой панели редактора объектов групповой политики (рис. 400).

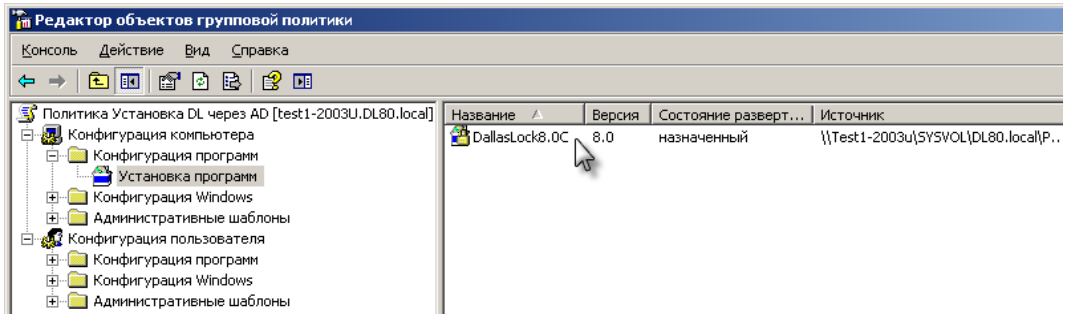


Рис. 400. Появление назначенного пакета установки в окне конфигурации

Таким образом, произведена конфигурация для групповой политики удаленной установки системы защиты Dallas Lock 8.0.

Теперь установочный пакет будет устанавливаться из общей сетевой папки на компьютеры, входящие в состав подразделения с назначенной групповой политикой, удаленно, при загрузке ОС. Установка будет происходить с двумя перезагрузками этих компьютеров. Первая необходима для применения назначенной политики. Вторая — как условие установки Dallas Lock 8.0 — принудительная перезагрузка.

После второй перезагрузки вход уже будет осуществляться на защищенный системой Dallas Lock 8.0 компьютер (см. «Вход на защищенный компьютер»).

Централизованное удаление Dallas Lock 8.0

Ряд предварительных настроек для централизованного удаления, аналогичны тем, что и в процессе централизованной установки (см. «Централизованная установка Dallas Lock 8.0 средствами СБ»).

Для централизованного удаления необходимо выполнить следующие шаги:

1. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Удалить СЗИ клиентов…».
2. Добавить клиентов для удаленных операций. Для этого доступны следующие операции:

— добавить имя или IP-адрес клиента;

— удалить имя или IP-адрес клиента;

— добавить список клиентов из файла;

— сохранить список клиентов в файл;

— сканировать сеть;

— удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 401). Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном

диапазоне возможно выводить адреса в числовом виде и проверять установленные версии Dallas Lock.

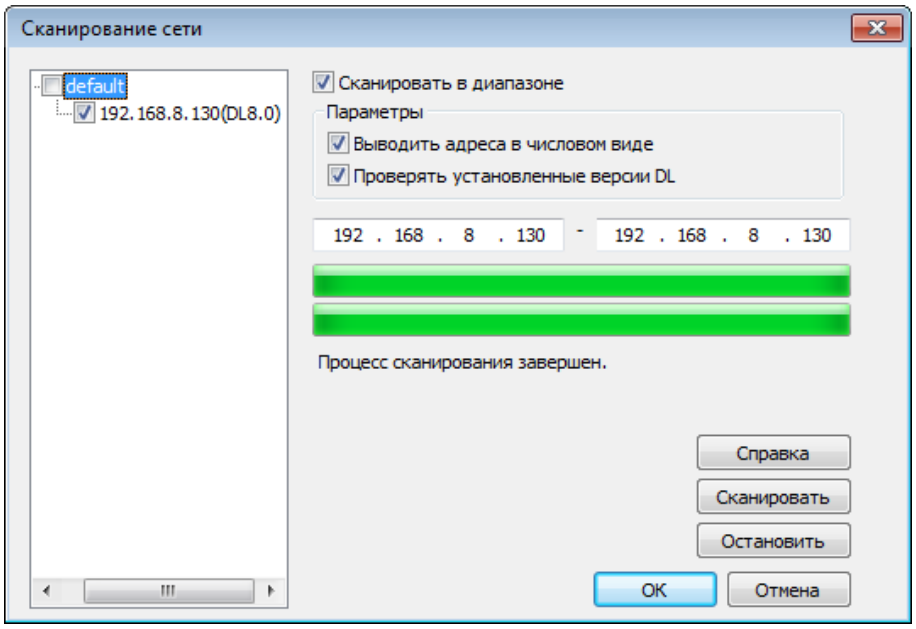


Рис. 401. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить».

3. Ввести логин и пароль суперадминистратора Dallas Lock 8.0 на целевых клиентах. Для продолжения удаления нажать кнопку «Продолжить».
4. Поставленный флаг «Перезагрузить» позволяет автоматически перезагрузить клиент после завершения удаления, иначе клиент должен быть перезагружен пользователем самостоятельно. Для продолжения удаления нажать кнопку «Продолжить».
5. Далее можно просматривать состояние процесса удаления для каждого клиента. Здесь же появятся соответствующие комментарии после удачного или не удачного завершения операции (рис. 402).

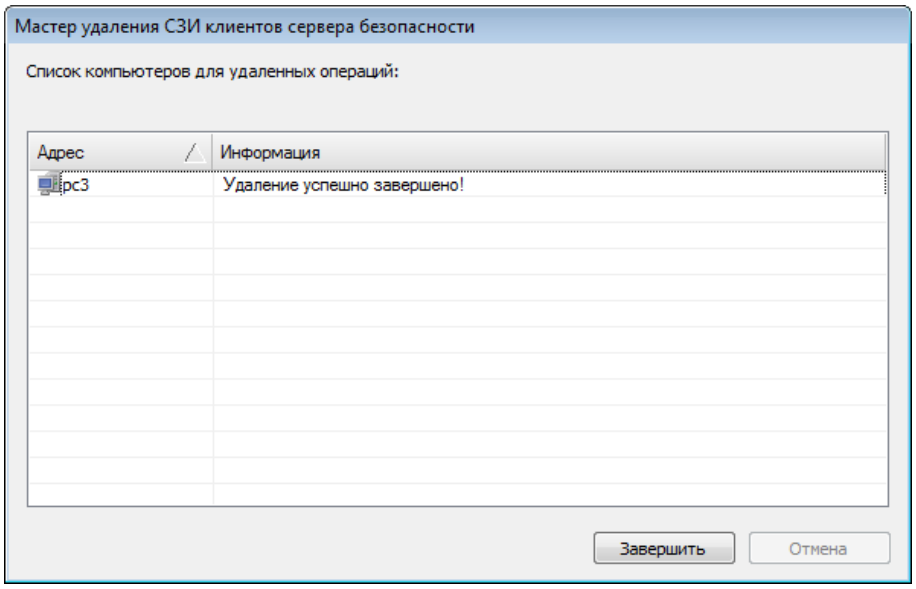


Рис. 402. Информация о ходе централизованного удаления

При выборе поля с комментарием в отдельном окне откроется список с историей событий в результате операции (рис. 403).

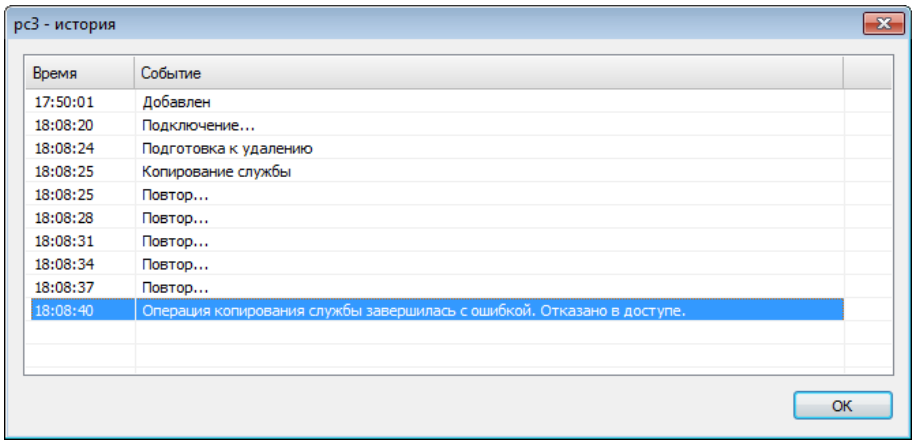


Рис. 403. Список событий в ходе централизованного удаления

После удачного завершения удаления Dallas Lock 8.0 на выбранных клиентах появится подтверждающее сообщение, а в дереве объектов КСБ удалится значок клиента.

19.10.4 Взаимодействие с Kaspersky Security Center

В случае совместного использования средств СЗИ НСД Dallas Lock 8.0 и ПО Лаборатории Касперского имеется возможность связать Сервер безопасности и Сервер администрирования Касперского (далее — KSC) между собой с применением протокола OpenAPI для того, чтобы получать в Консоли Сервера безопасности информацию о важных событиях на KSC, а также о событиях на клиентских АРМ с установленным клиентом Dallas Lock 8.0 (введенным в домен безопасности вышеуказанного Сервера безопасности) и ПО Kaspersky Endpoint Security (далее — ПО KES), связанных с оповещением о событиях безопасности ПО KES (АРМ с ПО KES должны централизованно управляться KSC с помощью установленного также АРМ Агента администрирования Касперского).

В данном случае рассматривается взаимодействие со следующим ПО Лаборатории Касперского:

1. Сервер администрирования Касперского (Kaspersky Security Center) версии:
   - Kaspersky Security Center 10 (10.5.1781.0)
   - Kaspersky Security Center 11 (11.0.0.1131 (патч b))
   - Kaspersky Security Center 12.2 (12.2.0.4376)
   - Kaspersky Security Center 13 (13.0.0.11247)
2. Kaspersky Endpoint Security 11 версии:
   - 11.0.0.6499
   - 11.1.1.126 (патч pf7523)
   - 11.3.0.773
   - 11.6.0.394

Для совместной работы СБ и Kaspersky Security Center необходимо открыть дополнительное меню КСБ  → «Взаимодействие с Kaspersky Security Center». Отобразится окно (рис. 404) с полями для ввода следующих параметров:

- Имя сервера KSC. Необходимо указать сетевое имя или ip-адрес сервера KSC.
- Логин администратора KSC.
- Пароль администратора KSC.
- Номер порта для подключения к KSC. Необходимо указать тот же номер порта, который был выбран в KSC для Kaspersky Security Center Web Console в консоли KSC – “Свойства Сервера администрирования” - “Параметры подключения к Серверу администрирования” – “Порты подключения” (стандартный порт - 13299).

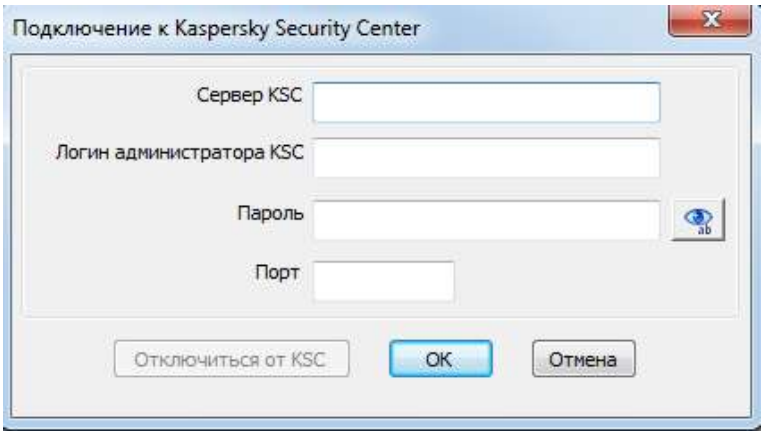


Рис. 404. Окно Подключения

После заполнения полей нужно нажать кнопку «ОК» для подтверждения подключения к KSC. Для отмены подключения нужно нажать «Отмена».
Если взаимодействие СБ и KSC уже было настроено, то для отключения СБ от KSC необходимо нажать на кнопку «Отключиться от KSC» и подтвердить действие.

Значки объектов, обозначающие клиентов СБ с установленным ПО KES и подключенных к KSC, в зависимости от состояния клиента могут принимать следующий вид:

 — клиент выключен;

 — связь с клиентом отсутствует свыше заданного на СБ времени, которое определяется параметром «Оповещение при отсутствии связи с клиентом» (при условии, что настроено оповещение об отсутствии связи с клиентом);

 — на клиенте не отвечает Dallas Lock 8.0;

 — клиент включен;

 — СБ собирает журналы с клиента Dallas Lock 8.0;

 — на клиенте установлена более старая версия Dallas Lock 8.0. Для таких клиентов не доступно ОУ и не работает синхронизация;

 — на клиенте установлена более старая версия Dallas Lock 8.0, при этом клиент работает в «неактивном режиме СЗИ»;

 — клиент работает в «неактивном режиме СЗИ».

KSC собирает журналы со всех клиентов с установленным ПО KES, а также предоставляет СБ журнал событий, полученных на АРМ с установленным KSC.

Перечень событий KSC представлен далее.

Предупреждение
• Лицензионное соглашение. • Устройство долго не проявляет активности в сети. • Разорвано соединение с подчиненным KSC. • Разорвано соединение с главным KSC. • Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN. • Началось удаление событий из базы данных, так как превышено ограничение числа событий. • Удалены события из базы данных, так как превышено ограничение числа событий. • Срок действия лицензии истекает.
Критический уровень
• Лицензионное ограничение превышено. • Вирусная атака. • Устройство стало неуправляемым. • Статус устройства «Критический». • Файл ключа в черном списке. • Режим ограниченной функциональности. • Срок действия лицензии истекает. • Срок действия сертификата истек. • Обновления модулей программы «Лаборатории Касперского» отозваны.

Отказ функционирования
• Ошибка времени выполнения. • Для одной из групп лицензионных программ превышено ограничение числа установок. • Не удалось выполнить опрос облачного сегмента. • Не удалось выполнить копирование обновлений в заданную папку. • Нет свободного места на диске. • Недоступна папка общего доступа. • Недоступна информационная база KSC. • Нет свободного места в информационной базе KSC.
Информационное событие
• Ключ использован более чем на 90%. • Найдено новое устройство. • Устройство автоматически добавлено в группу. • Устройство удалено из группы: долгое отсутствие активности в сети. • Для одной из групп лицензионных программ число разрешенных установок исчерпано более чем на 95%. • Появились файлы для отправки на анализ в «Лабораторию Касперского». • Идентификатор экземпляра FCM мобильного устройства изменен. • Обновления успешно скопированы в заданную папку. • Установлено соединение с подчиненным KSC. • Установлено соединение с главным KSC. • Базы обновлены. • Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно. • Прокси-сервер KSN был остановлен. • Аудит: Установлено соединение с Сервером администрирования. • Аудит: Изменение объекта. • Аудит: Изменение статуса объекта. • Аудит: Изменение параметров группы.

Для фиксации событий, получаемых с KSC на СБ, существует категория «Журнал Kaspersky» вкладки «Журнал СБ» (см. «Журнал СБ»).

При переходе на уровень СБ на вкладке «Состояние» в верхней информационной панели отображается окно «Лаборатория Касперского».

При помощи кнопки «Сканировать клиентов» будет запущен процесс поиска вирусов на клиентских АРМ на уровне СБ (транслируя запрос с СБ на KSC как задачу поиска вирусов). Для запуска на уровне клиента необходимо на уровне клиента выбрать пункт «Сканировать клиента» в контекстном меню. Принудительное сканирование возможно только в отношении клиентских АРМ, на которых установлено ПО KES.

При нажатии на кнопку «Сканировать клиентские АРМ» появится окно (рис. 405) с выбором следующих элементов и кнопками «Далее» и «Отмена»:

- Системная память.
- Объекты автозапуска.
- Загрузочные секторы.
- Системное резервное хранилище.
- Все съемные диски.
- Все жесткие диски.
- Все сетевые диски.

Установка чекбокса означает, что необходимо проверить на вирусы соответствующий объект.

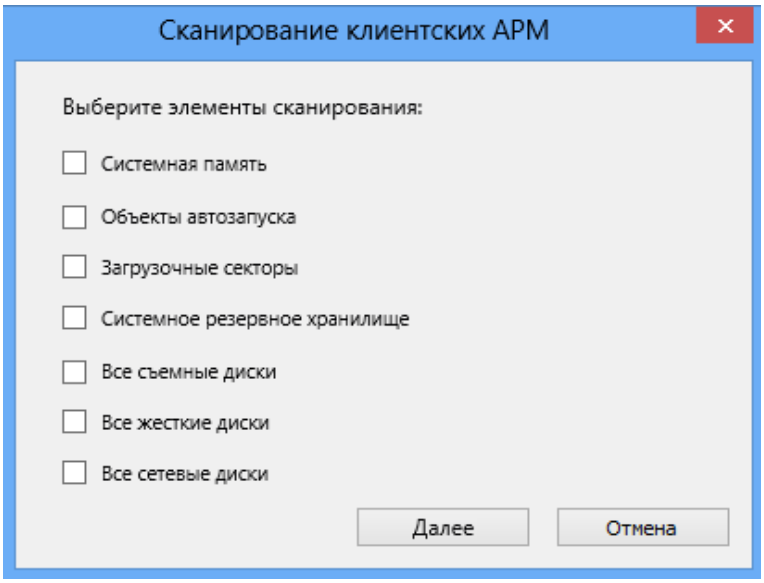


Рис. 405. Окно Сканирования

При помощи кнопки «Обновить антивирусные базы» будет запущен процесс обновления антивирусных баз данных на клиентских АРМ на уровне СБ, а также на уровне клиента (транслируя запрос с СБ на KSC как задачу обновления). Для запуска на уровне клиента необходимо на уровне клиента выбрать пункт «Обновить антивирусные базы» в контекстном меню. Принудительное обновление возможно только в отношении клиентских АРМ, на которых установлено ПО KES.

19.10.5 Параметры СБ для Windows клиентов

Для изменения параметров СБ необходимо открыть дополнительное меню КСБ → «Параметры Сервера безопасности…» → «Windows».

Появится окно «Параметры Сервера безопасности» для клиентов Windows (рис. 406).

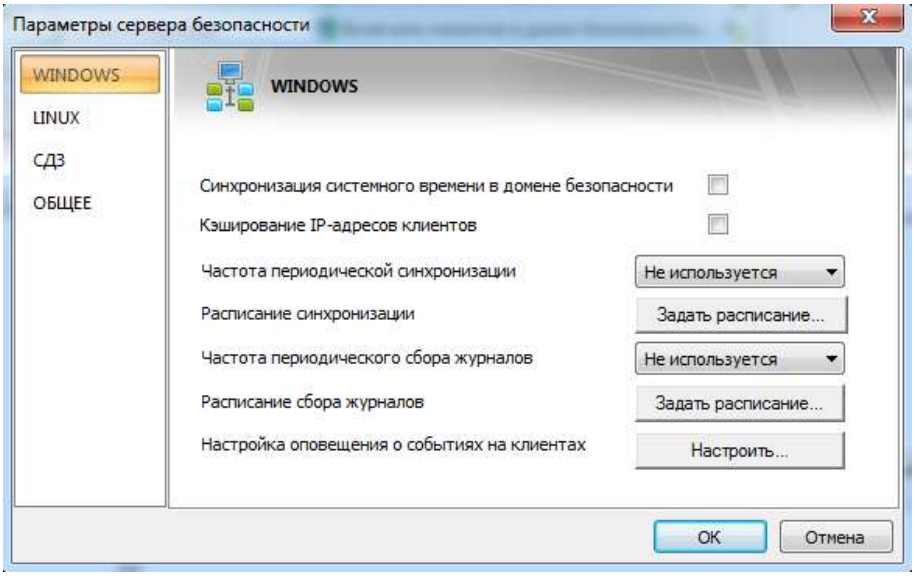


Рис. 406. Параметры СБ

Доступны следующие параметры.

Синхронизация системного времени в домене безопасности
При включении данного параметра осуществляется синхронизация системного времени клиентов ДБ с системным временем СБ.
Частота периодической синхронизации
Данный параметр позволяет производить автоматическую синхронизацию через указанный промежуток времени: от 10 минут до 24 часов. Для отключения необходимо выбрать значение «Не используется».

Расписание синхронизации
Данный параметр позволяет настроить автоматический сбор журналов по гибкому расписанию. В окне настройки расписания необходимо включить контроль, поставив флаг в поле «Использовать расписание», и составить расписание.
Частота периодического сбора журналов
Данный параметр позволяет производить автоматический сбор журналов через указанный промежуток времени: от 5 минут до ежемесячно. Для отключения необходимо выбрать значение «Не используется».
Расписание сбора журналов
Данный параметр позволяет настроить автоматический сбор журналов по гибкому расписанию. В окне настройки расписания необходимо включить контроль, поставив флаг в поле «Использовать расписание», и составить расписание.
Настройка оповещения о событиях на клиентах
Данный параметр позволяет настроить оповещения о событиях НСД на клиенте и почтовые уведомления (см. «Сигнализация об НСД»).

Сигнализация об НСД

Ситуации НСД на клиентах отслеживаются и сопровождаются сигнализацией на СБ. Сообщения о событиях НСД заносятся в журнал СБ. Сообщения о событиях клиента приходят на СБ пачками с интервалом (около 30 секунд), при этом время каждого события записывается фактическое, когда событие произошло на клиенте. На ПК с запущенной КСБ воспроизводится звуковой сигнал и выводится всплывающее сообщение на панели задач (рис. 407).

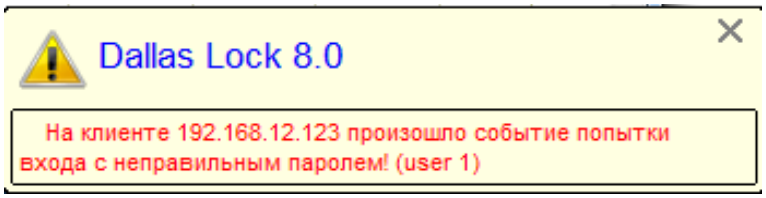


Рис. 407. Сигнализация на СБ

Для настройки оповещений и звукового сигнала необходимо открыть дополнительное меню КСБ  → «Параметры Сервера безопасности…» → «Windows» → нажать кнопку «Настроить» для параметра «Настройка оповещения о событиях на клиентах» (рис. 408).

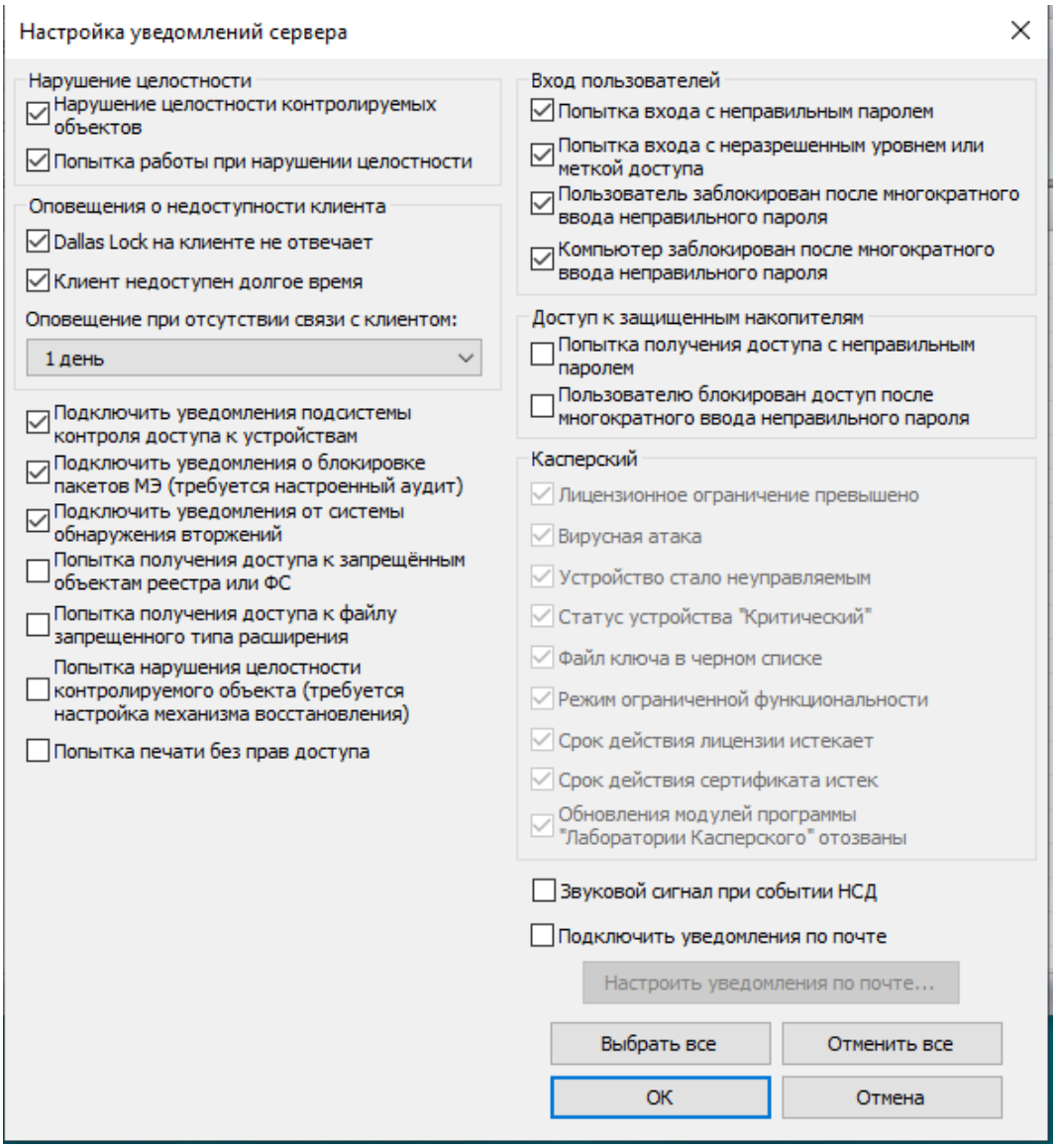


Рис. 408. Настройка уведомлений сервера

Доступны следующие параметры.

Нарушение целостности контролируемых объектов
При включении данного параметра осуществляется оповещение о событиях, связанных с нарушением целостности контролируемых объектов ФС/реестра. Сигнализация при нарушении целостности происходит при ее проверке. Если необходимо, чтобы целостность контролируемых файлов отслеживалась периодически, необходимо включить параметр «Периодический контроль целостности» (см. «Настройка параметров контроля целостности»). При нарушенной целостности сигнализация произойдет один раз и при первой проверке.
Попытка работы при нарушении целостности
При включении данного параметра осуществляется оповещение о попытке авторизоваться при нарушенной целостности объекта на клиенте.
Dallas Lock на клиенте не отвечает
При включении данного параметра осуществляется оповещение о том, что система защиты Dallas Lock 8.0 клиента не отвечает СБ. Возможная причина — несанкционированная деактивация системы защиты. Клиент в дереве КСБ будет отображаться специальным знаком .
Клиент не доступен долгое время
При включении данного параметра осуществляется оповещение об отсутствии связи клиента с СБ в течение длительного периода. Период определяется параметром «Оповещение при отсутствии связи с клиентом».

Оповещение при отсутствии связи с клиентом

Данным параметром устанавливается максимальный срок отсутствия связи клиента с СБ. По истечении установленного срока клиент в дереве КСБ будет отображаться специальным знаком  .

Подключить уведомления подсистемы контроля доступа к устройствам

При включении данного параметра осуществляется оповещение о попытках монтирования и работы с запрещенными устройствами на клиенте.

Подключить уведомления о блокировке пакетов МЭ (требуется настроенный аудит)

При включении данного параметра осуществляется оповещение о сработавших правилах МЭ. Предварительно на клиенте необходимо настроить «Журнал пакетов МЭ».

Подключить уведомления от системы обнаружения вторжений

При включении данного параметра осуществляется оповещение о сработавших сигнатурах СОВ и заблокированных адресах.

Попытка получения доступа к запрещенным объектам реестра или ФС

При включении данного параметра осуществляется оповещение о событиях попытки получения доступа к запрещенным объектам реестра или ФС.

Примечание. События регистрируются только при настроенном аудите. Например, при назначенном дескрипторе аудита отказа на объекте ФС или глобального аудита отказов. Сбор журналов с клиентов производить не нужно.

Попытка получения доступа к файлу запрещенного типа расширения

При включении данного параметра осуществляется оповещение о событиях попытки получения доступа к файлам запрещенного типа расширения.

Примечание. События регистрируются только при настроенном аудите. Например, при назначенном дескрипторе аудита отказа на объекте ФС или глобального аудита отказов. Сбор журналов с клиентов производить не нужно.

Попытка нарушения целостности контролируемого объекта (требуется настройка механизма восстановления)

При включении данного параметра осуществляется оповещение о событиях, связанных с нарушением целостности контролируемых объектов ФС и их восстановлением из резервных копий (в случае, если механизм восстановления настроен).

Попытка печати без прав доступа

При включении данного параметра осуществляется оповещение о попытках печати документов без прав доступа на данное действие.

Попытка входа с неправильным паролем

При включении данного параметра осуществляется оповещение о попытке входа пользователя с неправильным паролем.

Попытка входа с неразрешенным уровнем или меткой доступа

Данный параметр доступен только для Dallas Lock 8.0 редакции «С»

При включении данного параметра осуществляется оповещение о попытке входа пользователя с неразрешенным уровнем доступа или мандатной меткой.

Пользователь заблокирован после многократного ввода неправильного пароля

При включении данного параметра осуществляется оповещение о блокировке пользователя после многократного ввода неправильного пароля (настраивается параметром безопасности «Вход: максимальное количество ошибок ввода пароля»).

Компьютер заблокирован после многократного ввода неправильного пароля

При включении данного параметра осуществляется оповещение о блокировке компьютера после многократного ввода неправильного пароля (настраивается параметром безопасности «Вход: блокирование компьютера в случае ввода неправильных паролей»).

Попытка получения доступа с неправильным паролем

При включении данного параметра осуществляется оповещение о попытке получения доступа с неправильным паролем к преобразованному сменному накопителю.

Пользователю блокирован доступ после многократного ввода неправильного пароля

При включении данного параметра осуществляется оповещение о блокировке доступа к преобразованному сменному накопителю для пользователя после многократного ввода неправильного пароля (настраивается параметром безопасности «Вход: максимальное количество ошибок ввода пароля»).

Звуковой сигнал при событии НСД

Данный параметр позволяет включить звуковой сигнал при регистрации события НСД. Звуковой сигнал воспроизводится на ПК с запущенной КСБ.

Подключить уведомления по почте

Данный параметр позволяет подключить автоматическую отправку уведомлений о событиях НСД на электронную почту (см. «Отправка почтовых уведомлений об НСД»).

Kaspersky

Для комфортной работы и отслеживания состояния работы СБ совместно с ПО KES, пользователь может включить данные типы уведомлений (могут быть получено только при включенном взаимодействии СБ с KSC, по-умолчанию все включены):

- Лицензионное ограничение превышено;
- Вирусная атака;
- Устройство стало неуправляемым;
- Статус устройства «Критический»;
- Файл ключа в черном списке;
- Режим ограниченной функциональности;
- Срок действия лицензии истекает;
- Срок действия сертификата истек;
- Обновления модулей программ «Лаборатории Касперского» отозваны.

Внимание! Событие типа “вирусная атака” поступает непосредственно с ПО KES, потому сигнализация о нем происходит на уровне АРМ, с установленным KES для каждого конкретного АРМ.

Для получения событий: лицензионное ограничение превышено, устройство стало неуправляемым, статус устройства «Критический», файл ключа в черном списке, режим ограниченной функциональности, срок действия лицензии истекает, срок действия сертификата истек, обновления модулей программы «Лаборатории Касперского» отозваны (генерируемых именно KSC), — необходимо, чтобы:

- на АРМ с установленным KSC было установлено СЗИ Dallas Lock 8.0 и введено в домен безопасности СБ;
- на АРМ с установленным KSC был установлен KES под управлением этого KSC.

При соблюдении вышеуказанных условий указанные события будут поступать на уровне АРМ с установленным KSC.

События сигнализации отображаются в полученных с клиентов журналах, а также в интерфейсе КСБ на уровне клиента в категории «Состояние» → «События НСД» (рис. 409).

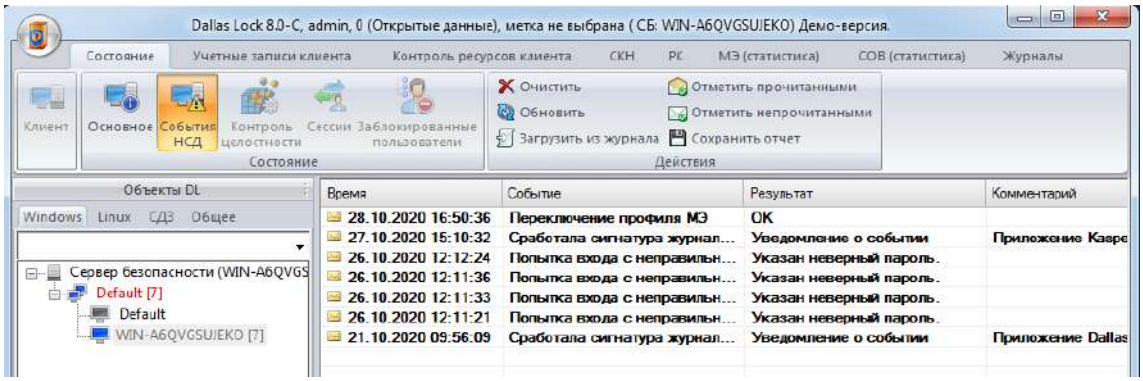


Рис. 409. Журнал событий сигнализации об НСД

Список событий НСД клиента собирается из журналов клиента.

С помощью панели действий для списка событий НСД возможно отметить все записи прочитанными или непрочитанными, обновить, очистить список и загрузить новый список НСД из журналов клиента. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

Также возможно сохранить отчет обо всех событиях НСД на клиенте (без учета их фильтрации). Для этого необходимо воспользоваться кнопкой «Сохранить отчет».

На уровне клиента при просмотре событий НСД в графу «Комментарий» можно добавить текстовые комментарии. Для этого необходимо двойным кликом мыши вызвать окно описания события и в текстовом поле ввести необходимую информацию (рис. 410). Для применения изменений нажать кнопку «Закрыть» либо перейти к следующему событию. Введенный текст отобразится в графе «Комментарий» и будет виден на вкладке «Состояние» → «Основное» (на уровне клиента, группы клиентов и СБ).

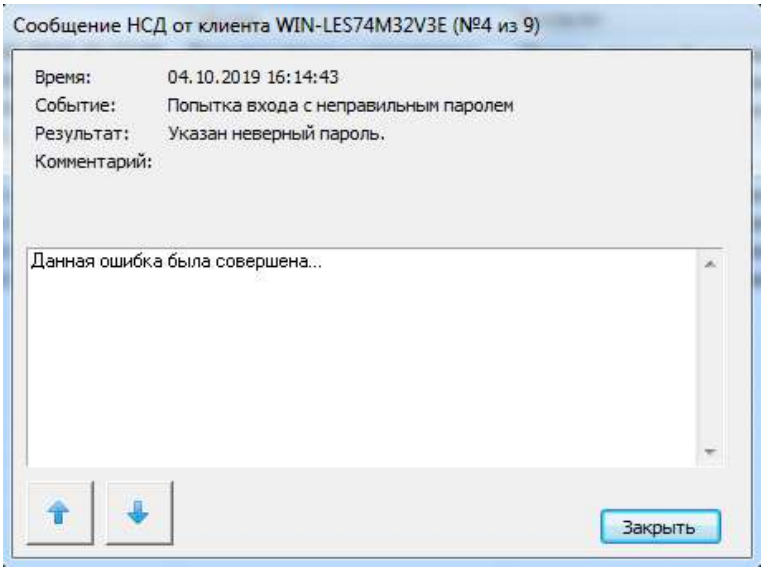


Рис. 410. Добавление комментария к событию НСД

Общее состояние всего ДБ возможно узнать на уровне СБ в категории «Состояние» → «Основное» (см. «Основное»).

Также количество полученных новых (непрочитанных) сообщений дополнительно отображается в дереве объектов КСБ: после имени клиента и наименования группы (общее количество сообщений с клиентов данной группы), после имени СБ (общее количество сообщений с клиентов всего ДБ) (рис. 411).

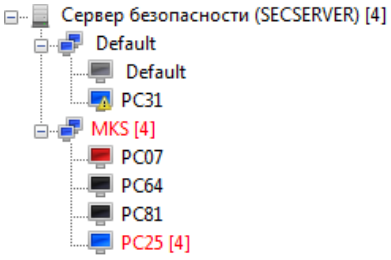


Рис. 411. Визуальное отображение оповещений о полученных событиях НСД

Операции с сообщениями НСД дополнительно доступны из контекстного меню выбранного объекта в дереве объектов КСБ.

Отправка почтовых уведомлений об НСД

Реализована возможность отправки почтовых уведомлений на e-mail (электронную почту) с СБ о событиях, связанных с НСД на клиентах ДБ.

Для настройки почтовых уведомлений об НСД необходимо открыть дополнительное меню КСБ → «Параметры Сервера безопасности…» → «Windows» → нажать кнопку «Настроить» для параметра «Настройка оповещения о событиях на клиентах». В окне «Настройка уведомлений сервера» активировать параметр «Подключить уведомления по почте» и нажать кнопку «Настроить уведомления по почте…».

Примечание. Взаимодействие с почтовыми серверами, использующими для защиты сетевого трафика SSL/TLS, не поддерживаются.

Появится окно «Настройка почтовых уведомлений» (рис. 412), в котором:

1. Необходимо задать имя исходящего почтового сервера SMTP или его IP — адрес и указать № порта SMTP-сервера (например, «mail.ru» или «192.168.0.249:25»).
2. Если на почтовом сервере требуется авторизация, необходимо выставить флаг и заполнить поля логина и пароля.
3. В поле «Кому» ввести e-mail, на котором необходимо принимать сообщения о НСД, в поле «От кого» ввести существующий e-mail отправителя.
4. Ввести заголовок и текст письма.

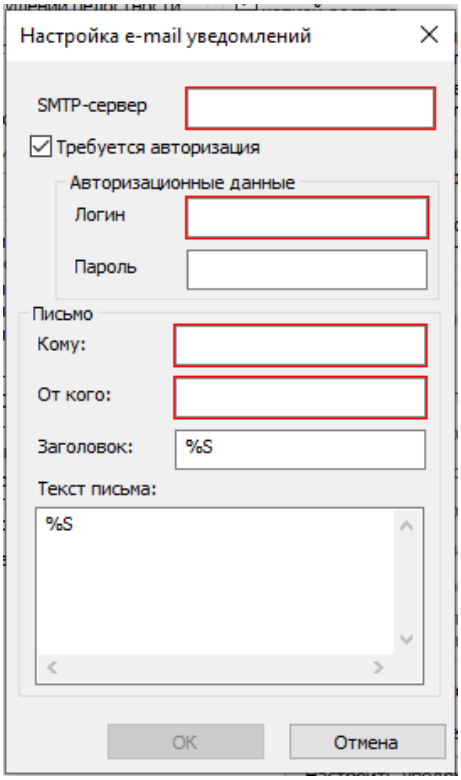


Рис. 412. Настройка почтовых уведомлений о НСД

Настройки оформления диаграмм

В СБ предусмотрена возможность пользовательской настройки визуализации диаграмм событий НСД в зависимости от приоритета и типа события. Кнопка настройки доступна на вкладке «Состояние» → «Основное» (рис. 413).

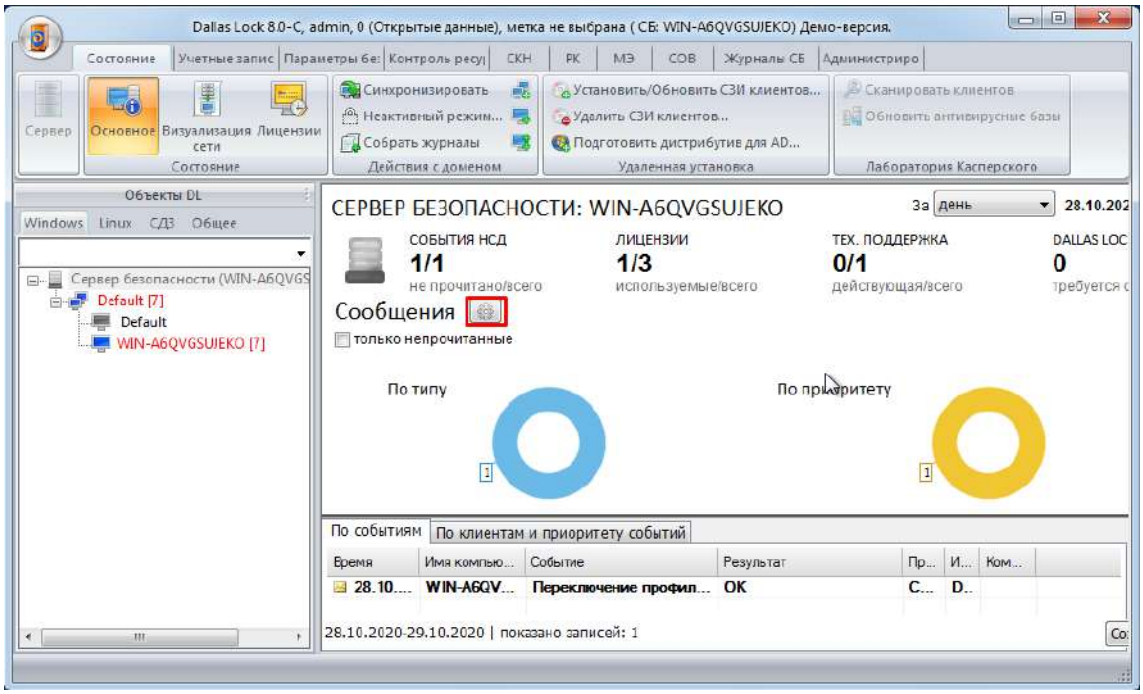


Рис. 413. Настройка оформления

При нажатии кнопки, появляется окно «Настройка оформления». В левой части окна расположены 3 категории:

- «Объекты наблюдения»;
- «Приоритеты»;
- «Цвета».

В категории «Объекты наблюдения» доступен выбор объекта домена, который находится под наблюдением (рис. 414).

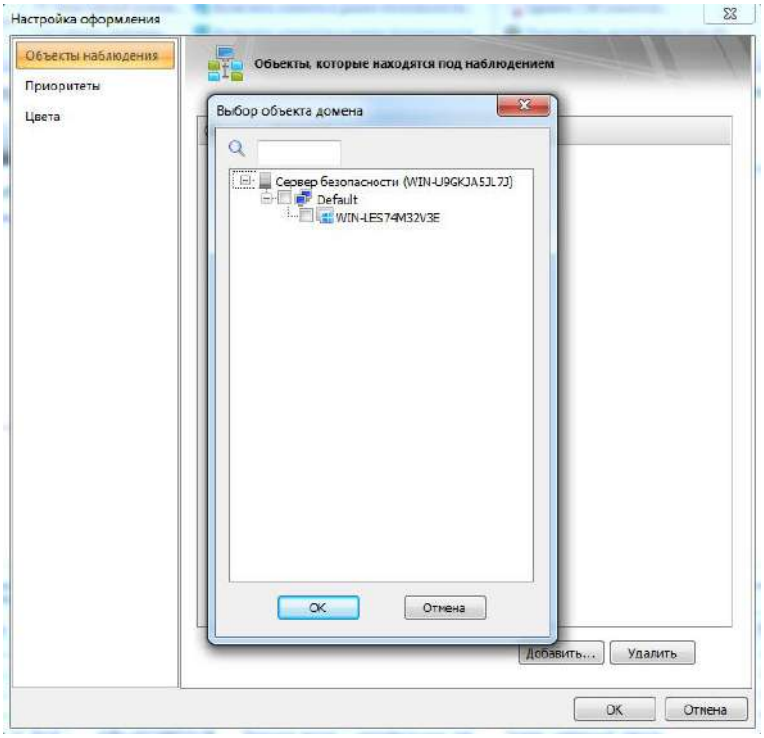


Рис. 414. Объекты наблюдения

В категории «Приоритеты» отображается список доступных приоритетов в виде таблицы настройки правил контроля приложений. Таблица состоит из полей «Событие НСД» и «Приоритет». Для каждого события можно изменить приоритет выбором одного из значений в выпадающем списке. Доступны приоритеты событий: «Высокий», «Средний» и «Низкий» (рис. 415).

Каждый приоритет выделяется следующим цветом:

- «Высокий» — красный цвет;

- «Средний» — желтый цвет;
- «Низкий» — зеленый цвет.

Над таблицей расположен чекбокс «Наследовать», предназначенный для уровней ниже СБ. При включенном чекбоксе настройки приоритетов будут наследоваться у вышестоящего уровня.

Настройки этой таблицы влияют на внешний вид диаграммы «Приоритет событий НСД» на вкладке «Состояние» → «Основное».

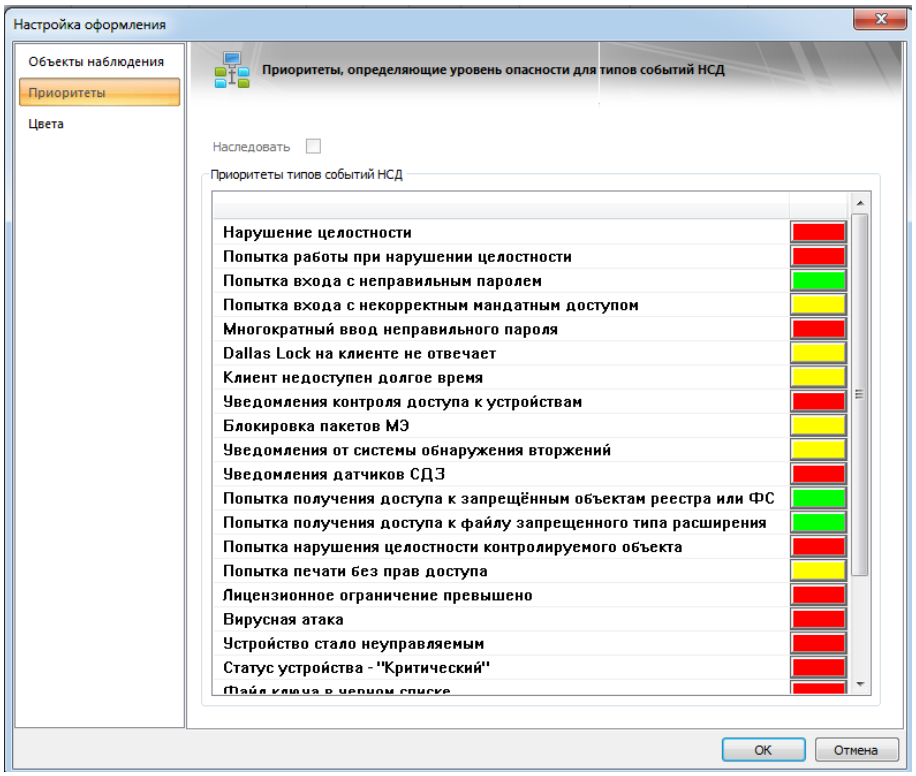


Рис. 415. Приоритеты

В категории «Цвета» отображается таблица, состоящая из полей «Событие НСД» и «Цвет». Она необходима для настройки раскраски сегментов диаграммы в зависимости от типа события НСД на вкладке «Состояние». Для смены цвета события нужно нажать на него левой кнопкой мыши и выбрать цвет из палитры (рис. 416).

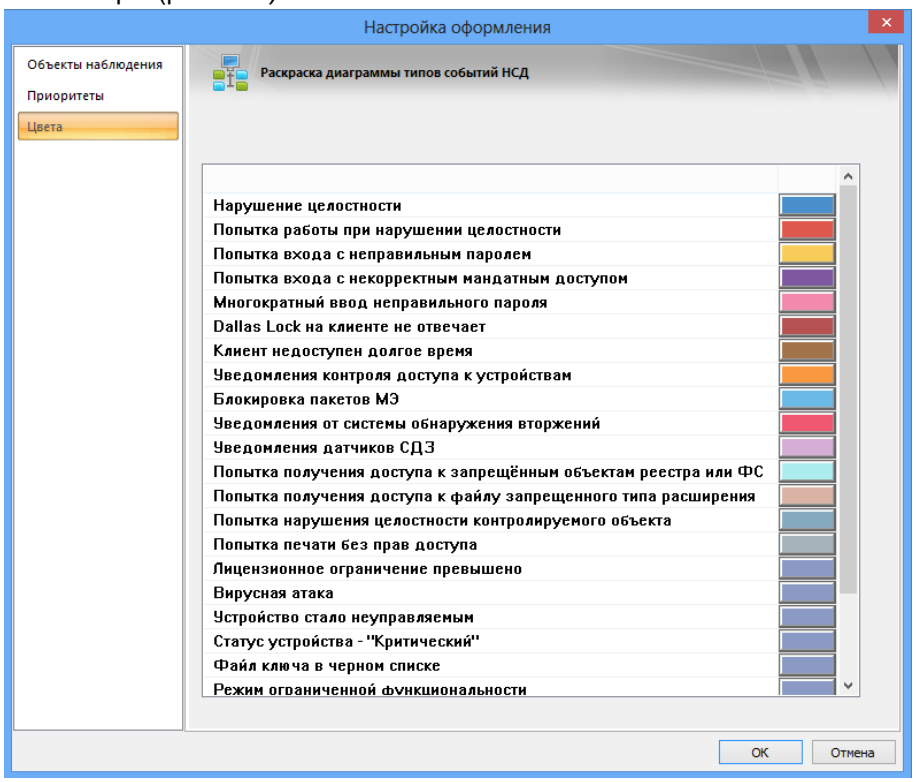


Рис. 416. Раскраска диаграммы типов событий НСД

Настройки этой таблицы влияют на внешний вид диаграммы «Типы событий НСД» на вкладке «Состояние».

19.10.6 Репликация

Под репликацией понимается процесс дублирования параметров безопасности серверов безопасности с целью повышения отказоустойчивости системы и повышения производительности.

В случае отказа одного из серверов безопасности, работа клиентов не будет нарушена, в следствие того, что все настройки, сделанные для одного сервера, применяются на всех Серверах безопасности, введенных в домен.

Примечание. Серверы в репликации практически по всем задачам распределяют нагрузку (это одна из задач, решаемых при построении кластера). В том числе это касается анализа состояния узлов в сети. Поэтому, если узел становится недоступным для какого-либо сервера, эта информация может быть синхронизирована с другими серверами в кластере. При обнаружении несоответствий фактической доступности клиентов с диагностируемой следует убедиться, что в репликации нет сервера, который не может установить с клиентом сетевое соединение.

Реализовано динамическое применение изменений параметров на сторонние серверы.

Реализована функция дублирования журналов. СБ (выбранный случайно клиентом или инициировавший сбор журналов) осуществляет сбор журналов с клиента. Проводится компоновка всех полученных журналов и теневых копий в блок данных, который рассылается на все сервера ДБ. Другие СБ принимают этот блок, преобразуют в файлы копий и журналов, и отправляют в папки своих клиентов. Сборка итоговых журналов проводится локально каждым СБ после получения.

При вводе нового сервера в существующий ДБ (см. «Настройки ДБ») все СБ в ДБ, в том числе не участвующие в непосредственной регистрации нового СБ, автоматически оповещаются о новом «участнике».

Примечание. При использовании СЛ следует обратить внимание на следующее: для СЛ в аппаратном ключе прописывается не число клиентов, а число лицензий на централизованное управление. Поэтому если имеется конфигурация из N клиентов с M реплицированными серверами, потребуется M*N лицензий на централизованное управление в аппаратном ключе (ключей может быть несколько, значения с нескольких ключей будут суммированы на СЛ). Соответственно, чем больше реплицированных серверов, тем быстрее расходуются лицензии на управление, тем меньше клиентов можно ввести в ДБ. Если же сервер лицензии не используется для обеспечения описанной выше или аналогичной конфигурации, потребуется M аппаратных ключей, на каждом из которых прописано N лицензий на централизованное управление: один ключ на один СБ.

19.10.7 Настройки ДБ

Для изменения настроек ДБ необходимо открыть дополнительное меню КСБ  → «Настройки домена безопасности…».

Появится окно «Настройки домена безопасности», где возможно ввести СБ в уже существующий ДБ для репликации (см. «Репликация») и изменить имя ДБ (рис. 417).

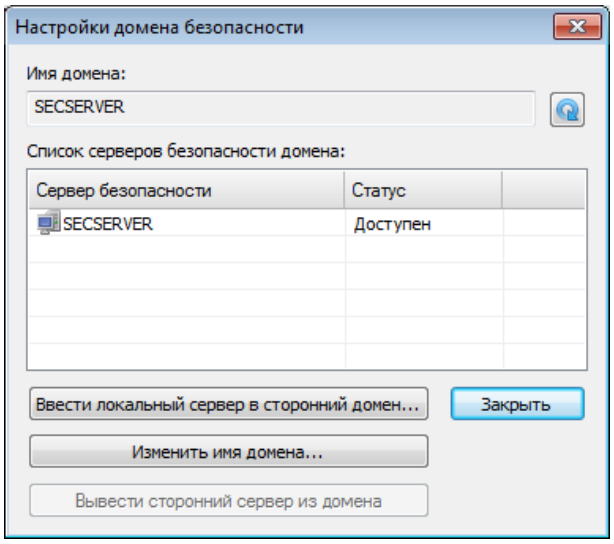


Рис. 417. Настройки ДБ

19.10.8 Настройка СБ для всего ДБ

На уровне СБ в верхней части консоли формируется набор вкладок для общей настройки параметров безопасности всего ДБ, всех клиентов данного СБ. При выборе определенной вкладки появляется возможность просматривать и редактировать параметры безопасности.

Примечание. Некоторые вкладки КСБ с параметрами, настраиваемыми для всего ДБ (для объекта СБ дерева объектов КСБ) аналогичны этим же категориям в оболочке администратора Dallas Lock 8.0 на ПК с СБ.

Но управлять зарегистрированными локальными учетными записями, правами пользователей и установкой параметров безопасности нужно из стандартной оболочки администратора на ПК с СБ, а отдельными доменными учетными записями и установкой параметров безопасности ДБ через КСБ.

Состояние СБ

Основное

Для удобства работы возможно узнать общее состояние всего ДБ, данные сведения отображаются в категории «Состояние» → «Основное» (рис. 418).

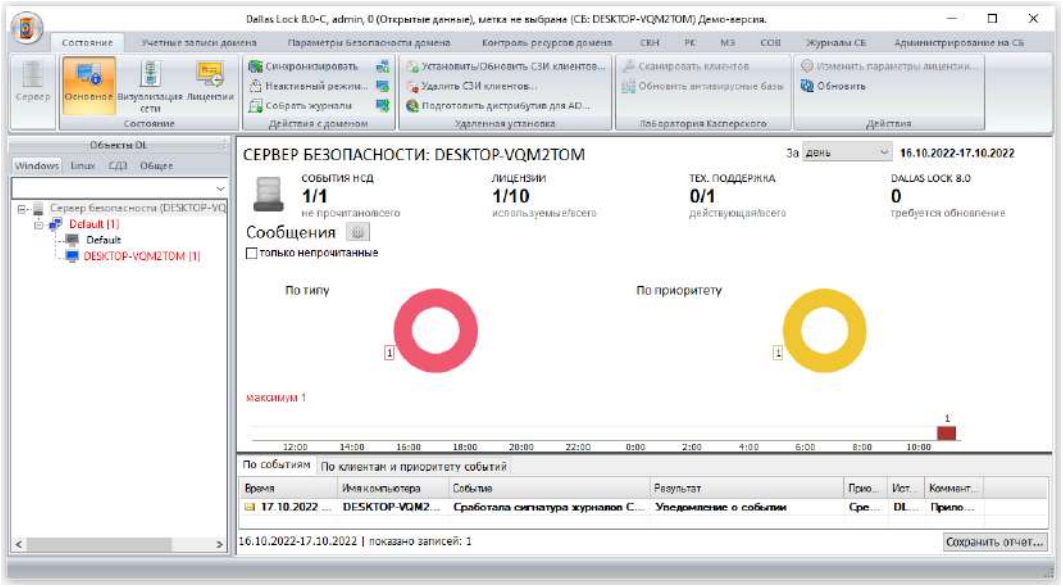


Рис. 418. Вкладка «Состояние» Сервера безопасности

Доступны следующие действия с ДБ:

1. Синхронизация параметров безопасности всего ДБ по команде администратора СБ.
2. Включение и настройка неактивного режима для всего ДБ (см. «Неактивный режим»).

3. Добавление новой группы клиентов, для последующей групповой настройки параметров безопасности для клиентов.
4. Добавление клиента/клиентов в ДБ (см. «Ввод клиента в ДБ»).
5. Сбор журналов с клиентов.
6. Установка, обновление и удаление СЗИ клиентов (см. «Централизованная установка Dallas Lock 8.0 средствами СБ», «Обновление версий Dallas Lock 8.0 средствами СБ» и «Централизованное удаление Dallas Lock 8.0» соответственно).
7. Подготовка дистрибутива для AD (см. «Централизованная установка Dallas Lock 8.0 средствами Active Directory»).

В верхней части информационной панели расположена следующая информация:

- Количество событий НСД на всех клиентах ДБ за выбранный период времени в формате: не прочитано/всего событий НСД.
- Количество используемых лицензий.
- Количество клиентов с активной технической поддержкой.
- Количество клиентов ДБ, которым необходимо обновить Dallas Lock 8.0.

При активном поле «только непрочитанные» в категории «Сообщения», на информационной панели будет отображаться информация только для непрочитанных событий НСД.

Период времени можно изменить в верхней правой части рабочей области, использовав выпадающий список «За» и выбрав период времени:

- день;
- неделю;
- месяц;
- период — при выборе данного пункта в появившемся окне (рис. 419) возможно задать необходимый отрезок времени);
- все время.

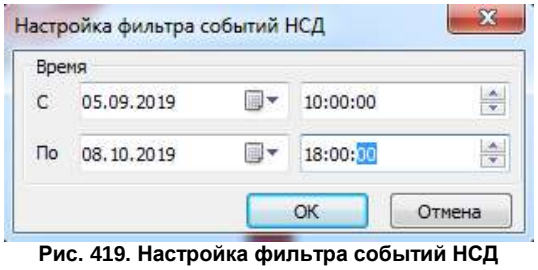


Рис. 419. Настройка фильтра событий НСД

В центральной части информационной панели расположены круговые диаграммы:

- Типы событий НСД, которая отображает количество событий НСД определенного типа. Для каждого типа событий можно настроить цвет (см. ниже).
- Приоритет событий НСД, которая отображает количество событий НСД по их приоритетам. Для каждого типа событий можно настроить приоритет (см. ниже).

Под круговой диаграммой расположена гистограмма, которая отображает количество событий НСД всех типов за выбранный период времени с определенным шагом. При нажатии на элемент гистограммы, в таблице отображаются события за выбранный шаг времени.

В правой части информационной панели отображаются объекты наблюдения. По умолчанию объекты наблюдения отсутствуют. В объектах наблюдения отображается суммарное количество событий НСД на клиенте или клиентах, входящих группу дерева КСБ, за выбранный период времени. Через слеш указывается количество непрочитанных (необработанных) событий НСД.

В нижней части информационной панели расположена таблица, содержимое которой зависит от выбранного элемента в круговых диаграммах или гистограмме (по умолчанию отображаются все события НСД). При нажатии на пустую область вокруг диаграммы, в таблице отображаются все события НСД. Таблица имеет следующие режимы работы:

- Показывать информацию по событиям НСД. Двойной клик по событию откроет запись в отдельном окне, в таблице данное событие будет помечено как прочитанное. Нажимая на кнопки «вверх» и «вниз» можно отмечать события как прочитанные, просматривая предыдущие или следующие события.
- Показывать информацию по клиентам и приоритету событий НСД.

Для того, чтобы сформировать отчет по представленным данным о событиях НСД с учетом настроенной фильтрации необходимо нажать кнопку «Сохранить отчет…» в нижнем правом углу рабочей области (под таблицей). Отчет возможно сохранить в одном из форматов:

- TXT;
- CSV (разделитель — точка с запятой);

- HTML;
- XML.

Описание настройки рабочей области приведено в разделе «Настройки оформления диаграмм».

Визуализация сети

В КСБ Dallas Lock 8.0 имеется средство отображения топологии ДБ. Для этого необходимо выбрать состояние отображения рабочей область «Визуализация сети» на вкладке «Состояние» для СБ (рис. 420).

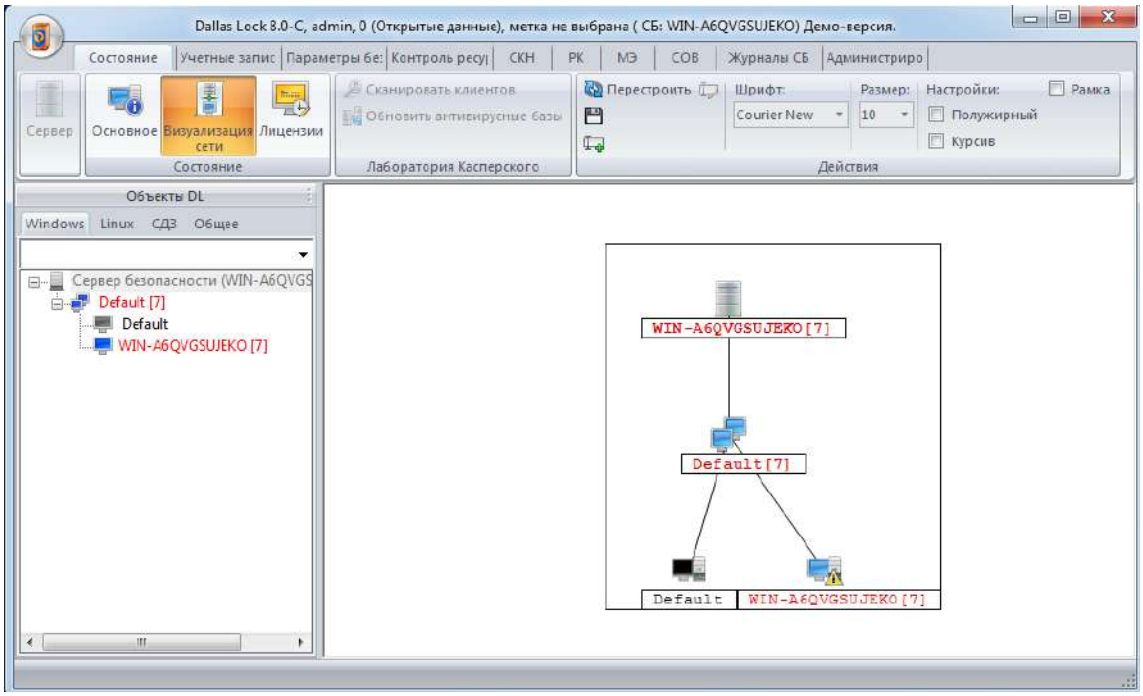


Рис. 420. Визуализация топологии ДБ

В рабочей области визуализации сети отображается многоуровневая архитектура ДБ: СБ, группы клиентов СБ, клиенты.

Манипулируя мышью, можно разнести объекты топологии по рабочей области (кликнув правой кнопкой мыши по объекту), передвинуть весь объект топологии (с помощью левой кнопки мыши).

С помощью панели действий можно добавлять и редактировать надписи в топологии, возвращать измененную топологию в исходное состояние (действие «Перестроить») и сохранить настроенный вид визуализации топологии сети в файл в формате на выбор .jpg, .png или .bmp (действие «Сохранить в файл»).

Лицензии

На информационной панели категории «Лицензии» отображается список всех клиентов (рис. 421), для которых:

- закончился срок действия технической поддержки,
- код технической поддержки не задан,
- срок действия технической поддержки не более 12 месяцев.

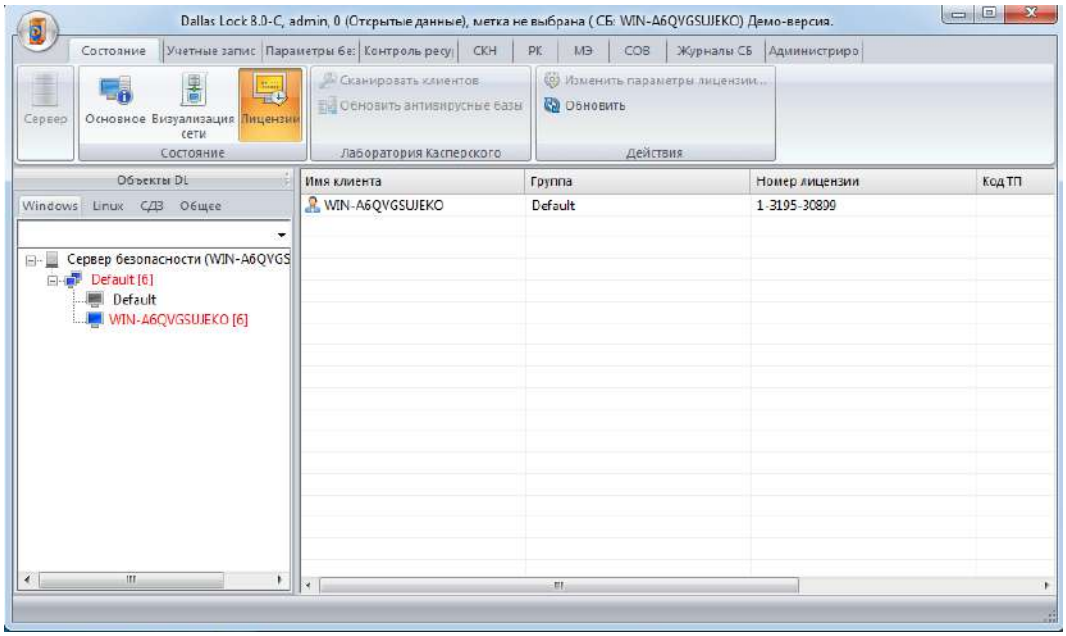


Рис. 421. Настройка лицензий клиентов

Для изменения номера лицензии или кода технической поддержки необходимо выбрать клиента (клиентов) в списке и нажать кнопку «Изменить параметры лицензии…». В появившемся окне ввести данные и подтвердить операцию.

Внимание! При изменении кодов со стороны КСБ: серийного, техподдержки, информационно-технического сопровождения — соответствующее изменение информации в КСБ отображается только после перезагрузки клиентского АРМ.

Учетные записи домена

Вкладка «Учетные записи домена» на уровне СБ позволяет управлять учетными записями ДБ. На всех клиентах ДБ могут работать учетные записи только из списка учетных записей ДБ (рис. 422).

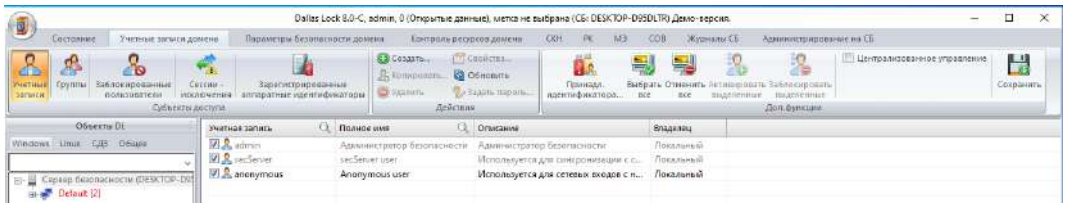


Рис. 422. Список учетных записей СБ

Создание учетной записи на СБ выполняется отдельно (см. ниже).

Через КСБ можно определить принадлежность аппаратного идентификатора так же, как и через оболочку администратора Dallas Lock 8.0 (см. «Определение принадлежности идентификатора»).

Для центрального управления через СБ на клиентах необходимо включить на панели «Доп.функции» функцию «Центральное управление». После включения централизованного управления, на клиентах будут удалены все группы, не заданные на СБ. Среди них могут оказаться служебные группы, созданные сторонним ПО для своей корректной работы. Рекомендуется предварительно создать такие группы на СБ. Все настройки для учетных записей пользователя на СБ будут автоматически синхронизироватся с клиентами СЗИ Dallas Lock 8.0.

Внимание! Учетные записи и группы СБ настраиваются через оболочку администратора. Через КСБ настраиваются только учетные записи и группы ДБ.

Создание пользователей ДБ

Список учетных записей ДБ в категории «Учетные записи домена» → «Учетные записи» формируется из учетных записей по умолчанию и зарегистрированных через КСБ.

Создание учетных записей с помощью КСБ имеет тот же механизм, что и в оболочке администратора. Однако следует учитывать, что в данном случае учетная запись Dallas Lock 8.0 и учетная запись Windows не создаются.

При задании пароля учетной записи ДБ необходимо, чтобы пароль не противоречил парольным политикам безопасности ОС Windows на клиентах ДБ. Если требование не будет соблюдено, то возникнет ошибка «Операция заблокирована ОС Windows» в процессе синхронизации учетных записей. Из-за данной ошибки, может наблюдаться следующее:

- проблема создания учетной записи с недостаточно сложным паролем;
- проблема синхронизации пароля учетной записи, если пользователь был создан ранее.

Во избежание ошибки синхронизации учетных записей, рекомендуется отключить парольные политики ОС Windows. Данная функциональная возможность реализована в Dallas Lock 8.0 независимо от механизмов ОС.

Примечание. Учетные записи суперадминистратора СБ Dallas Lock 8.0 и суперадминистратора Dallas Lock 8.0 на клиенте не синхронизируются.

После создания учетных записей, они автоматически появляются в списках учетных записей объектов ДБ: каждой группы (подгруппы) клиентов и каждого клиента.

Для каждой группы (подгруппы) клиентов и для каждого клиента возможно индивидуально определить, какие учетные записи из списка смогут работать на данных клиентах, а какие нет.

Для того, чтобы под учетной записью можно было работать на клиентах во всем ДБ, необходимо отметить ее на уровне СБ. Для того, чтобы запретить доступ на всех клиентах ДБ, необходимо снять отметку с данной учетной записи также на уровне СБ.

На всех клиентах, входящих в ДБ, параметры отмеченных пользователей будут идентичны.

Настройка учетных записей для групп и подгрупп клиентов описана в разделе «Учетные записи группы клиентов».

Настройка учетных записей для клиентов описана в разделе «Учетные записи клиента».

Создание группы пользователей ДБ

Список групп ДБ в категории «Учетные записи домена» → «Группы» формируется из групп по умолчанию и зарегистрированных через КСБ.

Создание групп ДБ с помощью КСБ имеет тот же механизм, что и в оболочке администратора.

В процессе синхронизации списки групп пользователей клиента и ДБ сравниваются, из списка клиента удаляются группы, которых нет в списке ДБ, и добавляются новые, которые уже добавлены в список ДБ, но не добавлены в список групп пользователей клиента. Таким образом, на всех клиентах, будут одинаковые группы.

Внимание! Следует учесть, что таким образом создаются группы ДБ, в которые можно добавлять только учетные записи ДБ. Доменные (AD) учетные записи добавляются в группы на контроллере домена.

Включение контроллера домена в ДБ

Для обеспечения управления учетными записями пользователей и группами безопасности на контроллере домена (доменными учетными записями) предварительно должно быть установлено СЗИ Dallas Lock 8.0 (редакции «К» или «С»). Контроллер домена должен быть введен в ДБ. При установке СЗИ Dallas Lock 8.0 на DC учетные записи пользователей в автоматическом режиме импортируются в DL установленный на контроллере домена.

Управление учетными записями и группами AD осуществляется на вкладке «Учетные записи домена» на уровне СБ (рис. 423).

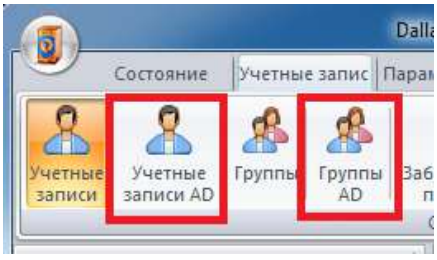


Рис. 423. Интерфейс управления учетными записями и группами AD

При нажатии на кнопку «Учетные записи AD» или «Группы AD» пользователю выдается комбинированный список, содержащий все введенные под управление СБ контроллеры домена. После выбора конкретного Контроллера домена, пользователь может непосредственно приступить к работе с доменными учетными записями выбранного контроллера домена (рис. 424).

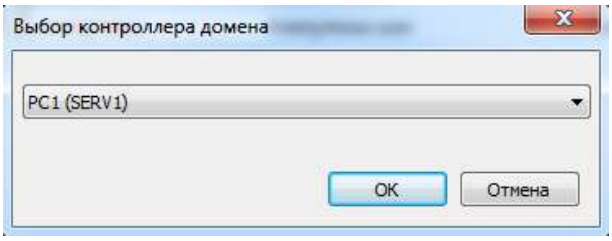


Рис. 424. Выбор контроллера домена

Режим ОУ происходит для пользователя в «скрытом» режиме, то есть выбранный для работы контроллер домена никак не выделяется.

Создание учетной записи происходит только в режиме скрытого ОУ с КСБ. При создании учетной записи пользователя в режиме скрытого ОУ на КСБ, данный пользователь появляется в группе безопасности Domain Users на Контроллере домена. Кроме того, созданная учетная запись автоматически появляется в глобальном списке на КСБ.

Редактирование свойств пользователя, назначение аппаратных ключей и мандатных меток в глобальном списке не доступно. Эти действия выполняются так же при нажатии кнопки «Учетные записи AD», выборе контроллера домена, выборе пользователя из списка и нажатии кнопки «Свойства» на панели сверху (рис. 425).

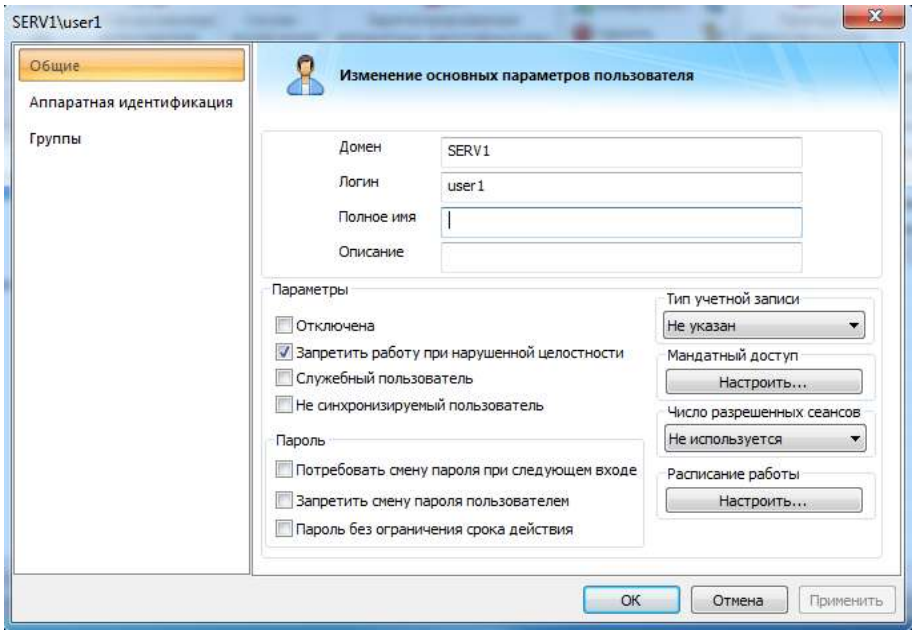


Рис. 425. Редактирование свойств пользователя домена AD

Средствами контроллера домена AD учетная запись данного пользователя может быть реплицирована на другие контроллеры домена, но он не появляется в консоли управления локальным СЗИ Dallas Lock 8.0 на контроллерах доменов, получивших реплику, и, соответственно, вход под данным пользователем на защищенную СЗИ Dallas Lock 8.0 рабочую станцию не возможен, если этому пользователю не был явно разрешен вход на конкретную рабочую станцию или контроллер домена через КСБ.

В случае, если имеются два и более контроллера домена в одном домене, на каждом из которых установлен СЗИ Dallas Lock 8.0, все они находятся под управлением СБ, и создается пользователь на одном из них, то при попытке создать нового пользователя с тем же именем на другом контроллере домена — он будет добавлен из глобального списка.

При изменении свойств пользователя (кроме включения/исключения из групп пользователей), необходимо выполнить синхронизацию учетных записей между СБ и тем клиентом, для которого включен соответствующий пользователь.

При удалении учетной записи в КСБ Dallas Lock 8.0 на контроллере домена данная учетная запись удаляется в глобальном каталоге AD.

Блокировка/активация учетной записи пользователя в КСБ производится в режиме скрытого ОУ и

влечет отключение учетной записи на контроллере домена.

Уполномоченный пользователь может перейти к просмотру списка групп по нажатию кнопки «Группы AD» (рис. 426).

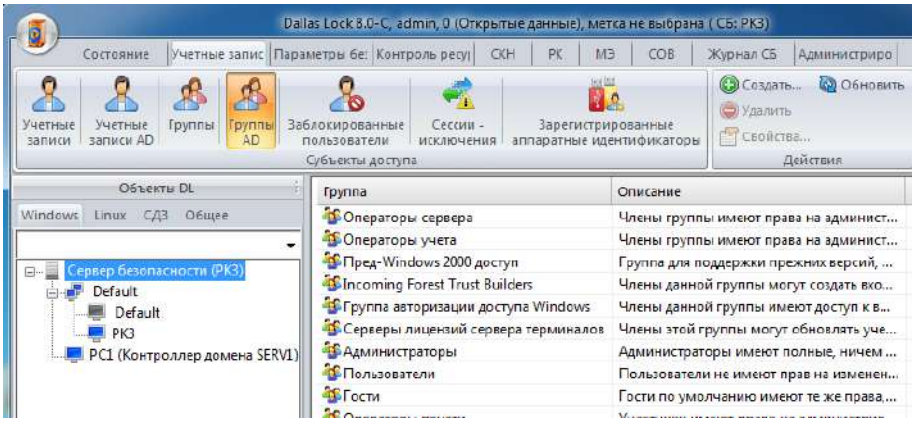


Рис. 426. Просмотр списка групп домена AD

Зарегистрированные аппаратные идентификаторы

Просмотр списка аппаратных идентификаторов, назначенных пользователям, доступен в категории «Зарегистрированные аппаратные идентификаторы» (рис. 427). При этом для просмотра данной категории пользователю должна быть назначена роль с привилегией «просмотр учетных записей (сессий, групп) и их настроек» (см. «Ролевая модель учетных записей СБ»).

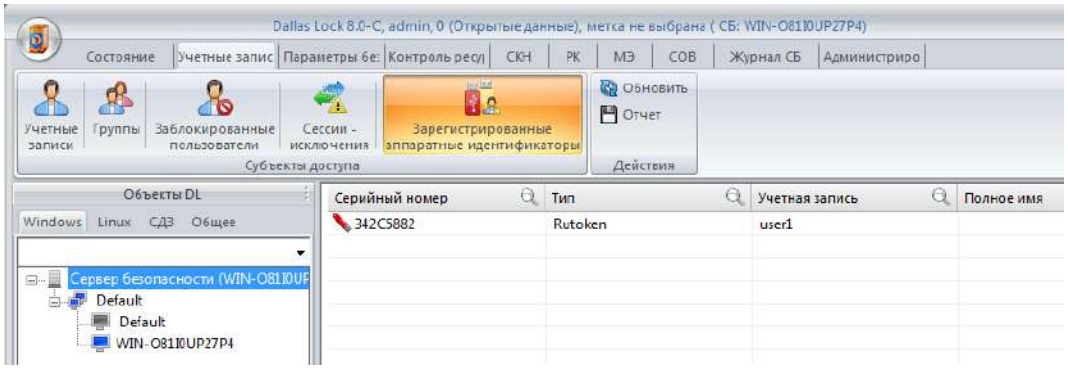


Рис. 427. Зарегистрированные аппаратные идентификаторы

На уровне СБ отображается список всех аппаратных идентификаторов ДБ. На уровне группы клиентов отображаются аппаратные идентификаторы пользователей, зарегистрированных на клиентах, входящих в данную группу.

Для формирования отчета по отображенным аппаратным идентификаторам необходимо нажать кнопку «Отчет». В отчете указывается серийный номер и тип аппаратного идентификатора, учетная запись, полное имя пользователя и владелец учетной записи, которой он назначен. Отчет формируется в формате TXT (текст, видимый на экране или с разделителем-табуляцией), CSV, HTML или XML.

Для обновления списка аппаратных идентификаторов необходимо нажать кнопку «Обновить».

Параметры безопасности домена

Вкладка «Параметры безопасности домена» позволяет редактировать параметры на уровне всего ДБ, после синхронизации на всех клиентах в ДБ применятся установленные настройки (рис. 428).

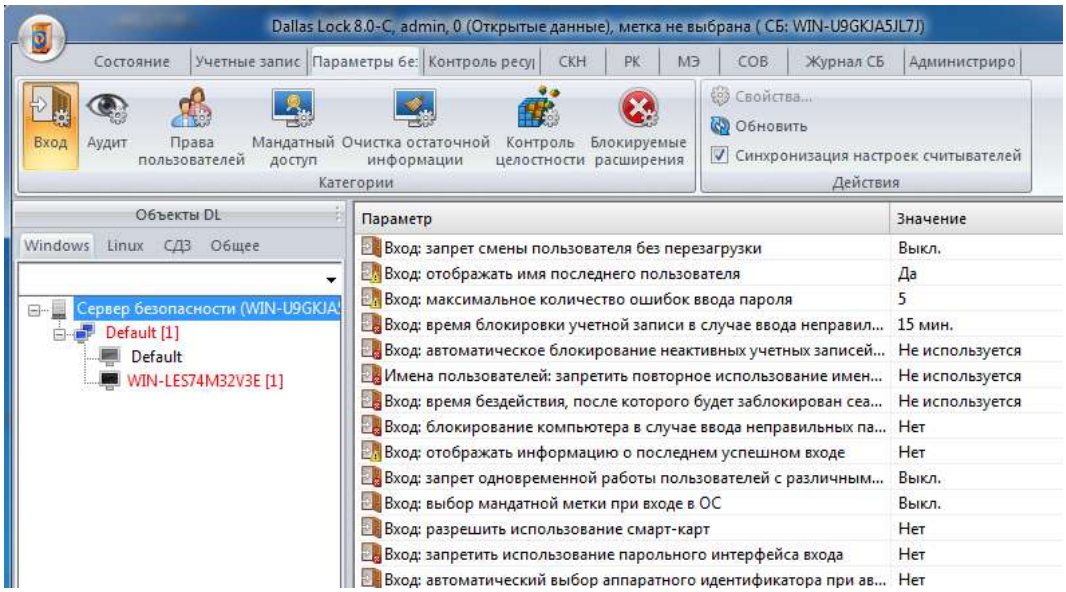


Рис. 428. Вкладка Параметры безопасности КСБ

Примечание. Существуют ограничения возможности переопределения политик ДБ. Следующие параметры могут переопределяться только на уровне ДБ (т. е. их нельзя переопределить для группы):

- «Сеть: Ключ защиты сетевого взаимодействия»;
- «Сеть: Список защищенных серверов»;
- «Настройка считывателей аппаратных идентификаторов»;
- «Текст сообщения при входе»;
- «Печать/редактировать штамп»;
- «Выгрузка журналов»;
- «Максимальное кол-во записей в журналах».

Доступны следующие категории.

Вход
Настройки входа будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Параметры входа»). Для того, чтобы при синхронизации на клиентах автоматически регистрировались считыватели аппаратных идентификаторов, необходимо их зарегистрировать на СБ и отметить поле «Синхронизация настроек считывателей». Обязательным условием является предварительная установка драйверов идентификаторов на необходимых клиентах. **Внимание!** Политика «Сеть: Ключ защиты сетевого взаимодействия» не синхронизируется с клиентами ДБ. При её изменении в СБ возможна потеря связи с клиентами из-за несовпадения ключей защиты сетевого взаимодействия (см. «Ключи защиты сетевого взаимодействия»). При этом политика «Сеть: Ключ защиты сетевого взаимодействия», установленная на уровне ДБ, используется при создании msi-файла для централизованной установки средствами СБ (см. «Подготовка msi-файла»).
Аудит
Настройки аудита будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Параметры аудита»).
Права пользователей
Настройки прав пользователей будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Полномочия пользователей на администрирование системы защиты» и «Разрешение и запрет интерактивного и удаленного входов в ОС»).

Внимание! При разрешенной для пользователя политике «Изменение системного времени и часового пояса» у данного пользователя появляется возможность для обхода рамок времени работы, установленных администратором. Политика «Изменение системного времени и часового пояса» позволяет запретить пользователям устройств, входящих в состав ДБ, изменять установленные дату и время, чтобы избежать возможные нарушения правил времени работы пользователей, групп пользователей.

Мандатный доступ

Настройки мандатного доступа будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Переименование уровней доступа и мандатных меток»).

Очистка остаточной информации

Настройки очистки остаточной информации будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Очистка остаточной информации»).

Контроль целостности

Настройки контроля целостности будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Настройка параметров контроля целостности»).

Блокируемые расширения

Настройки блокируемых расширений будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Блокировка работы с файлами по расширению»).

Контроль ресурсов домена

Вкладка «Контроль ресурсов домена» позволяет редактировать параметры на уровне всего ДБ, после синхронизации на всех клиентах в ДБ применятся установленные настройки (рис. 429).

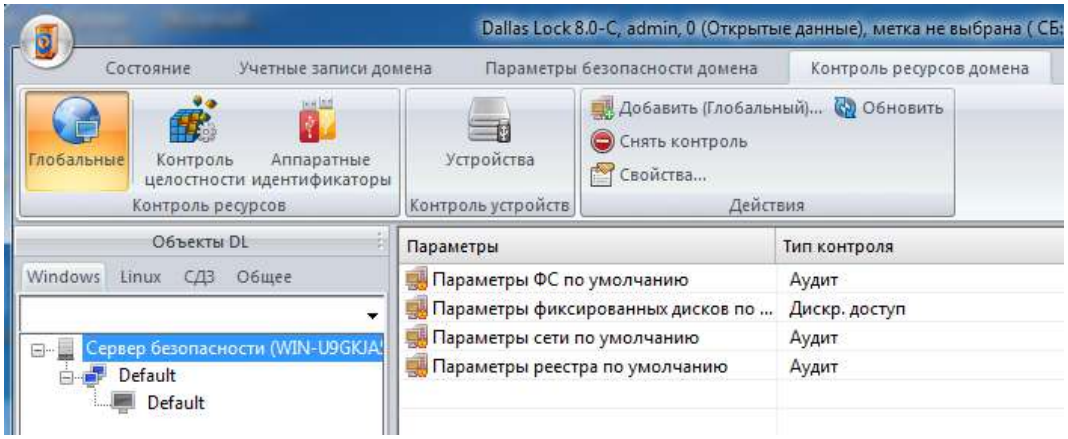


Рис. 429. Параметры контроля доступа

Доступны следующие категории.

Контроль доступа глобальных параметров ФС

Настройки для глобальных параметров контроля ФС будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Дискреционный доступ для глобальных параметров» и «Аудит глобальных параметров»).

Контроль целостности ДБ

Настройка контроля целостности для всего ДБ (см. «Контроль целостности ДБ»).

Контроль доступа к аппаратным идентификаторам

Настройки контроля доступа к зарегистрированным аппаратным идентификаторам для всего

ДБ. Для создания и настройки дескрипторов для всего ДБ пользователю должна быть назначена роль с привилегией «действия с ресурсами», а для просмотра – «просмотр списков контролируемых ресурсов и их параметров» в ветке привилегий «Контроль ресурсов».

Редактирование параметров дескриптора доступно только на том уровне, на котором он был создан.

Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Дискреционный доступ к аппаратным идентификаторам»). Для сохранения настроек необходимо нажать кнопку «Сохранить» в панели «Действия и параметры».

Контроль доступа к устройствам

Настройки доступа к устройствам будут установлены для всего ДБ. Данные настройки задаются только на уровне классов устройств аналогично тому, как это осуществляется с помощью оболочки администратора (см. «Разграничение доступа к устройствам»). Чтобы настроить доступ к конкретным устройствам, необходимо подключиться к включенному клиенту из КСБ, и перейти на вкладку клиента «Контроль устройств», далее выполнить настройки аналогично локальному администрированию в оболочке администратора (см. «Разграничение доступа к устройствам»).

Контроль целостности ДБ

С помощью СБ возможно централизованное управление контролем целостности на клиентах ДБ.

Данный механизм работает следующим образом. Первоначально на СБ настраивается список объединений. Объединение — это группа дескрипторов КЦ, которые будут назначены для объектов ФС клиентов ДБ. При синхронизации, на клиентах создаются дескрипторы КЦ для соответствующих объектов ФС.

Внимание! Если при синхронизации некоторые объекты ФС из объединений СБ отсутствуют в ФС клиента, то данные объекты игнорируются. При этом в «Журнал ресурсов» клиента регистрируется ошибка о создании дескриптора.

Поэтому для работы данного механизма, необходимо предварительно выделить группы клиентов с полным или частичным совпадением ПО, его конфигурации и данных.

Необходимость пересчета КС, если ее определил администратор СБ, доводится до клиентов в рамках синхронизации.

Внимание! Если в ДБ имеются клиенты с версией ОС различной разрядности, то необходимо создать группы дескрипторов КЦ для каждой разрядности.

Список объединений общий для всего ДБ формируется в категории «Контроль ресурсов домена» → «Контроль целостности» (рис. 430).

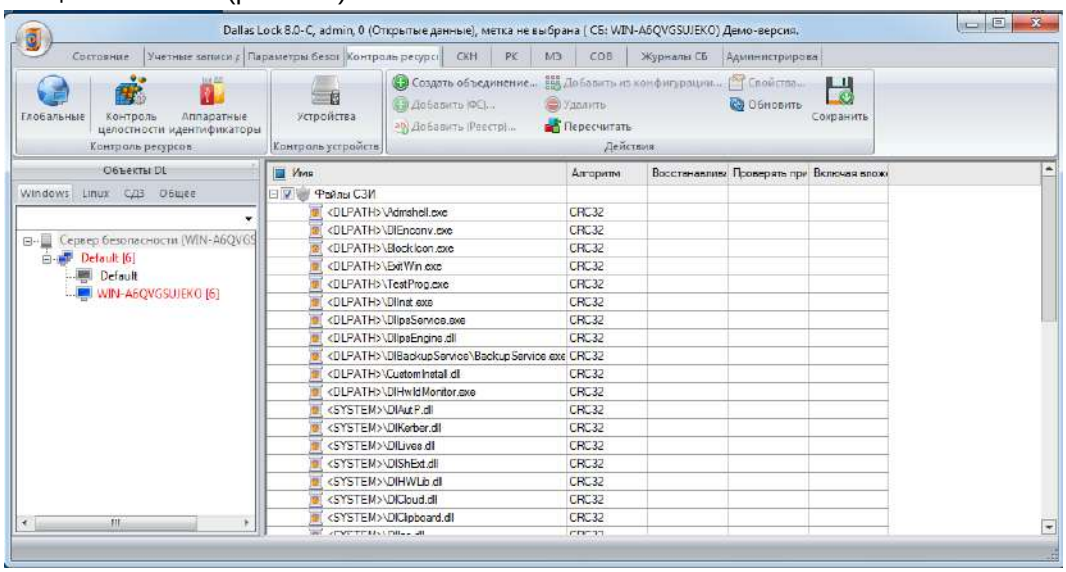


Рис. 430. Вкладка Контроль ресурсов КСБ

По умолчанию в СБ создано объединение «Файлы СЗИ», куда входят все необходимые дескрипторы КЦ для работы Dallas Lock 8.0.

Для упрощения работы АИБ возможно загрузить уже готовый список дескрипторов используя сохраненную конфигурацию Dallas Lock 8.0. Для этого необходимо:

1. Разместить на компьютере, на котором запущена КСБ, конфигурационный файл Dallas Lock 8.0.
2. На уровне СБ открыть категорию «Контроль ресурсов домена» → «Контроль целостности» и нажать кнопку «Создать объединение».
3. Ввести имя нового объединения и нажать кнопку «ОК».
4. Выделить созданное объединение и нажать кнопку «Добавить из конфигурации».
5. Найти и выбрать в проводнике конфигурационный файл и нажать кнопку «Открыть».
6. После применения конфигурационной файла появится отчет, в котором можно ознакомиться со списком дескрипторов КЦ добавленных в объединение.

Пример. Для создания нового объединения дескрипторов необходимо:

1. На уровне СБ открыть категорию «Контроль ресурсов домена» → «Контроль целостности» и нажать кнопку «Создать объединение».
2. Ввести имя нового объединения и нажать кнопку «ОК».
3. Выделить созданное объединение и нажать кнопку «Добавить (ФС)…» или «Добавить (Реестр)…».
4. Выбрать компьютер, ФС которого будет использоваться. Для выбора доступны ФС СБ и всех клиентов ДБ.
5. Далее, как в проводнике Windows необходимо найти нужный объект ФС или выбрать ветку реестра и нажать кнопку «Выбрать» или «Принять». Для выбранного объекта откроется окно дескриптора.
6. В окне дескриптора выбрать вкладку «Контроль целостности» (рис. 431).

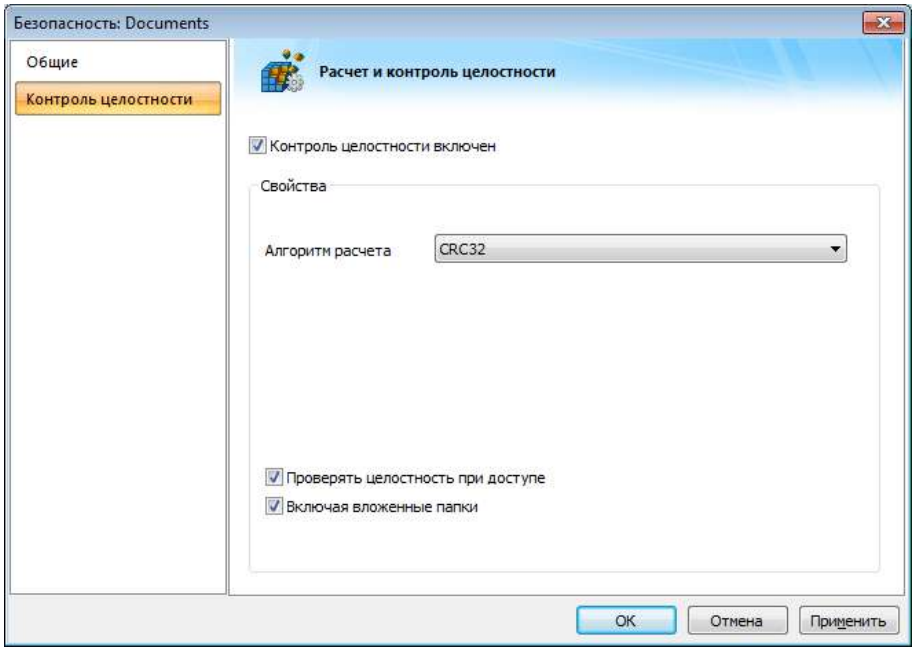


Рис. 431. Назначение прав дискреционного доступа

7. Отметить флагом «Контроль целостности включен» и выбрать алгоритм расчета контрольной суммы (CRC32, Хэш ГОСТ Р 34.11-94, Хэш MD5).
8. При необходимости нужно отметить следующие параметры для следующих объектов:
   - **Для файлов —** «Проверять контроль целостности при доступе» и «Восстанавливать в случае нарушения целостности». При попытке доступа к файлу, у которого нарушена целостность, но отмечено поле «Проверять контроль целостности при доступе», ПК пользователя заблокируется (при условии, что в свойствах учетной записи включен параметр «Запретить работу при нарушении целостности»). Правило распространяется и для веток реестра.
   - **Для папок** — «Проверять целостность при доступе» и «Включая вложенные папки». Если поле «Включая вложенные папки» не отмечено, то контроль целостности будет распространяться только на содержимое корневой папки. Изменение содержимого

вложенных папок к нарушению целостности не приведет. Если данное поле отмечено, то помимо корневой папки, на которую назначен контроль целостности, он будет распространяться и на содержимое внутренних (вложенных) папок. Правило распространяется и для веток реестра.

- **Для веток реестра** — «Включая вложенные ветки» и «Восстанавливать в случае нарушения целостности».

9. Нажать кнопку «ОК».

Объект, для которого будет создан дескриптор КЦ, автоматически появится в созданном объединении.

Для пересчета контрольных сумм объектов ФС на всех клиентах ДБ необходимо нажать кнопку «Пересчитать» и выполнить синхронизацию с клиентами.

После создания объединений, они автоматически появляются в списках объединений объектов ДБ: каждой группы (подгруппы) клиентов и каждого клиента.

Для каждой группы (подгруппы) клиентов и для каждого клиента возможно индивидуально определить, какие объединения (группы дескрипторов) из списка создадутся на данных клиентах, а какие нет.

Для того, чтобы отметить объединение для создания на клиентах во всем ДБ, необходимо поставить флаг для объединения. Объединение будет отмечено флагом для всех клиентов и групп клиентов. Для того, чтобы удалить объединение (группу дескрипторов) на всех клиентах ДБ, необходимо снять флаг рядом для объединения.

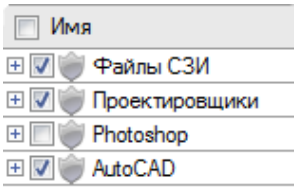


Рис. 432. Создание пользователя в ДБ

На всех клиентах, входящих в ДБ, отмеченные объединения будут идентичны.

Настройка контроля целостности для групп и подгрупп клиентов описана в разделе «Контроль ресурсов группы».

Настройка контроля целостности для клиентов описана в разделе «Контроль ресурсов клиента».

Обновление ПО и его контрольных сумм

Для обновления ПО и его контрольных сумм, на клиентах необходимо выполнить следующие действия:

1. Включить «неактивный режим» в части контроля целостности на клиентах, для которых будет выполнено обновление ПО. Для включения «неактивного режима» для группы клиентов, необходимо на уровне группы открыть вкладку «Состояние» и нажать кнопку «Неактивный режим…» (рис. 433).

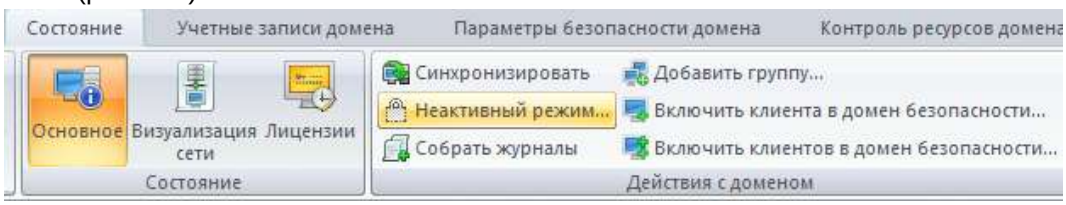


Рис. 433. «Неактивный режим» для группы клиентов

В окне «Настройка неактивного режима» установить флаги «Неактивный режим включен» и «Контроль целостности» и нажать кнопку «ОК» (рис. 434).

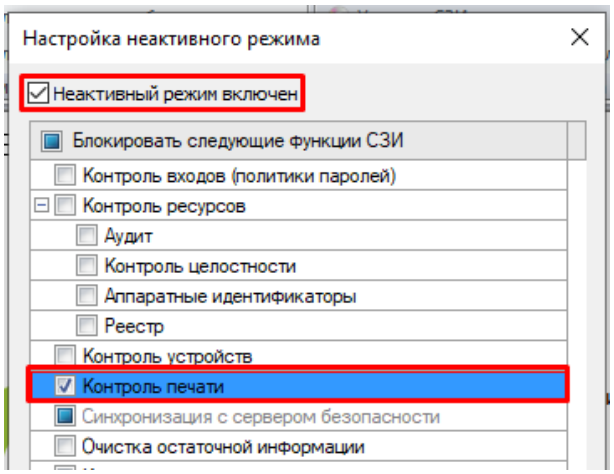


Рис. 434. Настройка «неактивного режима»

Далее выполнить синхронизацию клиентов.

2. Обновить ПО на клиентах.
3. Произвести пересчет контрольных сумм объектов ФС клиентах с обновленным ПО. Для группы клиентов необходимо на уровне группы открыть категорию «Контроль ресурсов домена» → «Контроль целостности», нажать кнопку «Пересчитать» и выполнить синхронизацию с клиентами.
4. Выключить «неактивный режим» на клиентах с обновленным ПО.
5. Добавить новые дескрипторы в объединения при необходимости.

Доменные настройки СКН

Управление сменными накопителями ДБ

Для удобства работы назначение дескрипторов для объектов ФС (файлов и папок) на сменных накопителей выделено в отдельную категорию «Сменные накопители».

С помощью СБ возможно централизованное управление данным списком. Список установленных дескрипторов на ресурсы ФС сменных накопителей общий для всего ДБ формируется в категории «СКН» → «Сменные накопители».

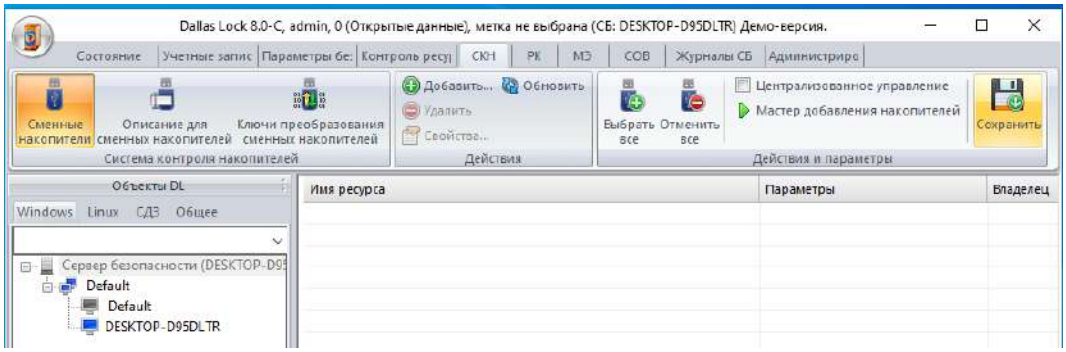


Рис. 435. Сменные накопители ДБ

Управление списком дескрипторов сменных накопителей для ДБ включается в себя следующие действия:

1. Формирование списка дескрипторов. Установка дескрипторов на сменные накопители (необходимые права доступа для необходимых учетных записей, аудит, контроль целостности объектов ФС) с помощью КСБ имеет тот же механизм, что и в оболочке администратора. Список дескрипторов автоматически обновляется для всех клиентов и групп клиентов.
2. Индивидуальная настройка списка **для каждой группы и подгруппы клиентов, а также самих клиентов.** Открывая для каждого объекта вкладку «Сменные накопители», необходимо выбрать, какие дескрипторы необходимы для работы на клиентах.

Имя ресурса	Параметры
[Флешка Савельева Н.В.]:\Ком. предложение	Аудит;
[Флешка Савельева Н.В.]:\HPSCANS	Аудит;
[Флешка Савельева Н.В.]:\DL80C Анонс.docx	Мандатн. доступ;
Flash(BD3A59E4-B4FE5315):\	Аудит;
Flash(BD3A59E4-B4FE5315):\setup.exe	Дискр. доступ;

Рис. 436. Выбор дескрипторов на сменных накопителях для установки на клиенте

3. Задание режима управления сменными накопителями: централизованного или локального:

- Если выбран централизованный режим (отмечено поле «Включить централизованный режим»), то в процессе синхронизации у клиентов, у которых также выбран режим централизованного управления, отмеченные дескрипторы создадутся, а не отмеченные — удалятся. Если на клиенте имелись локально созданные дескрипторы, которые не совпадали с дескрипторами, созданными в ДБ для данного клиента, то в процессе синхронизации с СБ, эти ключи будут удалены.
- Если режим централизованного управления не включен (поле не отмечено), то синхронизации дескрипторов не произведется, но останется возможность редактирования списка дескрипторов сменных накопителей СБ. Это необходимо для независимого от настроек СБ управления списком дескрипторов, подключившись к защищенному ПК в режиме ОУ с помощью функции сетевого администрирования (см. «Сетевое администрирование»).

После определения списка дескрипторов накопителей на вкладке «Сменные накопители» клиентов в настройках групп и подгрупп клиентов поля с дескрипторами будут принимать следующий вид:

☑ — отмеченное флагом поле означает, что дескриптор установлен на всех клиентах в группе (подгруппе);

■ — затемненное поле означает неопределенность, дескриптор установлен на одних и не установлен на других клиентах;

☐ — пустое поле означает, что дескриптор не установлен ни на одном клиенте.

Также с помощью СБ возможна централизованная установка описания для сменных накопителей (см. «Описание для сменных накопителей»). Присвоенное для накопителя описание на СБ, будет единственным во всем ДБ и при синхронизации установится на всех клиентах ДБ.

Управление ключами преобразования ДБ

Механизм преобразования сменных накопителей подробно описан в главе «Преобразование сменных накопителей».

Работа с преобразованными накопителями возможна только на тех ПК, которые защищены Dallas Lock 8.0, и на которых установлен ключ преобразования аналогичный тому, которым преобразование было выполнено. При невыполнении этих условий доступ к накопителю будет заблокирован.

С помощью СБ возможно централизованное управление списком ключей преобразования для клиентских ПК: создание, редактирование, удаление ключей, формирование списка ключей, для работы на клиентах.

Список ключей преобразования сменных накопителей общий для всего ДБ формируется в категории «СКН» → «Ключи преобразования сменных накопителей» (рис. 437).

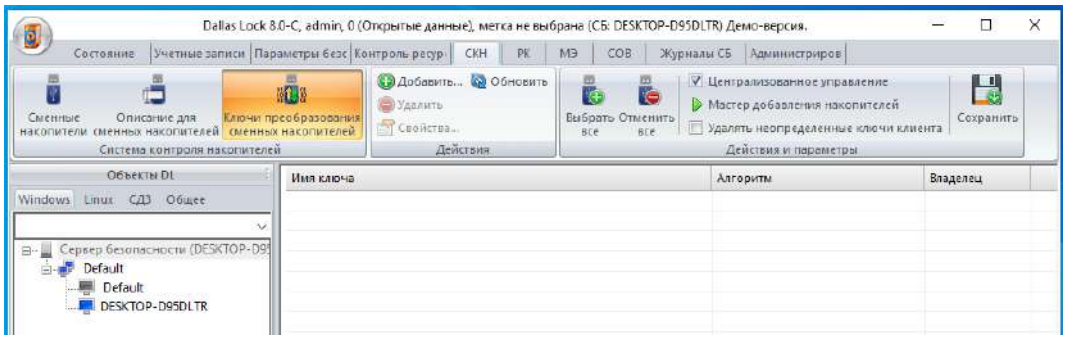


Рис. 437. Настройка ключей преобразования накопителей в ДБ

Управление списком ключей преобразования для ДБ включает в себя следующие действия (параллельные или последовательные):

1. Создание ключей преобразования. Создание ключей преобразования с помощью КСБ имеет тот

же механизм, что и в оболочке администратора. Созданный список ключей преобразования автоматически обновляется для всех клиентов и групп клиентов.

2. Индивидуальная настройка списка **для каждой группы и подгруппы клиентов, а также самих клиентов**. Открывая для каждого объекта вкладку «Ключ преобразования», необходимо выбрать, какие ключи преобразования необходимы для работы на клиентах.
3. Задание режима управления ключами преобразования: централизованного или локального:
   - Если выбран централизованный режим управления (отмечено поле «Включить централизованный режим»), то в процессе синхронизации клиентов, у которых также выбран режим централизованного управления, отмеченные ключи создадутся (станут активны, если ранее были созданы), а не отмеченные — заблокируются (переведутся в неактивное состояние). Если на клиенте имелись локально созданные ключи преобразования, которые не совпадали с ключами, созданными в ДБ для данного клиента, то в процессе синхронизации с СБ, эти ключи будут отключены.
   - Если режим централизованного управления не включен (поле не отмечено), то синхронизации ключей преобразования не произведется, но останется возможность редактирования списка ключей преобразования СБ. Это необходимо для независимого от настроек СБ управления списком ключей преобразования, подключившись к защищенному ПК в режиме ОУ с помощью функции сетевого администрирования (см. «Сетевое администрирование»).
4. Задание удаления неопределенных ключей клиента. Если на клиенте имелись локально созданные ключи преобразования, которые не совпадали с ключами, созданными в ДБ для данного клиента, то в процессе синхронизации они будут удалены.

После редактирования списка ключей преобразования в настройках групп и подгрупп клиентов поля «Включить централизованное управление» и «Удалять неопределенные ключи клиента» могут принимать следующий вид:

☑ — отмеченное флагом поле означает, что параметр включен на всех клиентах и на всех группах в ДБ;

■ — затемненное поле означает неопределенность, параметр включен на одних и выключен на других клиентах или группах в ДБ;

☐ — пустое поле означает, что параметр отключен во всем ДБ.

Список ключей для работы на клиентах применится после синхронизации. В локальной оболочке администратора клиента на вкладке «Параметры безопасности» → «Преобразование сменных накопителей» появится обновленный список ключей.

Доменные настройки РК

Вкладка доменных настроек резервного копирования (рис. 438) позволяет производить операции с заданиями на всех уровнях (СБ, группы и клиента). Переключение между уровнями позволяет отфильтровать отображение уже созданных заданий. На уровне СБ отображаются задания, имеющиеся во всем ДБ, на уровне группы — имеющиеся в рамках выбранной группы.

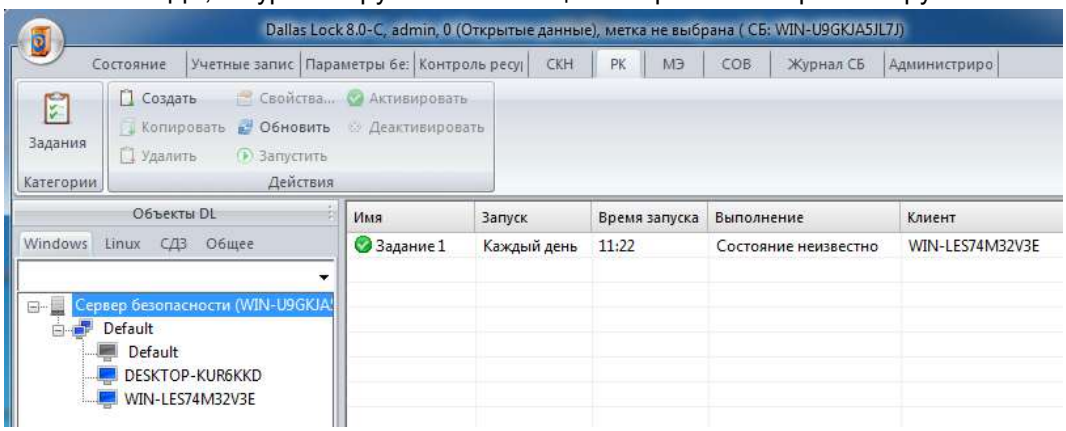


Рис. 438. Доменные настройки РК

Для создания нового задания необходимо:

1. Выбрать объект в дереве «Объекты DL» и нажать кнопку «Создать» в панели «Действия» или в контекстном меню в рабочей области. В случае, если объект выбран не будет, мастер создания заданий будет открыт с дополнительной вкладкой «Клиенты», на которой необходимо будет выбрать клиента(-ов), для которых настраивается задание по резервному копированию

(рис. 439).

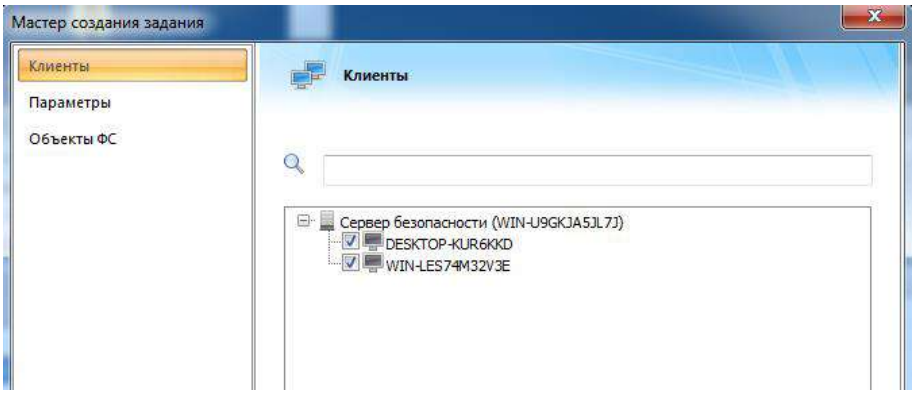


Рис. 439. Мастер создания заданий. Выбор клиента

2. Перейти на вкладку «Параметры» и осуществить настройку задания аналогично тому, как это делается в оболочке администратора (см. «Эксплуатация»).

   При настройке параметров необходимо убедиться, что учетная запись, из-под которой планируется проводить резервное копирование объектов ФС, наделена соответствующими правами доступа к клиентским машинам.

3. Перейти на вкладку «Объекты ФС» для выбора объектов ФС, подлежащих резервному копированию (рис. 440).

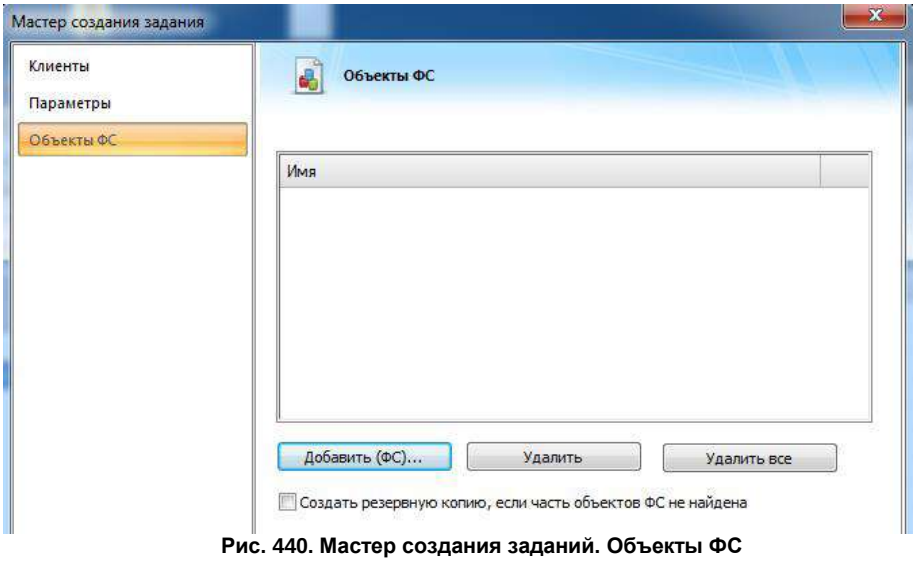


Рис. 440. Мастер создания заданий. Объекты ФС

Нажать кнопку «Добавить (ФС)…». Далее необходимо предварительно выбрать клиента, на котором располагается объект ФС. Для этого необходимо нажать на кнопку рядом с полем в левой верхней части открывшегося окна (рис. 441). В случае, если клиентский компьютер выбран не будет, задание будет установлено для объектов ФС, доступных на компьютере с установленным СБ, либо сетевом хранилище.

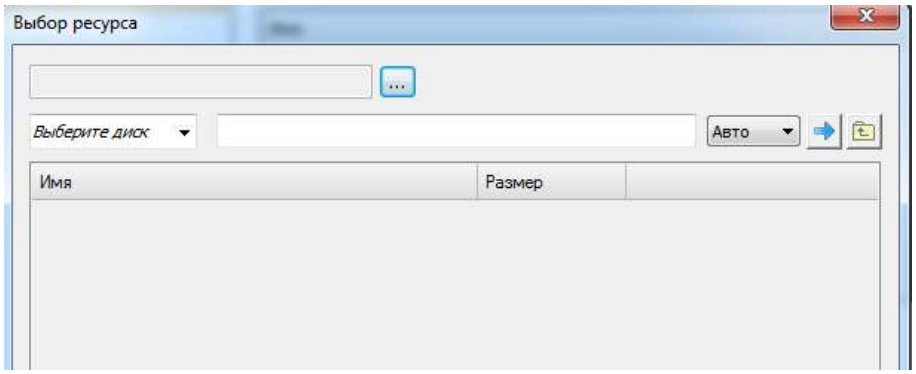


Рис. 441. Окно «Выбор ресурса»

В открывшемся диалоговом окне «Выбор клиентского компьютера» необходимо найти в списке, выбрать клиентский компьютер и нажать кнопку «ОК» (рис. 442). Для поиска можно воспользоваться поисковой строкой.

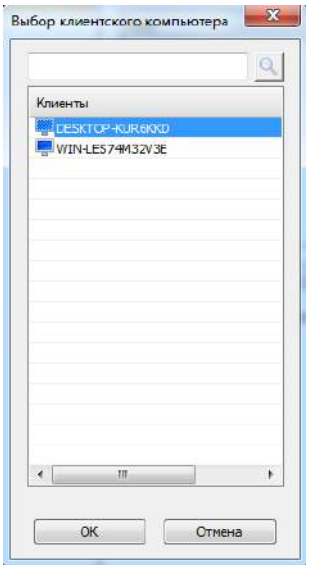


Рис. 442. Выбор клиентского компьютера

Затем необходимо указать путь к объекту ФС и нажать кнопку «ОК. Повторить данную процедуру для всех клиентов, на которых необходимо установить данное задание по резервному копированию.

Установить флаг в поле «Создать резервную копию, если часть объектов ФС не найдена» — в таком случае, резервная копия будет создаваться для всех обнаруженных объектов ФС, которые определены для резервного копирования. Если часть объектов окажется недоступна, в графе «Выполнение» в рабочей области будет отображен статус процесса «Архивирование выполнено частично».

В случае, если не обнаруживается ни одного из выбранных объектов ФС, процедура завершится ошибкой, а в графе «Выполнение» будет отображен статус процесса «Ошибка архивирования».

Функции копирования, удаления, просмотра свойств, обновления, запуска, активации и деактивации работают аналогично тому, как это описано для оболочки администратора (см. «Эксплуатация»).

Для просмотра списка заданий с клиентского компьютера необходимо обновить список заданий и перезапустить оболочку администратора.

Доменные настройки МЭ

Вкладка доменных настроек МЭ позволяет редактировать параметры МЭ, а также просматривать статистику МЭ на уровне всего ДБ, после синхронизации на всех клиентах в ДБ применятся установленные настройки (рис. 443).

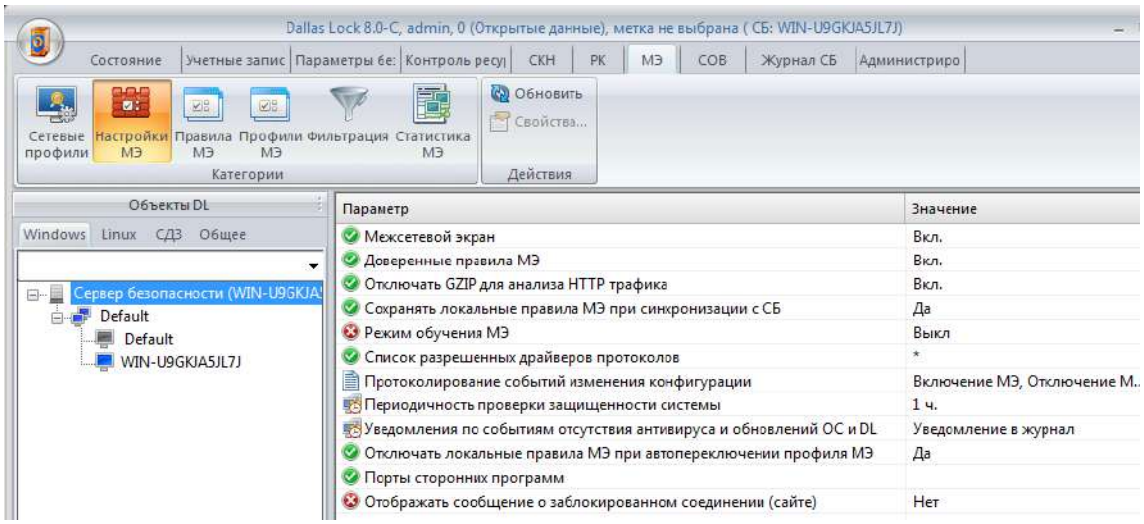


Рис. 443. Доменные настройки МЭ

Доступны следующие категории.

Сетевые профили
Настройки сетевых профилей будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Сетевые

профили»).
Настройки МЭ
Настройки межсетевого экрана будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Параметры»).
Правила МЭ
Настройки правил МЭ будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Правила МЭ»). Также доступно импортирование в СБ список правил МЭ клиента (см. «Импорт правил МЭ»).
Профили МЭ
Настройки профилей МЭ будут установлены для всего ДБ. На уровне СБ настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Правила МЭ»). На уровне групп дерева КСБ доступны дополнительные параметры (см. «Доменные настройки профилей МЭ на уровне групп»).
Фильтрация
Настройки фильтрации будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Фильтрация»).
Статистика МЭ
Статистика межсетевого экрана с клиентов всего ДБ. Отображаемая статистика аналогична отображаемой статистике в оболочке администратора за исключение диаграммы, отображающей статистику всего входящего/исходящего трафика (для ДБ диаграмма не строится) (см. «Статистика МЭ»).

Доменные настройки профилей МЭ на уровне групп

На уровне групп (подгрупп) возможно переключение текущего профиля и управление автовыбором профилей с помощью панели «Действия» в категории «Профили МЭ» (рис. 444).

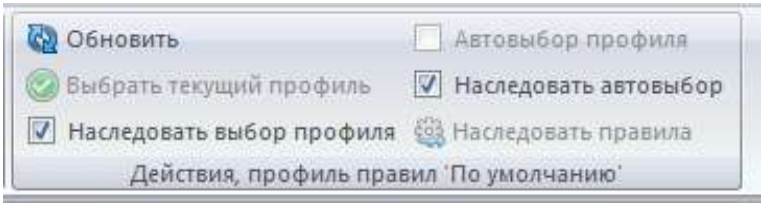


Рис. 444. Панель «Действия» на уровне группы

На панели «Действия» на уровне групп и подгрупп присутствует параметр «Наследовать выбор профиля», предназначенный для наследования текущего профиля МЭ у вышестоящего объекта дерева КСБ. При включенном значении данного параметра, ручное переключение профилей МЭ недоступно. По умолчанию параметр включен.

Статусы правил МЭ наследуемого профиля не наследуются.

Также доступен параметр «Наследовать автовыбор», предназначенный для наследования текущего значения параметра «Автовыбор профиля» у вышестоящего объекта дерева КСБ. При включенном значении данного параметра, смена значения параметра «Автовыбор профиля» недоступна. По умолчанию параметр включен.

При срабатывании событий, все действия происходят локально на клиентах.

Для просмотра в журнале СБ событий, связанных с автоматическим выбором профилей МЭ нужно на уровне СБ в категории «Журнал СБ» → «Настроить фильтр…» → «События НСД» → «Применить фильтр». При этом автоматически выбирается из списка событие «Переключение профиля МЭ» (рис. 445).

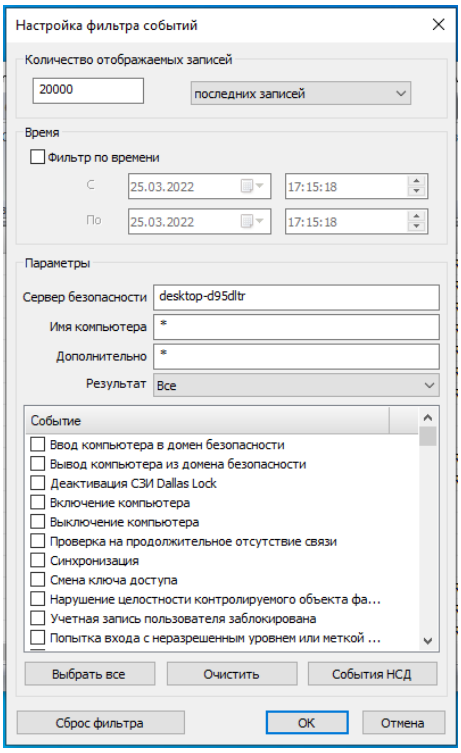


Рис. 445. Настройка фильтра событий

Импорт правил МЭ

СБ содержит общий список правил МЭ. Общий список правил МЭ — это эталонные правила МЭ для всего ДБ.

Существует возможность импортировать правила МЭ с клиента в общий список правил МЭ. Для этого необходимо:

1. На уровне СБ открыть категорию «МЭ» → «Правила МЭ» и нажать кнопку «Импортировать».
2. Выделить клиента, правила МЭ которого необходимо импортировать в общий список правил МЭ СБ, и нажать «ОК».
3. Выбрать необходимые правила МЭ и нажать кнопку «Импорт».

Выбранные правила МЭ автоматически появится в общем списке правил МЭ на СБ.

Доменные настройки СОВ

Вкладка доменных настроек СОВ позволяет редактировать параметры СОВ, а также просматривать статистику СОВ на уровне всего ДБ, после синхронизации на всех клиентах в ДБ применятся установленные настройки (рис. 446).

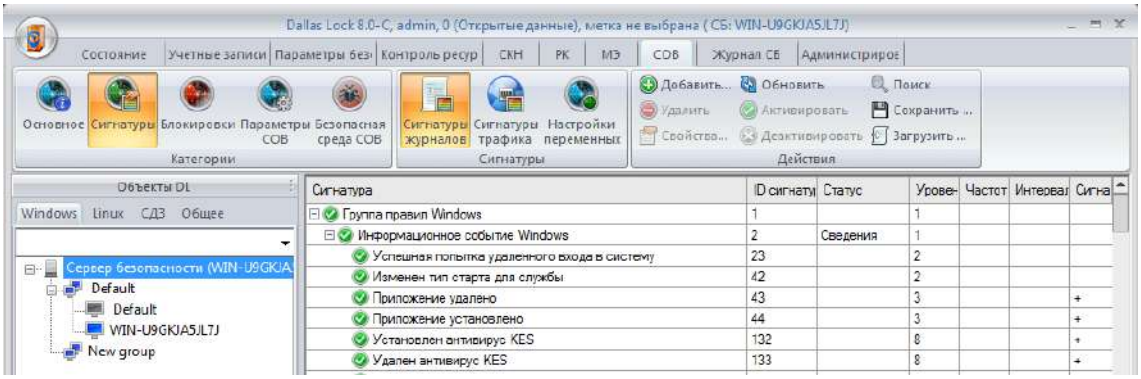


Рис. 446. Доменные настройки СОВ

Доступны следующие категории.

Основное
Информация и статистика системы обнаружения вторжений с клиентов всего ДБ. Подкатегория «Сетевые атаки» отображает список сетевых атак и их количество,

произошедших за сутки, неделю, месяц или весь период работы Dallas Lock 8.0. Подкатегория «Сигнатуры трафика» отображает список сработавших сигнатур трафика и их количество за сутки, неделю, месяц или весь период работы Dallas Lock 8.0. Подкатегория «Подозрительная активность» отображает список зарегистрированных событий подозрительной активности выбранного пользователя и их количество за сутки, неделю, месяц или весь период работы Dallas Lock 8.0.
Сигнатуры
Настройки сигнатур будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Настройки сигнатур»).
Блокировки
Настройки блокировок будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Блокировки»).
Параметры СОВ
Параметры СОВ будут установлены для всего ДБ. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Параметры СОВ»).
Безопасная среда СОВ
Параметры СОВ, предназначенные для обеспечения возможности запуска стороннего ПО в изолированной, безопасной среде — песочнице (см. «Безопасная среда СОВ (песочница)»).

Журнал СБ

Вкладка «Журнал СБ» позволяет просматривать в **категории «Журнал СБ»** регистрируемые события, связанные непосредственно с работой СБ (рис. 447).

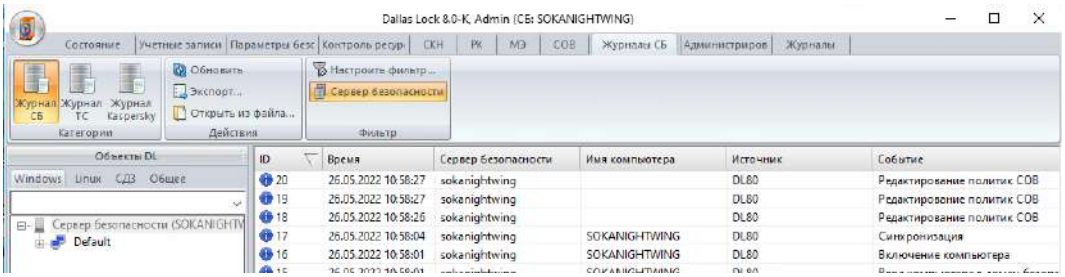


Рис. 447. Журнал СБ

Важно не путать журнал СБ с журналами клиентов (журнал входов, журнал управления учетными записями, журнал ресурсов, журнал печати, журнал управления политиками безопасности, журнал процессов, журнал резервного копирования и др.).

В журнал СБ регистрируются следующие события:

1. Ввод и вывод клиента из ДБ.
2. Синхронизация клиента. В поле «Дополнительно» заносятся данные о том, что именно было синхронизировано. Если в процессе синхронизации не понадобилось модифицировать какие-либо данные на клиенте, то такое событие в журнал не заносится.
3. Сбор журналов с клиентов.
4. Изменение ключа доступа.
5. Очистка журнала СБ.
6. Включение/выключение клиента.

Также в журнал СБ заносятся типы событий, при которых происходит событие сигнализации (воспроизводится звуковой сигнал и выводится сообщение):

1. Попытки входа на клиентскую рабочую станцию с неправильным паролем, неразрешенным уровнем доступа (только для Dallas Lock 8.0 редакции «С»).
2. Нарушение целостности ФС или программно-аппаратной среды клиентской рабочей станции.
3. Несанкционированная деактивация системы защиты.
4. Недоступность рабочей станции за определенный период и другие.

Если операция завершилась успешно, то соответствующая запись в журнале будет помечена значком синего цвета, если не успешно, то красного.

Панель «Действия» аналогична той, что есть в оболочке администратора: имеется возможность архивации записей, экспорта записей в файл в выбранном формате, настройка и применение фильтра, группировка записей (см. «Журналы»).

Подробнее о журналах, полученных с клиентов, см. «Журналы клиента».

Следует отметить, что на защищенном ПК в системной папке «C:\DLLOCK80» имеются следующие папки, содержащие журналы событий:

- Папка «Jrn» — папка с текущими журналами данной рабочей станции. Это те журналы, которые формируются и открываются с помощью вкладки «Журналы» оболочки администратора.
- Папка «Logs» — папка, хранящая сформированные автоматически при переполнении (>20000 записей) текущие журналы событий и журналы после их архивации данной рабочей станции, в том числе журнал СБ. А также, при установке на компьютер СБ, в папке «Logs» формируются папки с именами клиентских рабочих станций, в которых хранятся все собранные с клиентов журналы.
- В папке «DLSecServer» помимо установочных файлов СБ хранится текущий журнал данного СБ.

В **категории «Журнал ТС»** регистрируются события по работе с заявками пользователя в службу технической поддержки и информационные сообщения, отправленные производителем (рис. 448).

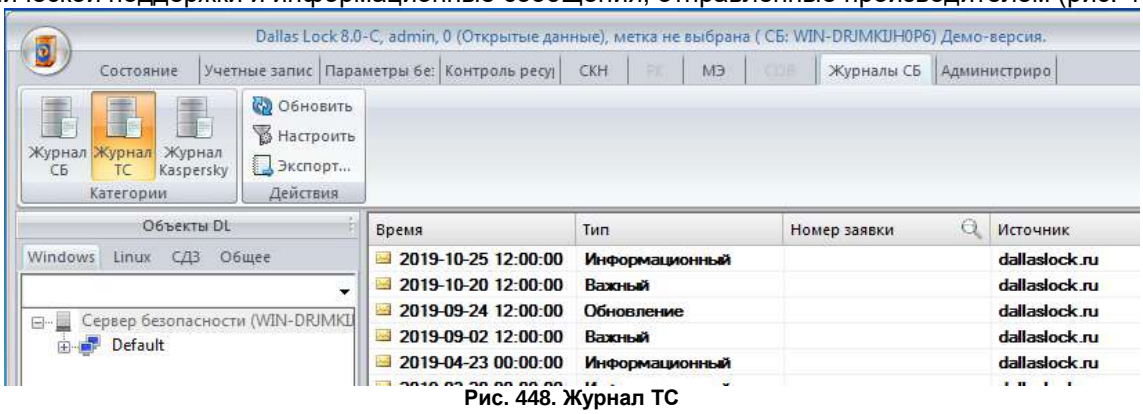


Рис. 448. Журнал ТС

При обращении пользователя в техническую поддержку через сайт производителя или соответствующую электронную почту ему необходимо указать:

- идентификационную информацию: номер лицензии СБ / номер лицензии клиентской части / код информационно-технического сопровождения (если используется в СБ);
- тему обращения.

По результатам обработки запроса в журнале появится соответствующее событие. При наличии интернет-соединения журнал обновляется каждые полчаса из базы данных СЗИ новостями, для которых установлен тип «Важные». Остальные типы сообщений, в том числе сообщения по заявкам заказчика, отображаются в журнале только после действий пользователя (вход в журнал, принудительное обновление с помощью кнопки «Обновить», открытие непрочитанного сообщения). При отсутствии подключения в журнале будут отображены только загруженные ранее сообщения.

Чтобы настроить тип получаемых сообщений, необходимо нажать кнопку «Настроить» в панели «Действия».

В открывшемся окне (рис. 449) представлены следующие типы сообщений:

- «Важный» — данный тип сообщений включает в себя важную информацию, касающуюся функционирования продукта. Является обязательным, нельзя отключить.
- «Техподдержка» — данный тип сообщений включает в себя информацию по работе с заявками пользователя. Является обязательным, нельзя отключить.
- «Информационный» — данный тип сообщений включает в себя информационные сообщения производителя, которые не отнесены в категорию «Важные».
- «Обновление» — данный тип сообщений включает в себя уведомления об обновлениях продукта.

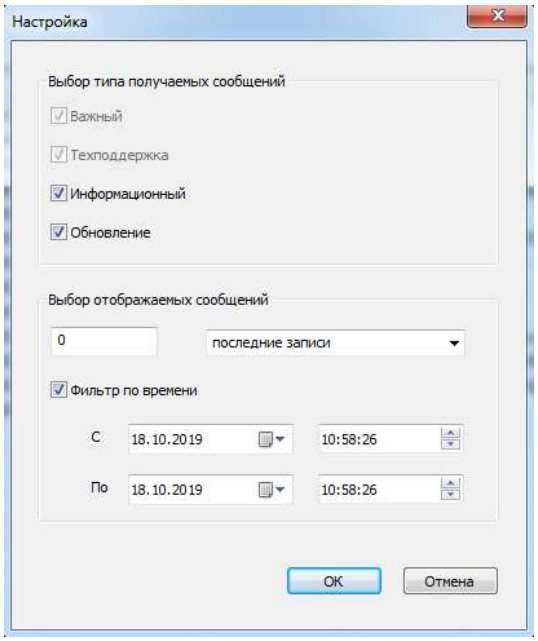


Рис. 449. Настройка получаемых сообщений

В данном окне также можно настроить фильтрацию отображаемых сообщений. Из выпадающего списка возможно указать количество отображаемых записей и выбрать, какие записи необходимо отобразить:

- все записи,
- первые записи,
- последние записи.

Также можно точно настроить фильтр по времени, указав диапазон дат и времени.

При установке СБ необходимо указать «Код активации технической поддержки», чтобы была возможна регистрация событий по работе с заявками пользователей в службу Технической поддержки. В противном случае в Журнале ТС будут регистрироваться только информационные сообщения, отправленные производителем.

Выбранные настройки реплицируются между СБ, находящимися в кластере, а также сохраняются в конфигурацию СБ.

Категория «Журнал Kaspersky» существует для фиксации событий, поступающих с KSC на СБ (Рис. 450).

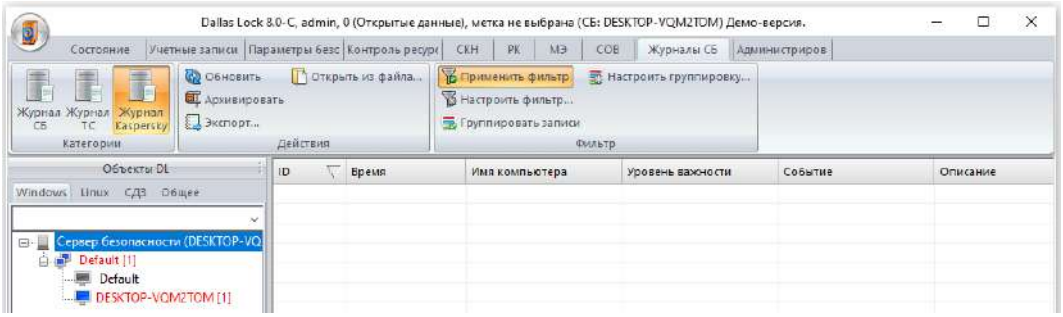


Рис. 450. Журнал Kaspersky

В СБ каждое событие, приходящее с KSC, имеет следующие атрибуты:

- ID;
- Время;
- Имя компьютера;
- Уровень важности (Информационное событие/Критический/Предупреждение/Отказ функционирования);
- Событие;
- Описание;
- Группа;
- Задача;
- Время регистрации;
- Имя виртуального сервера.

При нажатии на кнопку «Журнал Kaspersky» в верхней информационной панели отображаются кнопки:

1. Панель «Действия» с кнопками:

- «Обновить»;
- «Архивировать»;
- «Экспорт»;
- «Открыть из файла».

Действие кнопок панели «Действия» для категории «Журнал Kaspersky» аналогичны действиям кнопок панели «Действия» для категории «Журнал СБ».

2. Панель «Фильтр» с кнопками:

Использование фильтров дает возможность отсеять ненужные данные в журнале так, что они становятся невидимы при просмотре. В то же время информация при использовании фильтров из журналов не удаляется.
Чтобы произвести настройки в журнале, необходимо нажать кнопку «Настроить фильтр» и выбрать необходимые параметры фильтра в открывшемся окне, нажать «OK» (Рис. 451). После настройки необходимо нажать кнопку «Применить фильтр», после чего записи журнала будут отсортированы. Повторное нажатие «Применить фильтр» вернет полное содержание журнала.

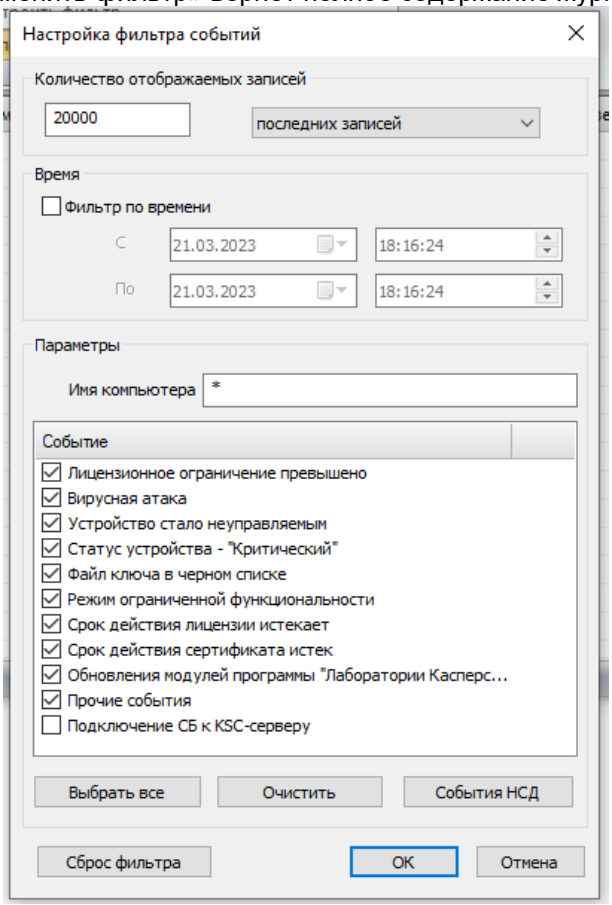


Рис. 451. Настройка фильтра событий

Чтобы настроить группировку записей в журнале, необходимо нажать «Настроить группировку» и выбрать необходимые параметры фильтра в открывшемся окне, нажать «OK» (Рис. 452). Для применения настроек группировки нажать на кнопку «Группировать записи».

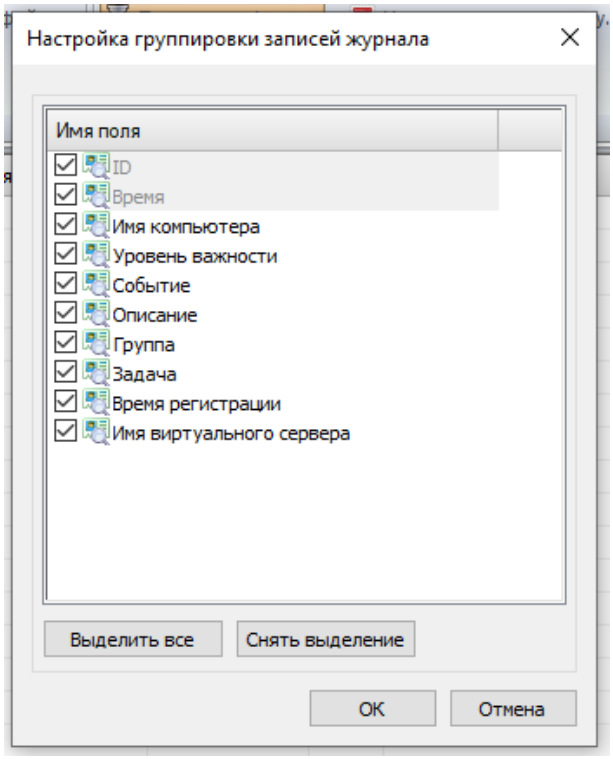


Рис. 452.Настройка группировки записей журнала

События, связанные с управлением KSC через OpenAPI, фиксируются «Журнале СБ». Регистрации подлежат следующие события:

- Подключение к KSC;
- Отключение от KSC;
- Сканирование клиентских АРМ;
- Обновление антивирусных баз.

Запись «Журнала Kaspersky» содержит следующие элементы:

- ID;
- Время;
- Имя компьютера;
- Уровень важности;
- Событие;
- Описание;
- Группа;
- Задача;
- Время регистрации;
- Имя виртуального сервера.

Журналы ДБ

Вкладка «Журналы» доступна только при использовании базы данных MS SQL Server. Она позволяет просматривать собранные СБ журналы со всех Windows клиентов ДБ.

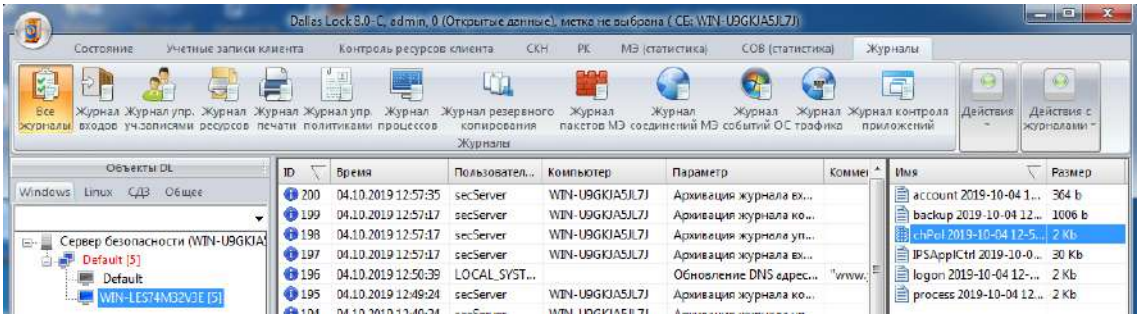


Рис. 453. Вкладка КСБ полученных с клиента журналов

В случае возникновении сбоя при сохранении данных аудита, собранные файлы журналов хранятся на СБ до тех пор, пока не будут загружены в БД. Зачистка файла журнала на клиенте выполняется только при успешной передаче файла СБ.

Формирование этих журналов и записей в них происходит на момент команды сбора журналов путем нажатия данной кнопки на вкладке «Состояние» клиента или на вкладке «Состояние» СБ, а также при настроенном периодическом сборе журналов в параметрах данного СБ.

Панель «Действия» аналогична той, что есть в оболочке администратора Dallas Lock 8.0: имеется возможность архивации записей, экспорта записей в файл в выбранном формате, настройка и применение фильтра, группировка записей (см. «Журналы»).

Примечание. С помощью клавиши «Delete» можно удалить файл журнала клиента в КСБ. Для этого выполнить следующее:

1. Выделить выбранный файл в журнале клиента и нажать клавишу «Delete».
2. Перед удалением файла из журнала пользователю выводится соответствующее сообщение.
3. При положительном ответе происходит удаление файла из журнала, при отрицательном операция будет отменена.

19.10.9 Клиенты и группы клиентов СБ

Группа Default и клиент Default

В дереве объектов КСБ всегда присутствуют группа «Default» и клиент «Default».

Примечание. При добавлении нового клиента в ДБ он всегда помещается в группу «Default» при следующих условиях:

1. Настройки безопасности для него копируются из настроек группы «Default».
2. Список учетных записей и ключей преобразования копируются из списка клиента «Default».

Создание группы клиентов возможно или на уровне родительского объекта «СБ» или на уровне родительского объекта «группа», поэтому:

1. При создании в дереве объектов новой группы на уровне СБ («Сервер безопасности» → «Добавить группу») для нее копируются параметры безопасности группы Default.
2. При создании новой группы как подгруппы (объект группы → «Добавить подгруппу») для нее копируются параметры безопасности родительской группы.

В дальнейшем, администратор СБ ЗАРМ может перенести нового клиента в любую другую группу, а также любую группу в качестве подгруппы в другую группу. Для этого можно воспользоваться контекстным меню («Переместить») или перетащить значок нужного объекта кнопкой мыши в поле другого значка («Drag-and-drop»).

При выборе каждой группы (подгруппы) и каждого клиента КСБ будет иметь типовой набор вкладок управления параметрами.

Внимание! В группе «Default» нельзя создавать подгруппы. Группу и клиента «Default» нельзя перемещать в какие-либо созданные администратором группы.

Настройка групп клиентов

При создании группы потребуется ввести ее наименование, которое можно впоследствии изменить. Удалить существующую группу можно с помощью кнопки «Удалить группу» на панели инструментов или, воспользовавшись контекстным меню.

Каждая группа (подгруппа) в дереве объектов содержит одинаковые вкладки для индивидуальной настройки параметров для клиентов и подгрупп в составе данной группы.

Состояние группы клиентов

Вкладка «Состояние» для выбранной группы в дереве объектов отображает общее состояние клиентов, входящих в группу (рис. 454).

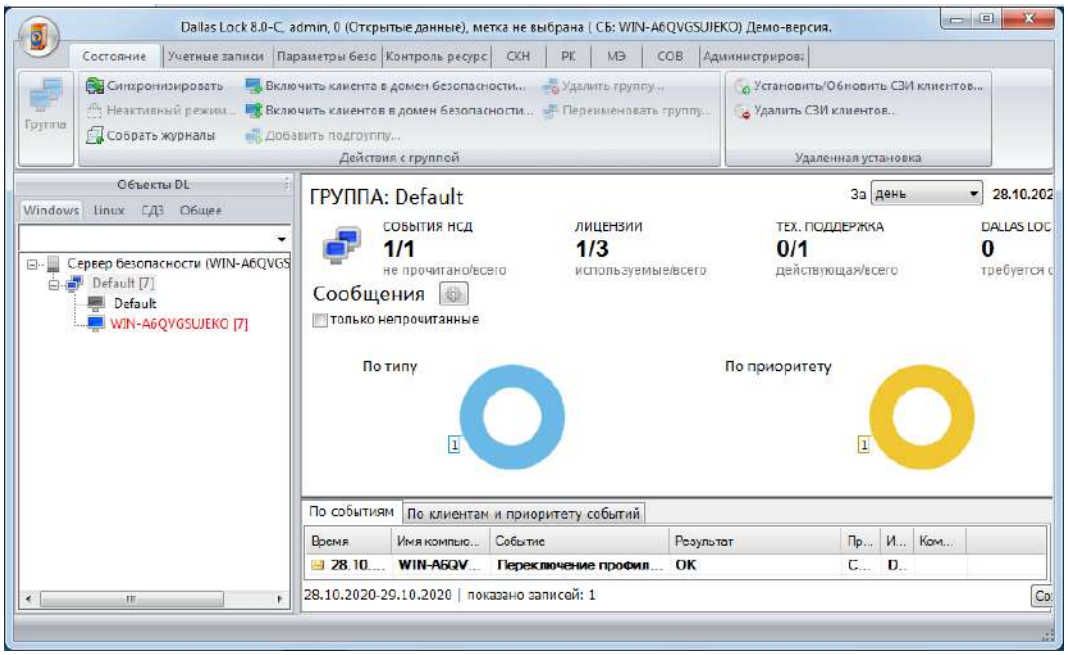


Рис. 454. Вкладка «Состояние» группы

Управление данной категорией аналогично управлению категории «Состояние» → «Основное» на уровне СБ (см. «Основное»).

Доступны следующие действия с группой клиентов:

1. По команде синхронизировать с СБ клиентов, входящих в данную группу (подгруппу).
2. Добавление клиента/клиентов в ДБ (см. «Ввод клиента в ДБ»).
3. Добавить в состав группы (подгруппы) новую подгруппу.
4. Включить «неактивный» режим для клиентов и подгрупп, входящих в группу. Настройка «неактивного» режима в КСБ происходит аналогично настройке из оболочки администратора (см. «Неактивный режим»).
5. Удалить группу из ДБ. Есть возможность удалить только ту группу, в которой нет клиентов. Группу «Default» удалить невозможно.
6. Переименовать группу.

Учетные записи группы клиентов

Вкладка «Учетные записи группы» на уровне группы содержит список учетных записей ДБ и отмеченных флагом для работы на клиентах в составе группы (подгруппы) (рис. 455) (см. «Создание пользователей ДБ»).

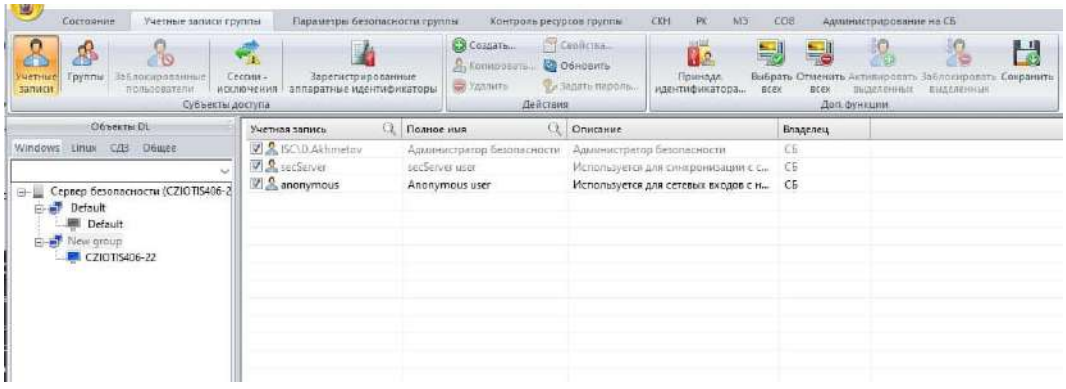


Рис. 455. Список учетных записей группы клиентов СБ

Список учетных записей группы клиентов СБ представляет собой таблицу с полями:

1. «Учетная запись», которое содержит логин учетной записи.
2. «Полное имя», которое содержит полное имя учетной записи.
3. «Описание», которое содержит описание учетной записи.
4. «Владелец», которое указывает на каком уровне дерева КСБ была создана учетная запись.

Примечание. Учетные записи не отображаются на панели «Учетные записи домена» на уровне выше, чем уровень, на котором была создана учетная запись. Например, на уровне СБ нельзя посмотреть учетные записи, созданные на уровне группы.

Примечание. Если учетная запись была создана на уровне СБ, то на уровне СБ поле «Владелец» будет иметь значение «Локальный», на уровне группы (подгруппы) и клиентов поле «Владелец» будет иметь значение «СБ».

Аналогично, если учетная запись была создана на уровне группы, то на уровне группы поле «Владелец» будет иметь значение «Локальный», на уровне клиентов группы, на которой была создана учетная запись поле «Владелец» будет иметь значение «Группа *Имя_группы*».

Учетные записи «secServer» и суперадминистратора Dallas Lock 8.0, отключить нельзя, так как они необходимы для корректной работы СЗИ.

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для группы необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

У клиентов ДБ существует также свой список учетных записей, в котором также можно выбрать необходимые для доступа к работе на клиенте.

Поэтому, особенностью списка учетных записей для группы клиентов является то, что после дополнительного формирования списка на самих клиентах, состояние отмеченных записей в списке группы (подгруппы) принимает вид:

- ☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на всех клиентах группы (подгруппы);
- ■ — затемненное поле означает неопределенность, запись включена на одних и выключена на других клиентах группы (подгруппы);
- ☐ — пустое поле означает, что запись отключена для работы на всех клиентах группы (подгруппы).

Группы учетных записей группы клиентов

Дополнительным инструментом управления правами учетных записей группы клиентов являются «Группы». Этот инструмент функционирует аналогично «Локальным группам» в ОС семейства Windows (рис. 456).

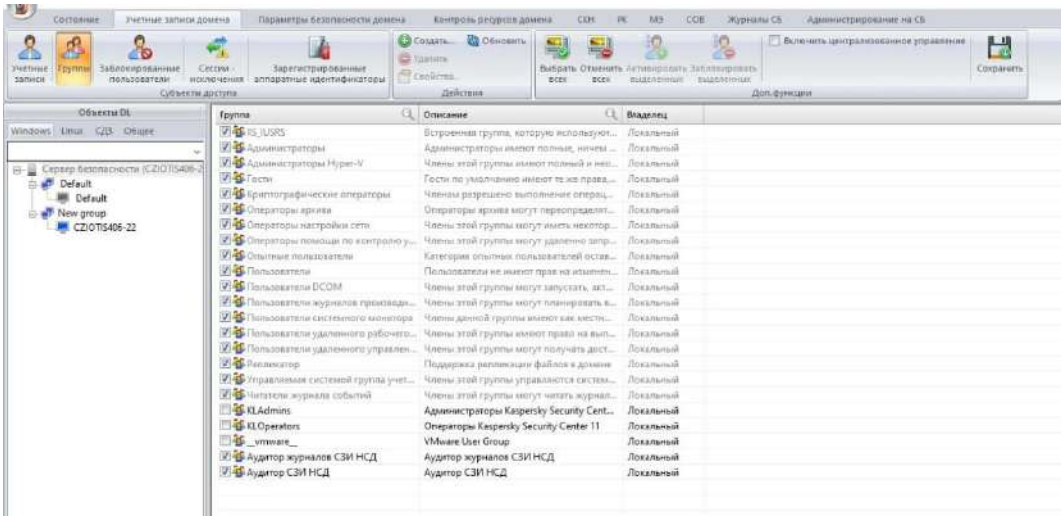


Рис. 456. Параметры безопасности для групп клиентов СБ

Рабочая область «Группы» представляет собой таблицу с полями:

1. «Группа», которое содержит имя группы.
2. «Описание», которое содержит описание группы.
3. «Владелец», которое указывает на каком уровне дерева КСБ была создана группа.

Примечание. Группы не отображаются на панели «Группы» на уровне выше, чем уровень, на котором была создана группа. Например, на уровне СБ нельзя посмотреть группы, созданные на уровне группы клиентов.

Примечание. Если группа была создана на уровне СБ, то на уровне СБ поле «Владелец» будет иметь значение «Локальный», на уровне группы (подгруппы) и клиентов поле «Владелец» будет иметь значение «СБ».

Аналогично, если группа была создана на уровне группы клиентов, то на уровне группы клиентов поле «Владелец» будет иметь значение «Локальный», на уровне клиентов группы (подгруппы клиентов), поле «Владелец» будет иметь значение «Группа *Имя_группы*».

На вкладке «Учетные записи домена» доступно только:

- создание и удаление групп;
- редактирование описания групп;
- просмотр информации о составе пользователей, входящих в группу.

Для просмотра состава пользователей группы, нужно нажать на кнопку «Свойства» панели «Действия» и перейти на вкладку «Пользователи» (рис. 457).

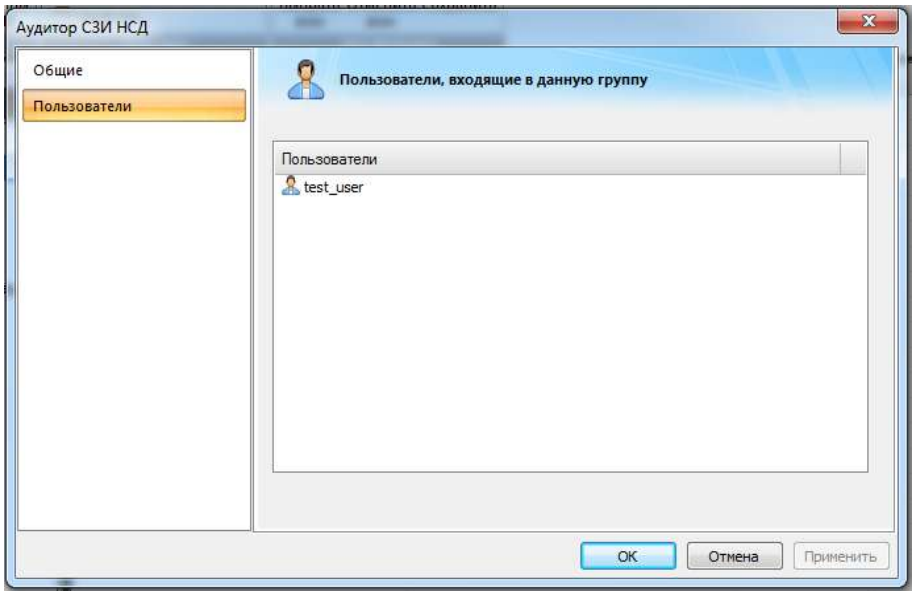


Рис. 457. Список пользователей, входящих в группу

Управление списком групп, в которые входит пользователь, осуществляется на вкладке «Учетные записи» категории «Учетные записи домена». Для изменения состава групп, в которые входит пользователь, необходимо выполнить следующие действия:

1. Выбрать из списка пользователя.
2. Нажать кнопку «Свойства» на панели «Действия».
3. Перейти на вкладку «Группы».
4. Отредактировать список групп в зависимости от необходимости.
5. Нажать кнопку «Ок».
6. Перейти в категорию «Состояние» и выполнить синхронизацию для применения изменений.

Для контроля созданных групп клиентов следует задать их на СБ. На панели доп. функций по умолчанию выключена настройка «Включить централизованное управление». После включения централизованного управления на клиентах будут удалены все группы, не заданные на СБ. Среди них могут оказаться служебные группы, созданные сторонним ПО для своей корректной работы. Рекомендуется предварительно создать такие группы на СБ (Рис. 458).

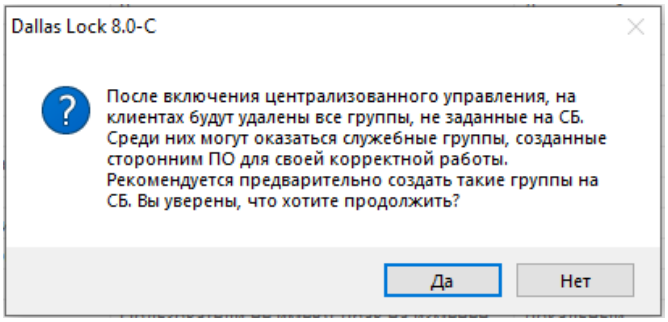


Рис. 458. Включить централизованное управление

Параметры безопасности группы клиентов

Вкладка «Параметры безопасности группы» на уровне группы позволяет редактировать параметры безопасности на уровне группы (подгруппы) (рис. 459).

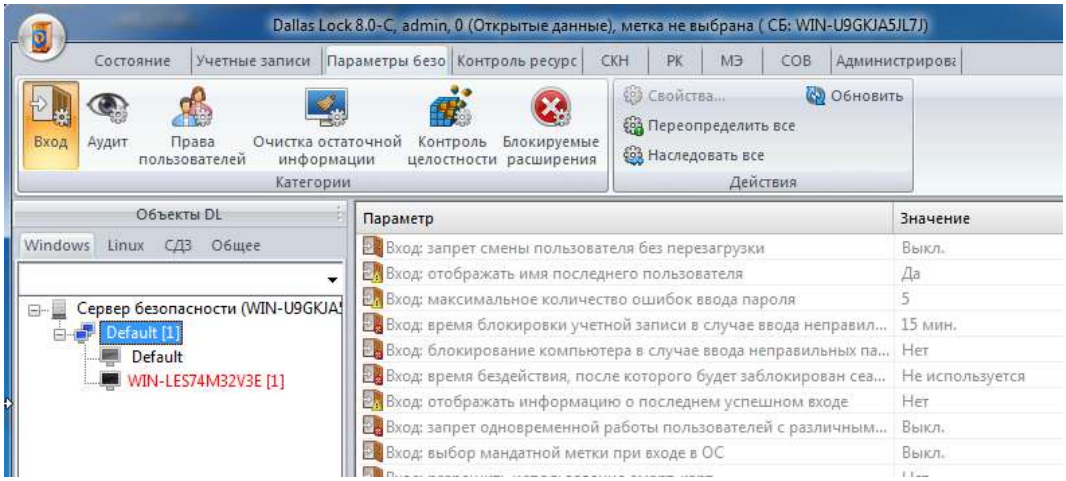


Рис. 459. Параметры безопасности для групп клиентов СБ

Настройка параметров безопасности для группы производится аналогично настройке параметров безопасности для ДБ (см. «Параметры безопасности домена»). Для применения параметров на клиентах необходима синхронизация.

Параметры могут наследовать установленные настройки (от СБ или от группы, в состав которой входит данная группа) или принимать индивидуальные значения следующим образом:

1. Параметры, для которых отмечено наследование, примут значения, установленные для родительского объекта в дереве объектов КСБ: значения для СБ или группы. В этом случае параметры будут отображаться нечетким серым цветом.
2. Параметры, для которых выбраны и установлены оригинальные настройки, будут отображаться четким черным цветом.

Для того, чтобы установить или снять наследование настроек, имеются следующие возможности:

1. Для того, чтобы все параметры наследовали значения, установленные для родительского объекта дерева, необходимо на панели действий выбрать «Наследовать все».
2. Если на панели действий выбрать «Переопределить все», то все параметры одновременно станут обозначены как индивидуально настроенные.
3. Для отдельно выбранного параметра при его настройке имеется возможность выбрать оригинальное значение или отметить свойство наследования (рис. 460).

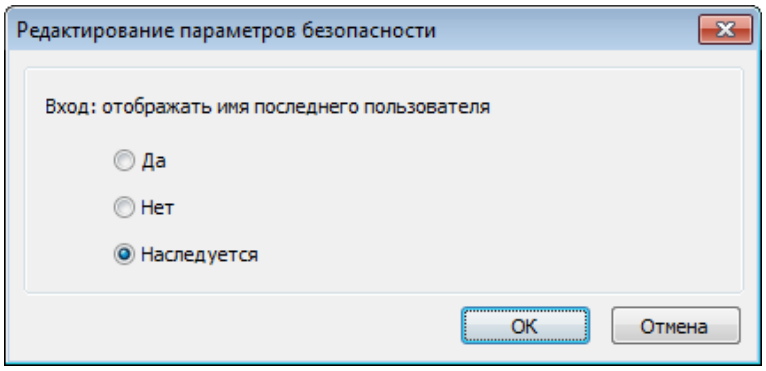


Рис. 460. Установка наследования значения параметра

4. Для списка блокируемых расширений доступно или полное наследование, или полное переопределение.

Управление правами учетных записей и групп на уровне группы клиентов осуществляется в категории «Параметры безопасности группы» → «Права пользователей» (рис. 461).

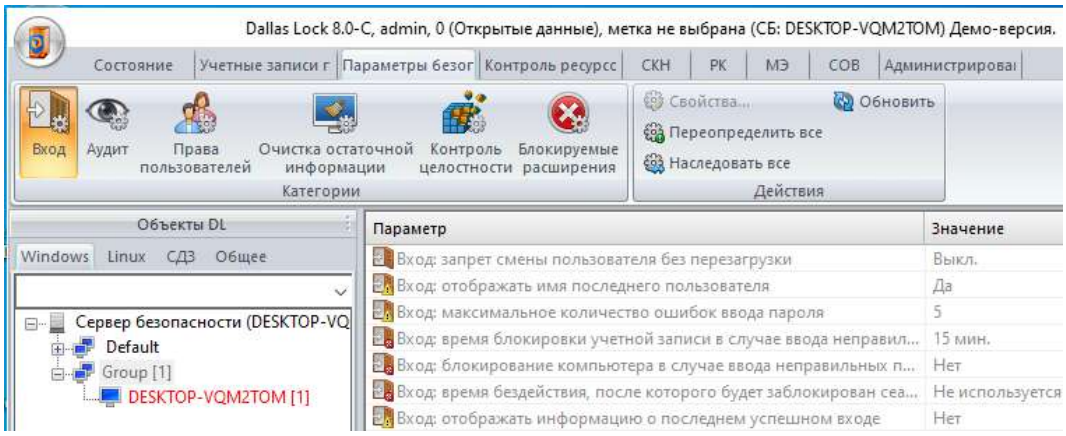


Рис. 461. Установка наследования значения параметра

Данная вкладка позволяет осуществлять назначение категорий прав для групп пользователей или учетных записей. По умолчанию наследуются настройки вышестоящего объекта дерева КСБ. Настройки по умолчанию отображаются серым цветом, оригинальные настройки выделены черным шрифтом.

Для изменения назначений прав, нужно выбрать параметр, нажать кнопку «Свойства» на панели «Действия». После внесения изменений, необходимо перейти в категорию «Состояние» и выполнить синхронизацию.

Контроль ресурсов группы

Управление глобальными параметрами ФС и контролем целостности на уровне групп пользователей осуществляется в категории «Контроль ресурсов группы».

Контроль ресурсов включает вкладки:

1. «Глобальные».

   На вкладке «Контроль ресурсов группы» на уровне группы расположен список назначений глобальных параметров ФС для группы клиентов (рис. 462).

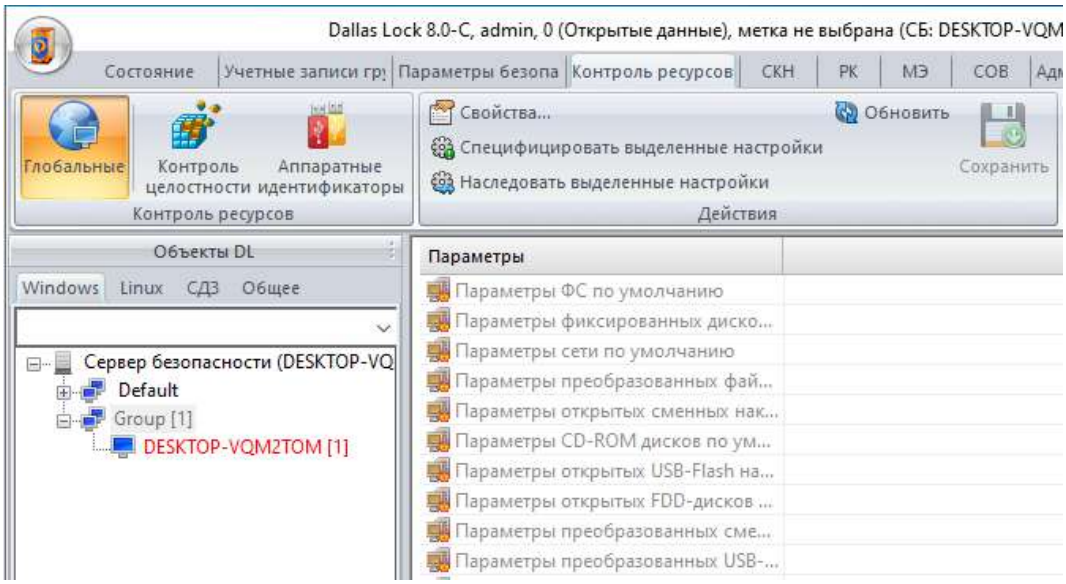


Рис. 462. Глобальные параметры ФС для группы клиентов

Управление значениями параметров осуществляется с помощью панели «Действия». Настройки можно специфицировать под нужды группы клиентов, нажав на панели «Действия» команду «Свойства» и выполнив настройку.

По умолчанию значения параметров наследуются с уровня СБ дерева клиентов. Наследуемые настройки выделяются серым цветом.

После выполнения всех изменений, необходимо сохранить изменения, нажав соответствующую кнопку на панели «Действия».

2. «Контроль целостности».

На вкладке «Контроль ресурсов группы» на уровне группы формируется список объединений (групп дескрипторов), которые должны быть созданы на клиентах группы (рис. 463).

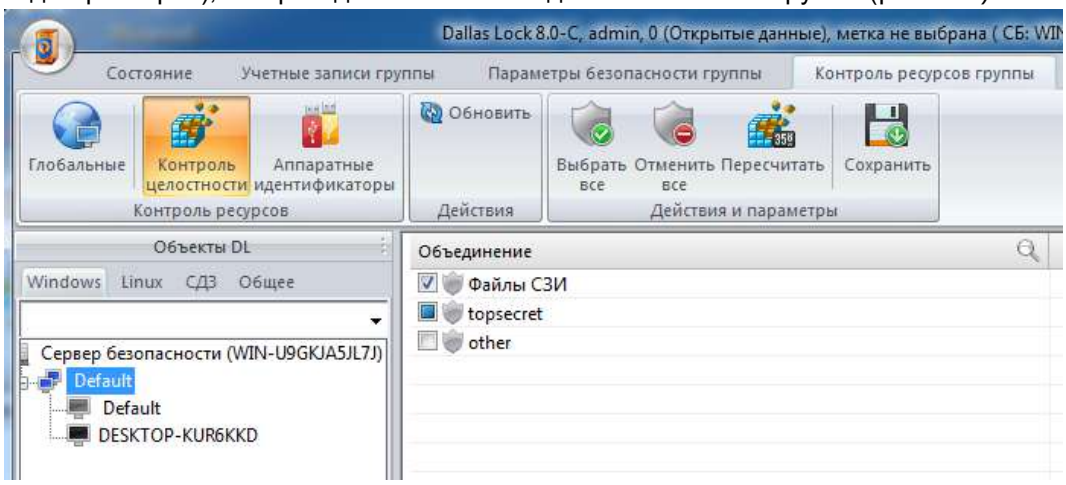


Рис. 463. Объединения группы клиентов

Вспомогательные кнопки помогают одновременно отметить все объединения.

После формирования списка объединений, необходимо нажать «Сохранить». Для создания на клиентах дескрипторов, входящих в объединения, необходима синхронизация.

Для пересчета контрольных сумм объектов ФС на всех клиентах группы необходимо нажать кнопку «Пересчитать» и выполнить синхронизацию с клиентами.

У клиентов ДБ существует также свой список объединений, в котором также можно выбрать необходимые группы дескрипторов для создания на клиенте. Поэтому, после дополнительного формирования списка объединений на самих клиентах, состояние отмеченных дескрипторов в списке группы имеет вид:

- ☑ — отмеченное флагом поле означает, что объединение установлено на всех клиентах в группе (подгруппе);
- ■ — затемненное поле означает, что объединение установлено на некоторых (не на всех) клиентах группы (подгруппы);

— пустое поле означает, что объединение не установлено ни на одном клиенте группы (подгруппы).

3. «Аппаратные идентификаторы».

На вкладке «Контроль ресурсов группы» на уровне группы формируется список аппаратных идентификаторов (рис. 464).

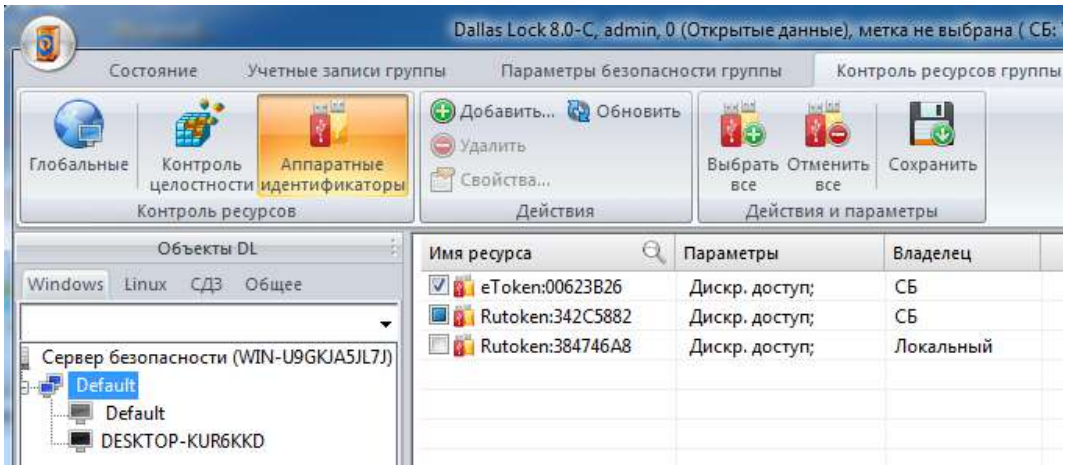


Рис. 464. Аппаратные идентификаторы группы

Вспомогательные кнопки помогают одновременно отметить все аппаратные идентификаторы.

После формирования списка аппаратных идентификаторов, необходимо нажать кнопку «Сохранить».

— отмеченное флагом поле означает, что аппаратный идентификатор добавлен на всех клиентах в группе (подгруппе);

— затемненное поле означает, что аппаратный идентификатор добавлен на некоторых (не на всех) клиентах группы (подгруппы);

— пустое поле означает, что аппаратный идентификатор не добавлен ни на одном клиенте группы (подгруппы).

Групповые настройки МЭ

Вкладка групповых настроек «МЭ» на уровне группы позволяет редактировать параметры МЭ, а также просматривать статистику МЭ со всех клиентов группы (подгруппы) (рис. 465).

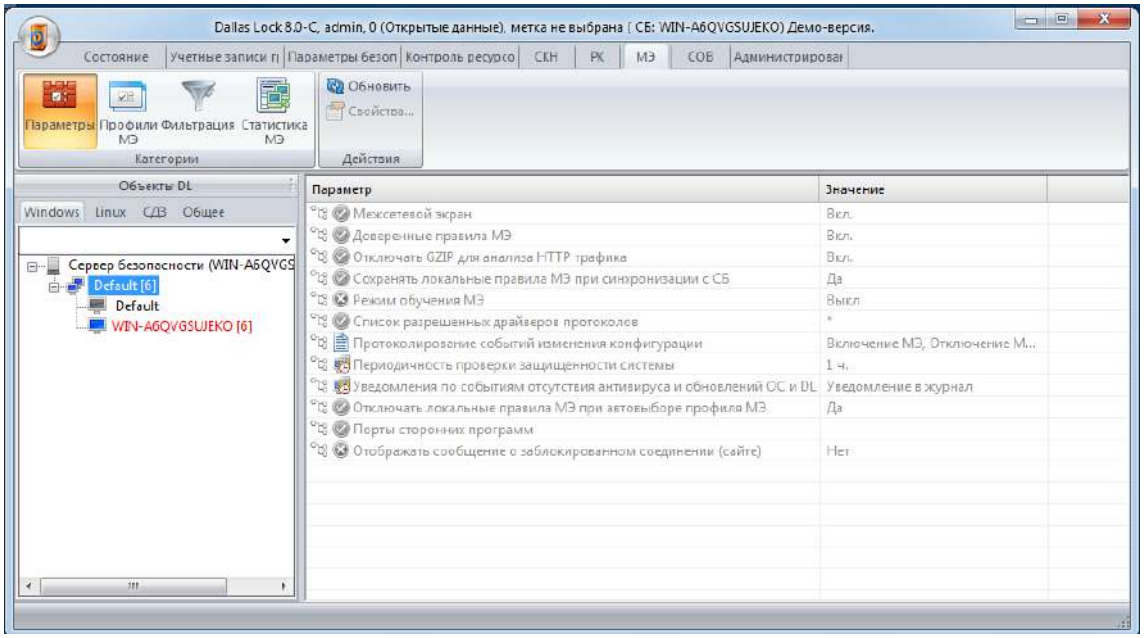


Рис. 465. Групповые настройки МЭ

Настройка МЭ для группы производится аналогично настройке МЭ для ДБ (см. «Доменные настройки МЭ»), с тем лишь отличием, что после настройки необходимо нажать кнопку «Сохранить». Для применения параметров на клиентах необходима синхронизация.

Параметры могут наследовать установленные настройки (от СБ или от группы, в состав которой

входит данная группа) или принимать индивидуальные значения. Поэтому состояние параметров принимает следующий вид:

— отмеченное флагом поле означает, что параметр включен и имеет индивидуальные настройки. Параметр будет отображаться четким черным цветом;

— пустое поле означает, что параметр отключен и имеет индивидуальные настройки. Параметр будет отображаться четким черным цветом;

— параметр наследует значение, установленное для родительского объекта в дереве объектов КСБ. Параметр будет отображаться нечетким серым цветом.

Примечание. Если для группы клиентов требуется сформировать отличный от других групп набор правил МЭ (в том числе иные настройки аудита Журнала пакетов), то эту задачу можно решить с помощью Профилей МЭ.
Для этого требуется:

- создать на уровне ДБ все необходимые правила МЭ;
- перейти в категорию «Профили МЭ»;
- создать новый профиль МЭ, активировав в нем только те правила, которые должны быть в этой группе клиентов, и деактивировав уникальные для этой группы правила в профиле МЭ, который используется по умолчанию другими группами клиентов;
- перейти на уровень группы клиентов, включить сформированный ранее профиль МЭ и (при необходимости) изменить приоритеты.

Групповые настройки СОВ

Вкладка групповых настроек «СОВ» на уровне группы редактировать параметры СОВ, а также просматривать статистику СОВ со всех клиентов группы (подгруппы) (рис. 466).

Рис. 466. Групповые настройки СОВ

Настройка СОВ для группы производится аналогично настройке СОВ для ДБ (см. «Доменные настройки СОВ»), с тем лишь отличием, что после настройки необходимо нажать кнопку «Сохранить». Для применения параметров на клиентах необходима синхронизация.

Параметры могут наследовать установленные настройки (от СБ или от группы, в состав которой входит данная группа) или принимать индивидуальные значения.

Следует учитывать, что:

1. Настройки переменных на уровне групп доступны только для просмотра.
2. Параметры подписанных и неподписанных приложений по умолчанию просматривать и переопределять на уровне группы нельзя.

Групповые настройки СКН

Список установленных дескрипторов на ресурсы ФС сменных накопителей, общий для всего ДБ. Список формируется на уровне СБ в категории «СКН» → «Сменные накопители» (см. «Контроль целостности ДБ»).

В категории «Сменные накопители» на уровне группы формируется список дескрипторов, в соответствии с которыми пользователи могут работать на клиентах группы (рис. 467).

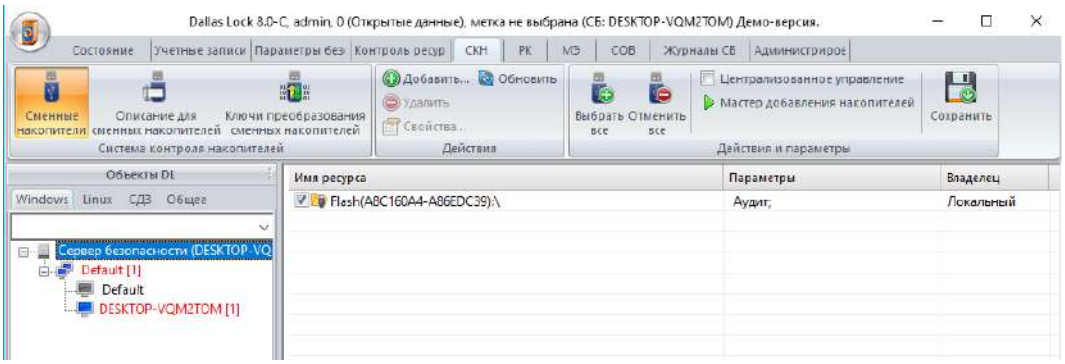


Рис. 467. Список дескрипторов сменных накопителей для группы клиентов

Для того, чтобы список дескрипторов на клиентах группы управлялся с СБ, а не локально, необходимо отметить «Централизованное управление». После формирования списка дескрипторов сменных накопителей необходимо нажать кнопку «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

У клиентов ДБ существует также свой список учетных записей, в котором также можно выбрать необходимые для доступа к работе на клиенте. Поэтому, после дополнительного формирования списка сменных накопителей на самих клиентах, состояние отмеченных дескрипторов в списке группы имеет вид:

- — отмеченное флагом поле означает, что дескриптор установлен на всех клиентах в группе (подгруппе);
- — затемненное поле означает, что дескриптор установлен на некоторых (не на всех) клиентах группы (подгруппы);
- — пустое поле означает, что дескриптор не установлен ни на одном клиенте группы (подгруппы).

Для поля «Централизованное управление» данное свойство распространяется.

Механизм преобразования сменных накопителей описан в разделе «Преобразование сменных накопителей». С помощью СБ возможно централизованное управление списком ключей преобразования для клиентов.

Список ключей преобразования сменных накопителей общий для всего ДБ. Список формируется на уровне СБ в категории «СКН» → «Ключи преобразования сменных накопителей» (см. «Преобразование сменных накопителей»).

В категории «Ключи преобразования сменных накопителей» на уровне группы формируется список ключей, которые будут созданы на клиентах группы (рис. 468).

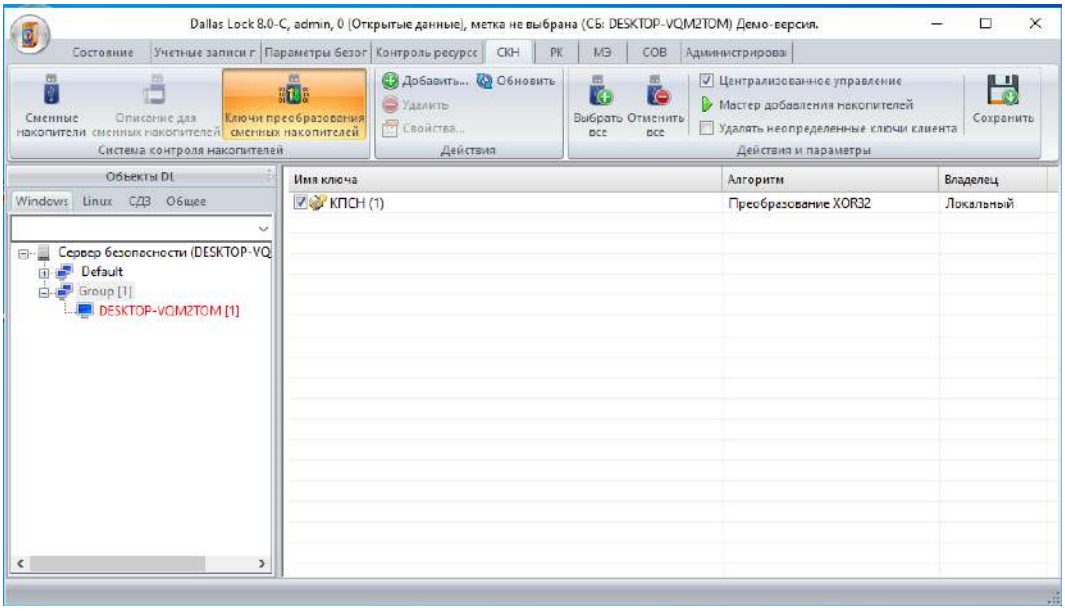


Рис. 468. Список ключей преобразования для группы клиентов

Для того, чтобы список ключей на клиентах группы управлялся с СБ, а не локально, необходимо отметить «Централизованное управление». После формирования списка ключей преобразования необходимо нажать кнопку «Сохранить». Для применения списка ключей преобразования на клиентах необходима синхронизация.

Для группы клиентов, также как для всего ДБ, можно задать удаление неопределенных ключей на клиентах.

У клиентов ДБ существует также свой список ключей преобразования, в котором можно выбрать необходимые для работы на клиенте. Поэтому, после дополнительного формирования списка сменных накопителей на самих клиентах, состояние отмеченных дескрипторов в списке группы имеет вид:

- — отмеченное флагом поле означает, что ключ преобразования создан на всех клиентах группы (подгруппы);
- — затемненное поле означает неопределенность, что ключ преобразования создан на некоторых (не на всех) клиентах группы (подгруппы);
- — пустое поле означает, что ключ преобразования не создан на клиентах группы (подгруппы).

Для полей «Централизованное управление» и «Удалять неопределенные ключи клиента» данное свойство также распространяется.

Сменные накопители можно добавить с клиентов на СБ через «Мастер добавления накопителей».

1. Нажмите на «Мастер добавления накопителей» на панели «Действия и параметры». Откроется окно «Мастер добавления сменных накопителей», в котором необходимо выбрать имя компьютера, на котором подключены USB-накопители (Рис. 469).

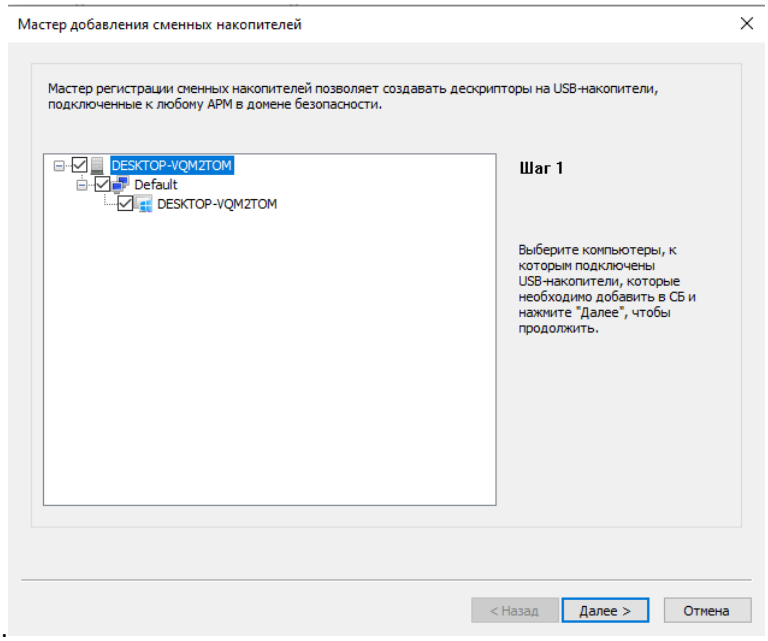


Рис. 469. Мастер добавления сменных накопителей

2. На втором шаге осуществляется сбор информации о USB-накопителях, подключенных к АРМ клиентов (Рис. 470).

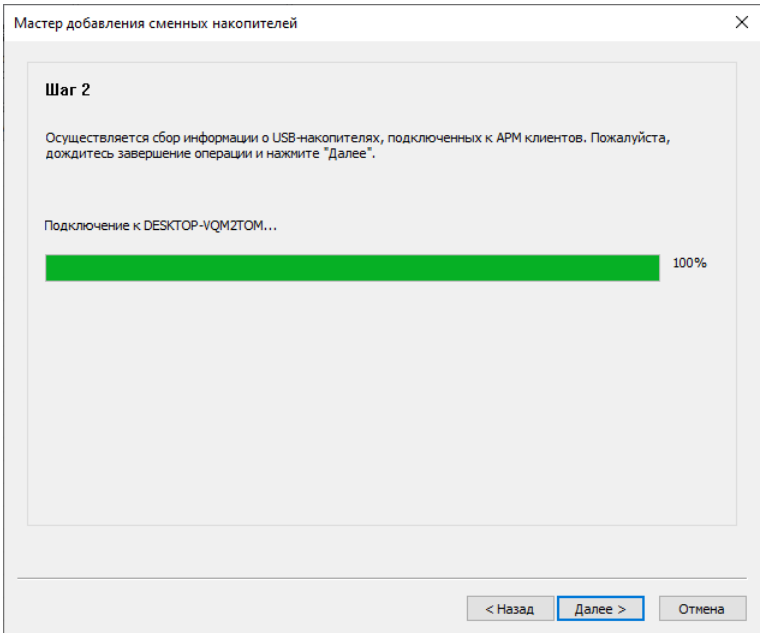


Рис. 470. Сбор информации о USB-накопителях

3. После завершения второго шага нажмите «Далее». В списке выберете USB-накопители, которые необходимо добавить на СБ (Рис. 471). После выбора нажмите «Готово».

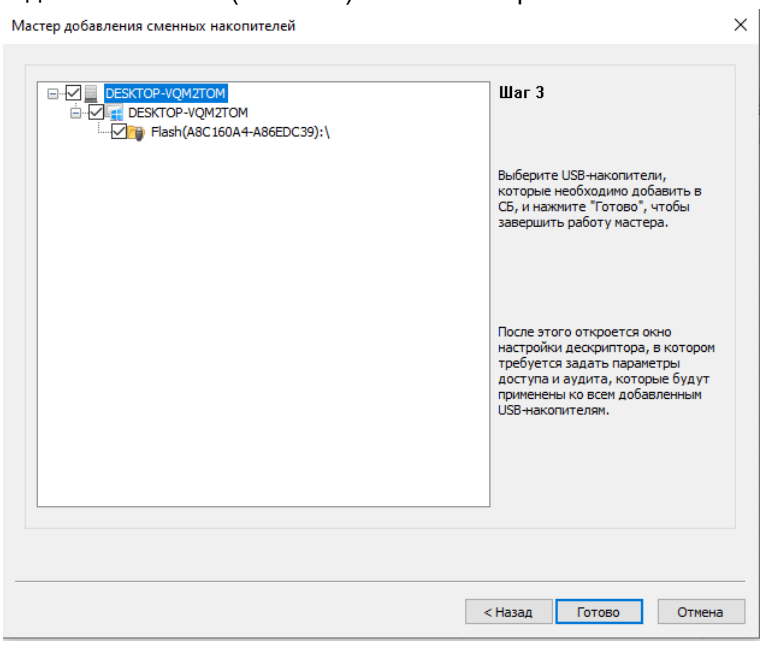


Рис. 471. Список USB-накопителей

4. Следом откроется окно «Список дескрипторов» (Рис. 472), в котором можно настроить доступ для сменного носителя (см. «Система контроля накопителей»).

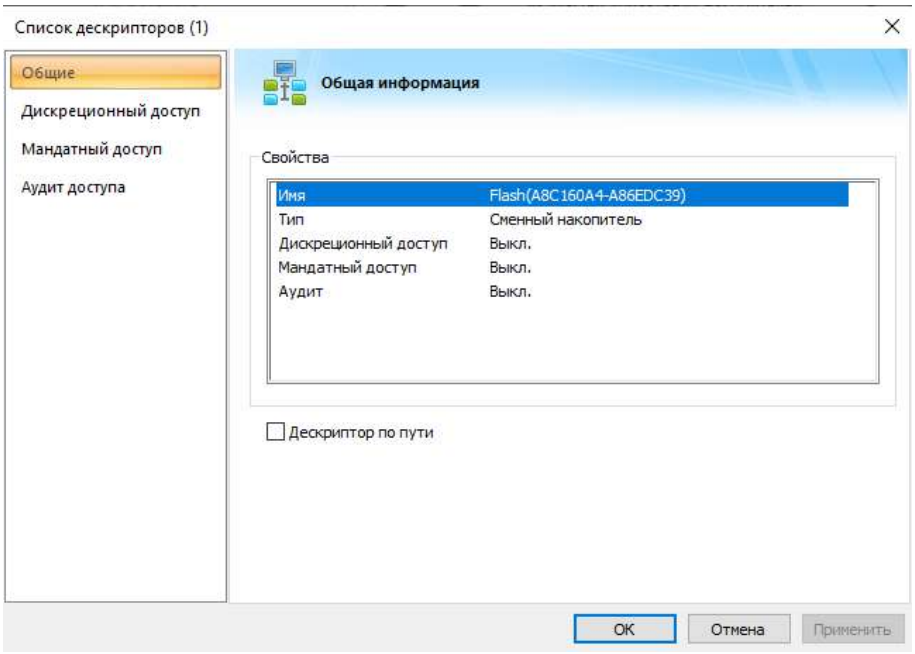


Рис. 472. Список дескрипторов

Настройка клиентов

В дереве объектов присутствует клиент «Default» и другие зарегистрированные в ДБ клиенты. Для клиента «Default» кроме настройки списка пользователей, ключей преобразования и неактивного режима другие настройки недоступны; в тоже время для каждого вновь созданного в ДБ клиента автоматически копируются данные настройки клиента «Default» и доступны дополнительные.

Параметры безопасности на уровне клиента отображаются на нескольких основных вкладках.

Состояние клиента

Вкладка «Состояние» на уровне клиента отображает общее состояние клиента (рис. 473).

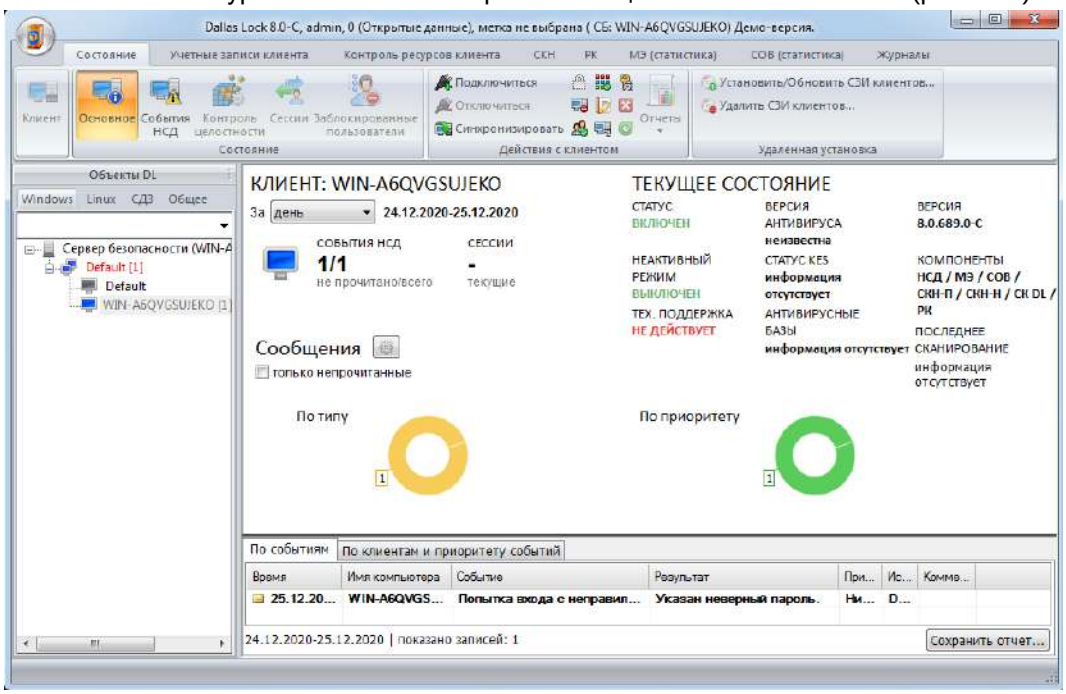


Рис. 473. Вкладка «Состояние» Клиента

Доступны следующие категории.

Основное
В верхней части информационной панели отображается следующая информация: • имя клиента;

- количество событий НСД на клиенте за выбранный период времени;
- количество текущих сессий (интерактивных) на клиенте;
- текущее состояние клиента:
  - статус клиента;
  - статус неактивного режима СЗИ;
  - статус технической поддержки;
  - версия установленного на АРМ антивируса (в случае взаимодействия СБ с KSC и использования ПО KES на данной АРМ указывается версия ПО KES);
  - статус KES (в случае взаимодействия СБ с KSC и использования ПО KES на данной АРМ), отображающий статус ПО (включен / выключен);
  - актуальность антивирусных баз Kaspersky Endpoint Security (в случае взаимодействия СБ с KSC и использования ПО KES на данной АРМ) и дату последнего обновления;
  - версия Dallas Lock 8.0;
  - активные компоненты Dallas Lock 8.0.

Управление данной категорией аналогично управлению категории «Состояние» → «Основное» на уровне СБ (см. «Основное»).

Доступны следующие действия с клиентом (некоторые действия доступны только при подключении к клиенту):

- Подключиться (отключиться) к клиенту для ОУ. Некоторые функции и настройка параметров доступны только при подключении к клиенту.
- По команде синхронизировать клиента с СБ.
- Включить «неактивный» режим для клиента. Настройка «неактивного» режима в КСБ происходит аналогично настройке из оболочки администратора (см. «Неактивный режим»).
- Удалить клиента из ДБ (Dallas Lock 8.0 при этом не удаляется).
- Разблокировать пользователей клиента (см. выше или «Заблокированные пользователи»).
- Применить к клиенту сохраненный файл конфигурации с установленными настройками подобно тому, как это происходит в оболочке администратора (см. «Применение файла конфигурации Dallas Lock»).
- Изменить номер лицензии и код технической поддержки на клиенте.
- Сменить сетевое имя клиента. Данная опция применяется в случае, если при смене сетевого имени клиентский компьютер был не на связи с СБ, в результате чего на СБ не поступила информация о смене имени, и СБ не сможет связаться с клиентом.
- Установить краткое описание, которое будет добавлено к имени клиента в списке объектов.
- Установить пароль доступа СБ (учетной записи «secServer») для данного клиента. Используется при невозможности синхронизации клиента с СБ. В этом случае, вместе с установкой нового пароля доступа в КСБ для клиента, следует изменить и пароль учетной записи «secServer» в оболочке администратора на клиенте.
- Завершить работу клиента.
- Перезагрузить клиент.
- Сформировать отчеты с клиента (см. «Отчет о правах и конфигурации», «Создание паспорта программного обеспечения», «Создание паспорта аппаратной части ПК»).

События НСД

Отображается список событий НСД клиента. События, регистрируемые как НСД, настраиваются через параметры СБ (см. «Сигнализация об НСД»). Данный список формируется из журналов клиента. С помощью панели действий можно отметить все записи прочитанными или непрочитанными, обновить, очистить список, загрузить новый. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

Контроль целостности

Отображается состояние целостности объектов программно-аппаратной среды. Имеется возможность проверить целостность и пересчитать.

Сессии

Отображаются текущие (интерактивные) сессии на данном клиенте. Имеется возможность завершить определенную сессию или заблокировать компьютер. При подключении к

клиенту в списке сессий всегда находится учетная запись «secServer», так как именно под его учетной записью происходит подключение, при завершении сессии «secServer», подключение СБ к клиенту прекращается.
Заблокированные пользователи
Отображает список всех заблокированных на клиенте пользователей. Для просмотра списка заблокированных пользователей необходимо подключиться к клиенту. Для разблокировки пользователей на панели действий необходимо нажать кнопку «Разблокировать пользователей» (без подключения к клиенту) или подключиться к клиенту, выбрать пользователя в списке заблокированных и нажать кнопку «Разблокировать».

Учетные записи клиента

Вкладка «Учетные записи клиента» на уровне клиента содержит список учетных записей ДБ и отмеченных флагом для работы на клиенте (рис. 474) (см. «Создание пользователей ДБ»).

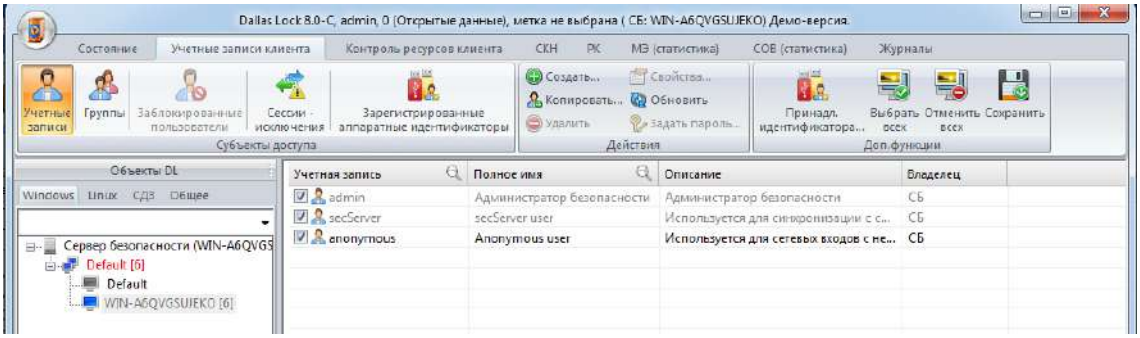


Рис. 474. Список учетных записей клиента

Учетные записи «secServer» и суперадминистратора, отключить нельзя, так как они необходимы для корректной работы Dallas Lock 8.0.

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для клиента необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

Так как все учетные записи клиентов управляются с СБ, следует учесть, что:

1. Если на клиенте в оболочке администратора созданы учетные записи, но не продублированы на СБ, то в процессе синхронизации они будут отключены (отображается соответствующим значком в оболочке администратора).
2. Не отмеченные учетные записи ДБ (снят флаг) после синхронизации будут отключены на клиенте.

Параметры безопасности клиента

Вкладка «Параметры безопасности клиента» на уровне клиента доступна только тогда, когда к клиенту осуществлено подключение из КСБ (кнопка «Подключиться» на вкладке «Состояние») (рис. 475).

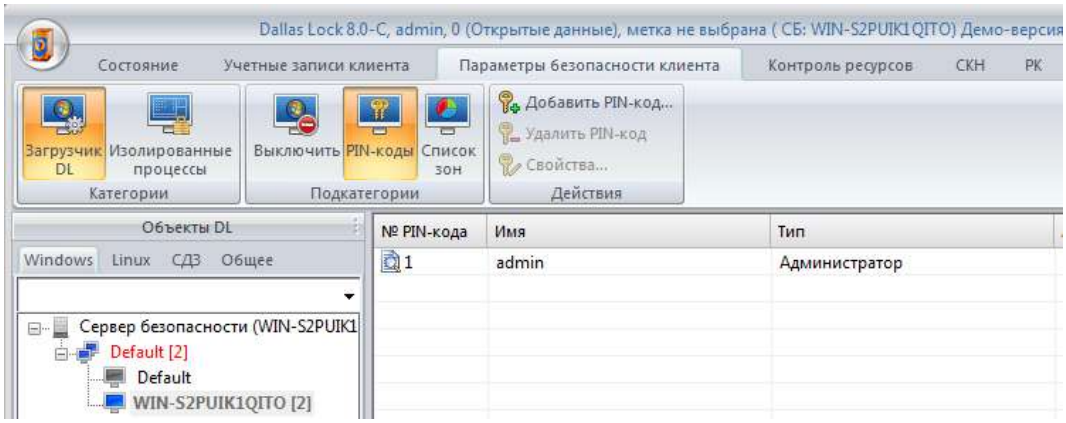


Рис. 475. Вкладка параметров безопасности клиента

Доступны следующие категории.

Загрузчик DL
Включение (выключение), создание и настройка PIN-кодов, прозрачное преобразование зон жесткого диска для клиента. Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Загрузчик DL»). Синхронизации настроек для данных параметров не требуется, так как они выполняются в режиме ОУ.
Изолированные процессы
Настройки выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Изолированные процессы»). Синхронизации настроек для данных параметров не требуется, так как они выполняются в режиме ОУ.

Контроль ресурсов клиента

При неактивном подключении к клиенту на вкладке «Контроль ресурсов» доступна категория «Контроль целостности». В категории отображается список объединений, общий для всего ДБ. Список формируется на уровне СБ в категории «Контроль ресурсов домена» → «Контроль целостности ДБ» (см. «Контроль целостности ДБ»).

На вкладке «Контроль ресурсов» на уровне клиента формируется список объединений (групп дескрипторов), которые должны быть созданы на клиенте (рис. 476).

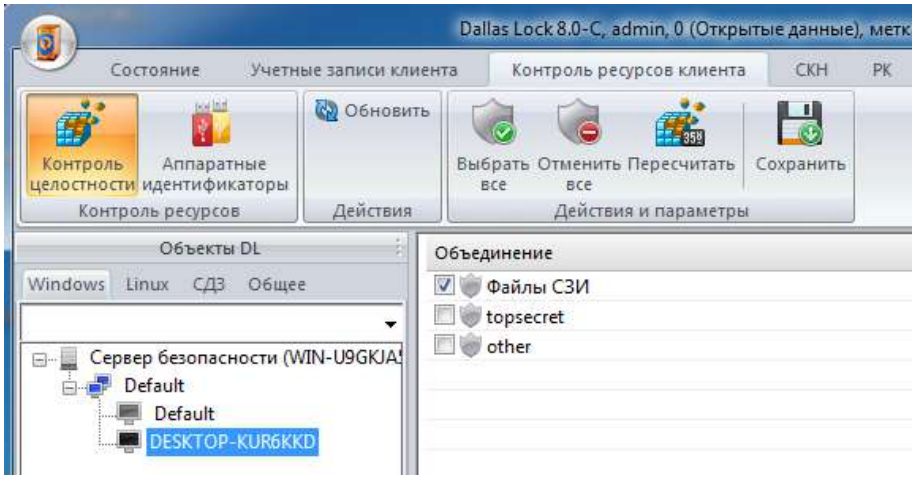


Рис. 476. Объединения клиента

Вспомогательные кнопки помогают одновременно отметить все объединения.

После формирования списка объединений, необходимо нажать «Сохранить». Для создания на клиентах дескрипторов, входящих в объединения, необходима синхронизация.

Для пересчета контрольных сумм объектов ФС на всех клиентах группы необходимо нажать кнопку «Пересчитать» и выполнить синхронизацию с клиентами.

При подключении к клиенту доступны следующие категории (рис. 477).

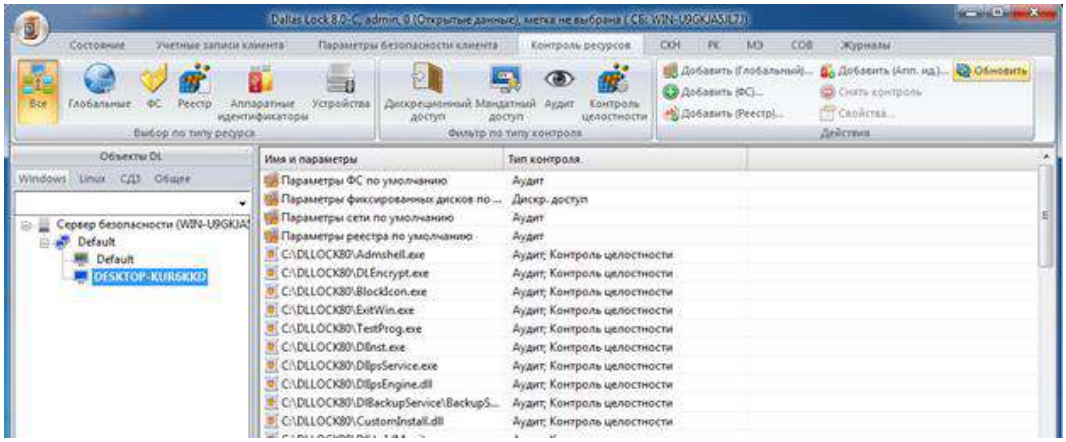


Рис. 477. Контроль ресурсов подключенного клиента

Все
Настройка списка дескрипторов разграничения доступа, аудита и контроля целостности для клиента. Настройка выполняются аналогично тому, как это осуществляется в оболочке

администратора.
Доступ
Настройка списка дескрипторов дискреционного разграничения доступа для клиента. Настройка выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Дискреционный доступ»).
Мандатный доступ
Настройка списка дескрипторов мандатного разграничения доступа для клиента. Настройка выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Мандатный доступ»).
Аудит
Настройка списка дескрипторов аудита для клиента. Настройка выполняются аналогично тому, как это осуществляется в оболочке администратора (см. «Аудит локальных объектов ФС и веток реестра»).
Контроль целостности
Список дескрипторов контроля целостности на клиенте, входящие в отмеченные объединения при неактивном подключении. Данный список полностью привязан к механизму централизованного управления контролем целостности. Поэтому для его редактирования необходимо редактировать объединения контроля целостности на уровне СБ (см. «Контроль целостности ДБ»).
Контроль доступа к устройствам
Настройки доступа к устройствам будут установлены для клиента. Данные настройки задаются только на уровне классов устройств аналогично тому, как это осуществляется с помощью оболочки администратора (см. «Разграничение доступа к устройствам»).. Чтобы настроить доступ к конкретным устройствам, необходимо подключиться к включенному клиенту из КСБ, и перейти на вкладку клиента «Контроль устройств», далее выполнить настройки аналогично локальному администрированию в оболочке администратора (см. «Разграничение доступа к устройствам»).

Настройка МЭ клиента

Вкладка «МЭ» на уровне клиента полностью доступна только тогда, когда к клиенту осуществлено подключение из КСБ, в противном случае на вкладке будет отображена только статистика на момент последнего подключения клиента (рис. 478). Настройки параметров производятся аналогично администрированию в оболочке администратора Dallas Lock 8.0.

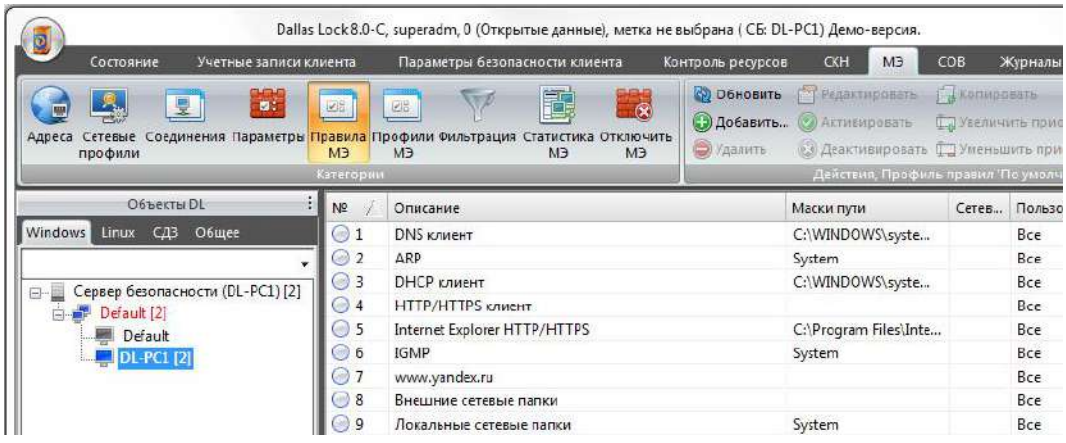


Рис. 478. Вкладка «МЭ» клиента. Правила МЭ

Настройка СОВ клиента

Вкладка «СОВ» клиента полностью доступна только тогда, когда к клиенту осуществлено подключение из КСБ, в противном случае на вкладке будет отображена только статистика на момент последнего подключения клиента (рис. 479). Настройки параметров производятся аналогично администрированию в оболочке администратора Dallas Lock 8.0.

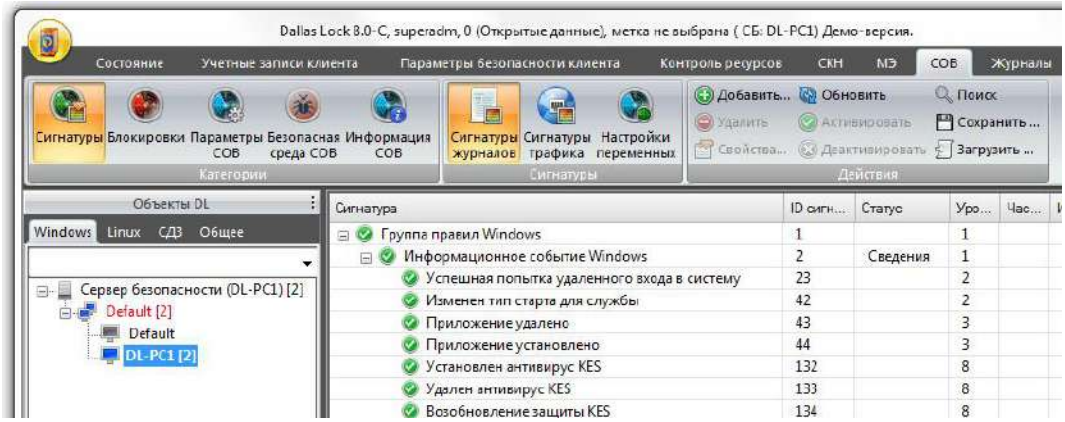


Рис. 479. Вкладка «СОВ» клиента

Настройка СКН клиента

Список установленных дескрипторов на ресурсы ФС сменных накопителей, общий для всего ДБ или клиентов в составе группы (подгруппы). Список формируется на уровне СБ или группы в категории «СКН» → «Сменные накопители» (см. «Преобразование сменных накопителей» и «Групповые настройки СКН»).

Для самого клиента в категории «СКН» → «Сменные накопители» имеется возможность индивидуально отметить те дескрипторы, с которыми возможно работать на клиенте (рис. 480).

Вспомогательные кнопки помогают одновременно отметить все дескрипторы.

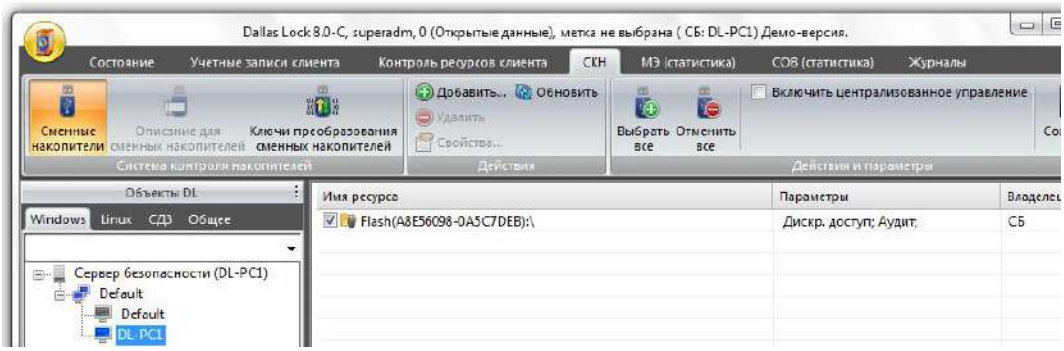


Рис. 480. Список дескрипторов сменных накопителей клиента

Для того, чтобы список дескрипторов на клиенте управлялся с СБ, а не локально, необходимо отметить «Включить централизованное управление». И наоборот, для того, чтобы управлять дескрипторами сменных накопителей локально или в режиме ОУ, независимо от изменения списка на СБ, необходимо снять флаг.

Если централизованное управление включено, то создание дескрипторов средствами ОУ становится невозможным, и появится предупреждение.

После формирования списка дескрипторов сменных накопителей для клиента необходимо нажать «Сохранить». Для применения списка сменных накопителей на клиентах необходима синхронизация.

Механизм преобразования сменных накопителей описан в разделе «Преобразование сменных накопителей». С помощью СБ возможно централизованное управление списком ключей преобразования для клиентов.

Список установленных ключей преобразования сменных накопителей, общий для всего ДБ или клиентов в составе группы (подгруппы). Список формируется на уровне СБ или группы в категории «СКН» → «Ключи преобразования сменных накопителей» (см. «Управление ключами преобразования ДБ» и «Групповые настройки СКН»).

Для самого клиента в категории «СКН» → «Ключи преобразования сменных накопителей» имеется возможность индивидуально отметить те ключи преобразования, с которыми возможно работать на клиенте (рис. 481).

Вспомогательные кнопки помогают одновременно отметить все дескрипторы.

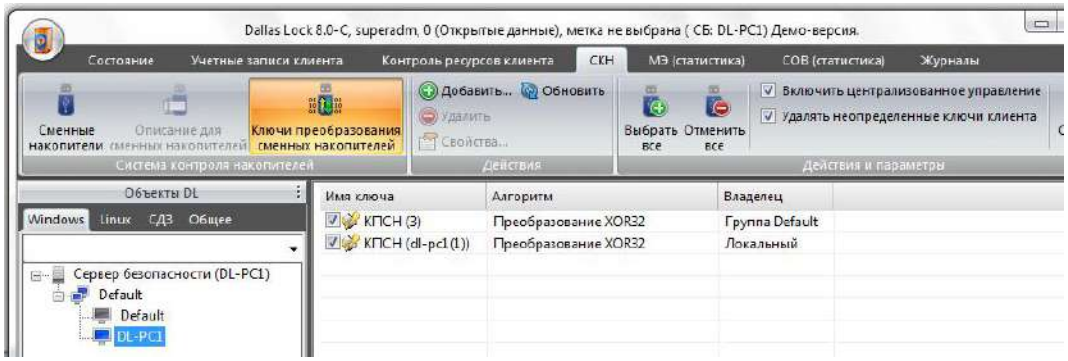


Рис. 481. Список ключей преобразования клиента

Для того, чтобы список ключей на клиенте управлялся с СБ, а не локально, необходимо отметить «Включить централизованное управление». И наоборот, для того, чтобы управлять дескрипторами сменных накопителей локально или в режиме ОУ, независимо от изменения списка на СБ, необходимо снять флаг.

Для индивидуальных клиентов, также как для всего ДБ и групп, можно задать удаление неопределенных ключей на клиентах (отметить данное поле).

После формирования списка дескрипторов сменных накопителей для клиента необходимо нажать «Сохранить». Для применения списка сменных накопителей на клиентах необходима синхронизация.

Журналы клиента

Вкладка «Журнал» на уровне клиента позволяет выбрать и открыть собранные СБ журналы с клиента (рис. 482).

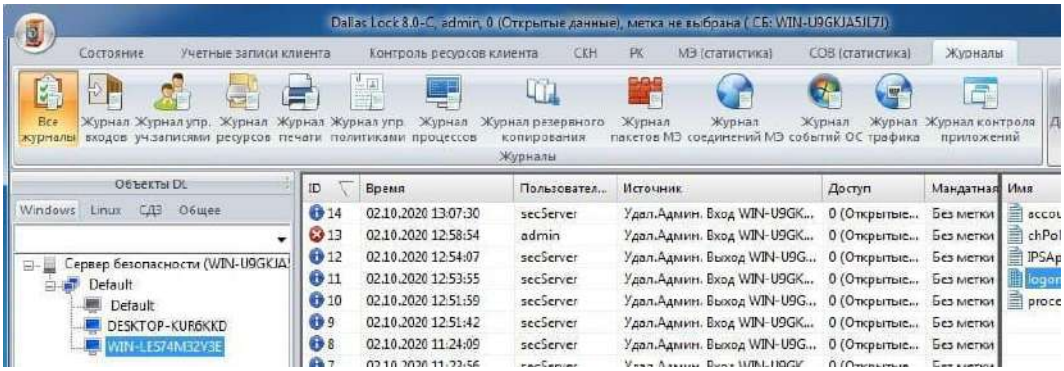


Рис. 482. Вкладка КСБ полученных с клиента журналов

Формирование этих журналов и записей в них происходит на момент команды сбора журналов путем нажатия данной кнопки на вкладке «Состояние» клиента или на вкладке «Состояние» СБ, а также при настроенном периодическом сборе журналов в параметрах СБ.

Принцип ведения журналов клиентов на СБ следующий. На СБ в момент получения журналов с клиента происходит объединение записей журналов одного типа с предыдущими. Объединение новых записей в процессе сбора журналов происходит до тех пор, пока не достигается максимальный размер (20000 записей). Далее журнал архивируется и начинает вестись заново.

В правой части окна формируется список всех полученных журналов и их размер в байтах, а в центральной — списки записей выбранного журнала.

Панель «Действия» аналогична той, что есть в оболочке администратора Dallas Lock 8.0: имеется возможность архивации записей, экспорта записей в файл в выбранном формате, настройка и применение фильтра, группировка записей (см. «Журналы»).

Следует отметить, что папке «C:\DLLOCK80» имеются следующие папки, содержащие журналы событий:

- Папка «Jrn» — папка с текущими журналами данной рабочей станции. Это те журналы, которые формируются и открываются с помощью вкладки «Журналы» оболочки администратора.
- Папка «Logs» — папка, хранящая сформированные автоматически при переполнении (>20000 записей) текущие журналы событий и журналы после их архивации данной рабочей станции, в том числе журнал СБ. А также, при установке на компьютер СБ, в папке «Logs» формируются папки с именами клиентских рабочих станций, в которых хранятся все собранные с клиентов журналы.

- В папке «DLSecServer» помимо установочных файлов СБ хранится текущий журнал данного СБ.

Примечание. С помощью клавиши «Delete» можно удалить файл журнала клиента в КСБ. Для этого выполнить следующее:

1. Выделить выбранный файл в журнале клиента и нажать клавишу «Delete».
2. Перед удалением файла из журнала пользователю выводится соответствующее сообщение.
3. При положительном ответе происходит удаление файла из журнала, при отрицательном операция будет отменена.

19.11 Клиенты Linux

Для управления Linux клиентами необходимо в списке клиентов ДБ выбрать вкладку «Linux» (рис. 483).

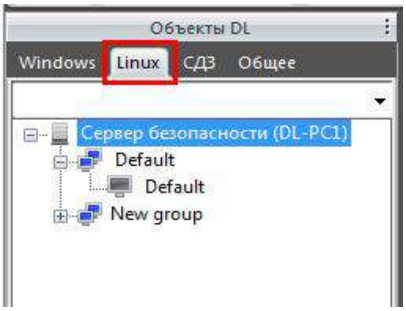


Рис. 483. Linux клиенты

19.11.1 Ввод клиента в ДБ

Для ввода Linux клиента/клиентов в ДБ, должны быть соблюдены следующие условия:

1. В ЛВС должен быть работающий СБ.
2. На СБ должны быть открыты TCP/IP порты 17496 и 17502, используемые для обмена данными с клиентами Linux.
3. Должен быть отключен МЭ на клиенте Linux.
4. Установить пользовательский (user.crt) и корневой (root.crt) сертификаты клиента Linux.

При вводе в ДБ количество пользователей в группе Linux клиента ограничено. В группе должно быть зарегистрировано не более 21 пользователя. В ином случае, могут возникнуть ошибки при синхронизации групп с СБ.

Для ввода одного клиента Dallas Lock Linux в ДБ необходимо:

1. Убедиться, что целевой клиент включен и доступен по сети для СБ.
2. На уровне СБ перейти на вкладку «Состояние» → «Основное» и нажать кнопку «Включить клиента в домен безопасности…».
3. В появившемся диалоговом окне необходимо заполнить следующие поля (рис. 484):
   - Клиент;
   - Администратор;
   - Пароль.

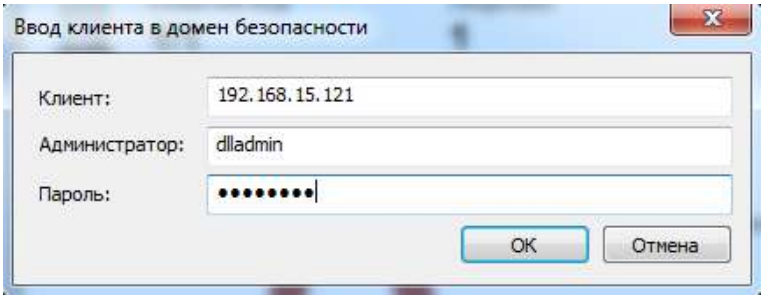


Рис. 484. Ввод клиента в ДБ

4. Нажать кнопку «ОК» после чего произойдет проверка доступности клиента и в дереве объектов

появится клиентский компьютер.

При попытке ввода клиента с включенным МЭ либо клиента, не доступного по сети, будет выведено сообщение об ошибке: «Ввод клиента невозможен. Проверьте настройки межсетевого экрана и доступность клиента по сети».

Для ввода нескольких клиентов в ДБ необходимо:

1. Убедиться, что целевые клиенты включены и доступны по сети для СБ.
2. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Включить клиентов в домен безопасности…».
3. Добавить клиентов для удаленных операций. Для этого доступны следующие операции:

 — добавить имя или IP-адрес клиента;

 — удалить имя или IP-адрес клиента;

 — добавить список клиентов из файла;

 — сохранить список клиентов в файл;

 — сканировать сеть;

 — удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 485).

Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном диапазоне возможно выводить адреса в числовом виде.

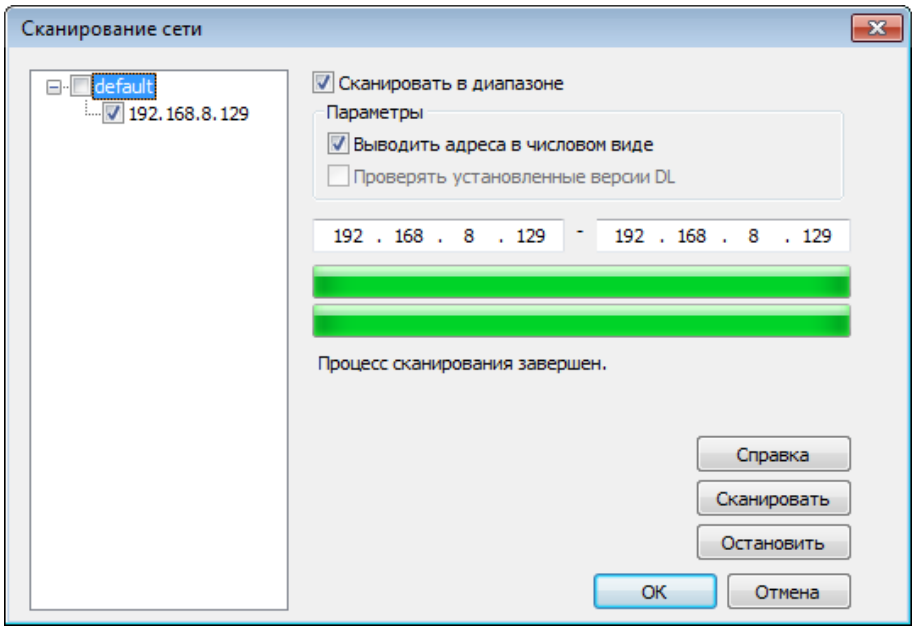


Рис. 485. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить».

4. Ввести логин и пароль администратора Dallas Lock Linux на целевых клиентах. Нажать кнопку «Продолжить».
5. Клиенты из списка будут введены в ДБ, сообщения об успешной операции появятся в списке (рис. 486).

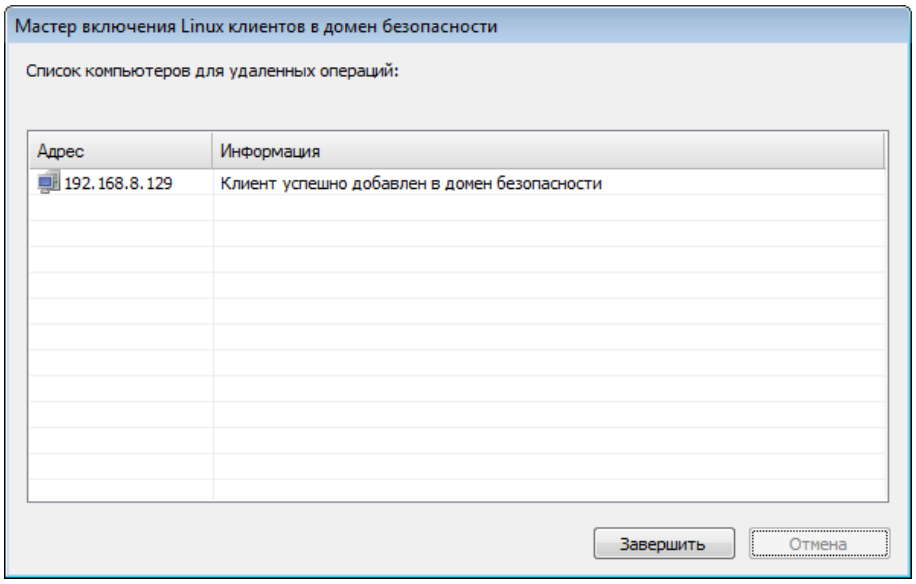


Рис. 486. Добавление клиента в ДБ

В дереве объектов КСБ появятся значки новых клиентов ДБ.

19.11.2 Вывод клиента из ДБ

Для вывода клиента через КСБ необходимо выбрать клиента в дереве объектов КСБ и на вкладке «Состояние» нажать кнопку «Удалить из ДБ» или выбрать соответствующую кнопку из контекстного меню, нажав правой кнопкой мыши по клиенту (рис. 487).

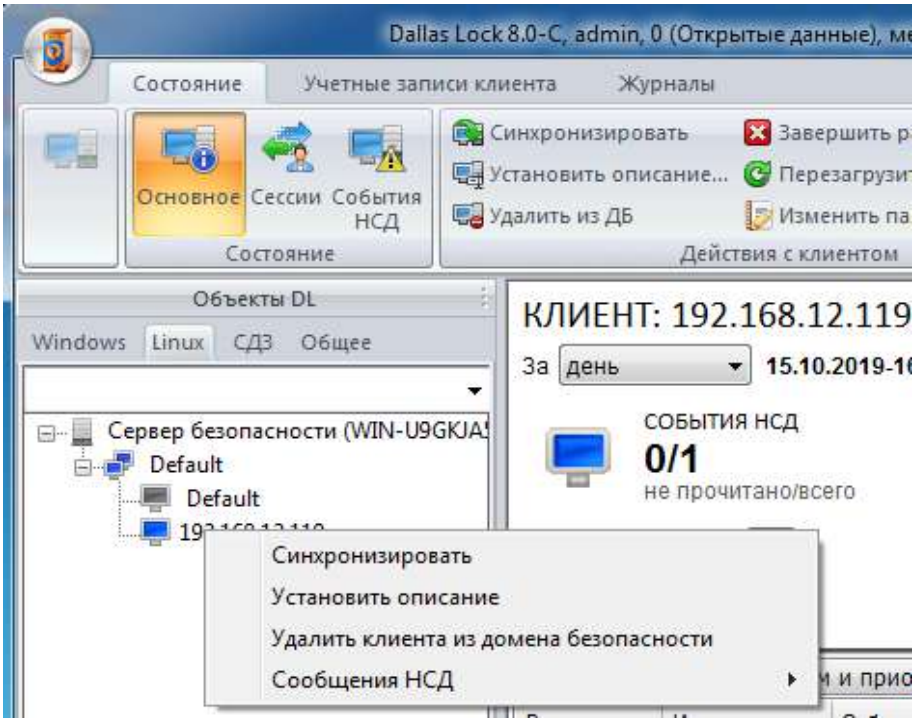


Рис. 487. Удаление клиента из ДБ в КСБ

Для вывода нескольких клиентов из ДБ одновременно необходимо:

1. Открыть вкладку КСБ «Состояние» на уровне СБ или группы клиентов и нажать кнопку «Удалить клиентов из домена безопасности…».
2. Добавить клиентов для удаленных операций. После добавления клиентов необходимо нажать кнопку «Продолжить».
3. Клиенты из списка будут удалены из ДБ, сообщения об успешной операции появятся в списке.

19.11.3 Централизованная установка Dallas Lock Linux

Существует возможность централизованно выполнить установку или удаление Dallas Lock Linux для

одного или нескольких компьютеров, расположенных в одной ЛВС.

Централизованная установка Dallas Lock Linux

Внимание! В процессе удаленной установки Dallas Lock Linux на клиентах автоматически создается учетная запись администратора Dallas Lock Linux с именем «*dlladmin*» и паролем «*dlladmin*». После установки рекомендуется сменить пароль администратора «*dlladmin*».

Внимание! Для установки Dallas Lock Linux требуется не менее 4.5 Гбайт пространствана жестком диске, из них не менее 100 Мбайт в /boot, не менее 1.5 Гбайт в /tmp, не менее 3 Гбайт в /.

Внимание! Удаленная установка Dallas Lock Linux невозможна на клиентах с ОС**:**

- ROSA Enterprise Linux Desktop x64;
- ROSA Enterprise Linux Server x64.

Удаленная установка возможна в следующих вариантах:

1. Для компьютеров следует использовать имя и пароль администратора ОС ЗАРМ и выполнять удаленную установку для группы компьютеров, имеющих одинаковые пароли администратора ОС ЗАРМ.
2. Для компьютеров, имеющих индивидуальные имя и пароль администратора ОС ЗАРМ, удаленную установку следует выполнять отдельно от других.

Необходимо выполнение следующих требований для удаленных операций:

1. При наличии модуля СОВ на СБ, на время централизованной установки рекомендуется выставить настройки уровней тревожности детекторов сетевых атак в значения по умолчанию или временно отключить модуль СОВ на СБ.
2. Наличие доступа к сети Интернет у целевых ПК.
3. При удаленном развертывании Dallas Lock Linux предварительно на целевых ПК необходимо установить и настроить SSH сервер. Рекомендуется использовать OpenSSH сервер. Установка клиента и сервера OpenSSH выполняется следующим образом.
   Для Ubuntu в терминале необходимо выполнить команды:
   - «sudo apt-get install openssh-server openssh-client».

   Для Debian, Astra Linux, Альт Рабочая станция в терминале необходимо выполнить команды:
   - «su (sudo для Astra Linux) apt-get install openssh-server openssh-client».

   Для CentOS, Fedora, RHEL, ЛотОС необходимо выполнить в терминале команды:
   - «su -c “yum install openssh-server openssh-client”».

   Для OpenSUSE в терминале необходимо выполнить команды[14]:
   - «zipper install openssh».

   В OpenSUSE пакет OpenSSH установлен по умолчанию.
   Для запуска службы OpenSSH необходимо выполнить команды:
   - для Ubuntu «sudo systemctl start ssh»;
   - для Debian «su -c “systemctl start ssh”»;
   - для CentOS, Fedora, RHEL, ЛотОС «su -c “systemctl start sshd.service”»;
   - для OpenSUSE «sudo systemctl start ssh»;
   - для Astra Linux «sudo systemctl start ssh»;
   - для Альт Рабочая станция «su -c “systemctl start ssh”».
4. По умолчанию пользователь root не имеет права на вход по SSH, для того, чтобы разрешить ему вход необходимо отредактировать конфигурационный файл sshd. Для OpenSUSE также необходимо включить аутентификацию по паролю.
   - открываем на редактирование файл: «/etc/ssh/sshd_config»;
   - ищем строку: «#PermitRootLogin no»;

[14] Если пакет OpenSSH не установлен по умолчанию.

- снимаем знак комментария «#»;
- изменяем значение на «yes» (PermitRootLogin yes);
- то же самое делаем со строкой «#PasswordAuthentication no»
- снимаем знак комментария «#»;
- изменяем значение на «yes» (PasswordAuthentication yes);
- перезапускаем демон sshd (команда «systemctl restart sshd»).

Для Debian, CentOS, Fedora, RHEL, ЛотОС, Astra Linux:

- открываем на редактирование файл «/etc/ssh/sshd_config»;
- ищем строку «PermitRootLogin no».
- изменяем значение на «yes» (PermitRootLogin yes);
- перезапускаем демон sshd (для Debian, Astra Linux — команда «systemctl restart ssh», для CentOS, Fedora, RHEL, ЛотОС — команда «systemctl restart sshd»).

Для Ubuntu:

- открываем на редактирование файл «/etc/ssh/sshd_config»;
- ищем строку с параметром PermitRootLogin;
- снимаем знак комментария «#», если он присутствует;
- изменяем значение на «yes» (PermitRootLogin yes);
- перезапускаем демон sshd (команда «systemctl restart ssh»).

Для Альт Рабочая станция:

- открываем на редактирование файл «/etc/openss/sshd_config»;
- ищем строку с параметром PermitRootLogin;
- снимаем знак комментария «#», если он присутствует;
- изменяем значение на «yes» (PermitRootLogin yes);
- перезапускаем демон sshd (команда «systemctl -c «restart ssh»).

после удаленной установки Dallas Lock Linux необходимо отключить SSH-сервер на целевых ПК.

Для удаленной установки Dallas Lock Linux необходимо выполнить следующие шаги:

1. На клиенте проверить список поддерживаемых протоколов по ssh — выполнить команду «*ssh – Q cipher».*

   Если в списке поддерживаемых протоколов нет следующих алгоритмов: 3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour, то в конфигурационный файл необходимо прописать «Ciphers +3des-cbc,aes192-cbc,aes128-cbc,arcfour128,arcfour»[15]. Сохранить файл после внесенных изменений.

   Примечание. СБ Dallas Lock для связи с Linux-клиентом использует алгоритмы шифрования «3des-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour», на стороне Linux-клиента список поддерживаемых алгоритмов может несущественно отличаться, и при этом удаленная установка СЗИ «Dallas Lock Linux» все равно будет возможна.

   После выполнения всех настроек в конфигурационном файле сервис sshd необходимо перезапустить.
2. Перед централизованной установкой необходимо разместить на компьютере, на котором запущена КСБ, дистрибутив Dallas Lock Linux.
3. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Установить СЗИ клиентов…».
4. Добавить клиентов для удаленных операций. Для этого доступны следующие операции:

    — добавить имя или IP-адрес клиента;

    — удалить имя или IP-адрес клиента;

    — добавить список клиентов из файла;

    — сохранить список клиентов в файл;

    — сканировать сеть;

[15] В ряде ОС символ «+» может не восприниматься, и строка будет считаться некорректной.

— удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 488). Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном диапазоне возможно выводить адреса в числовом виде.

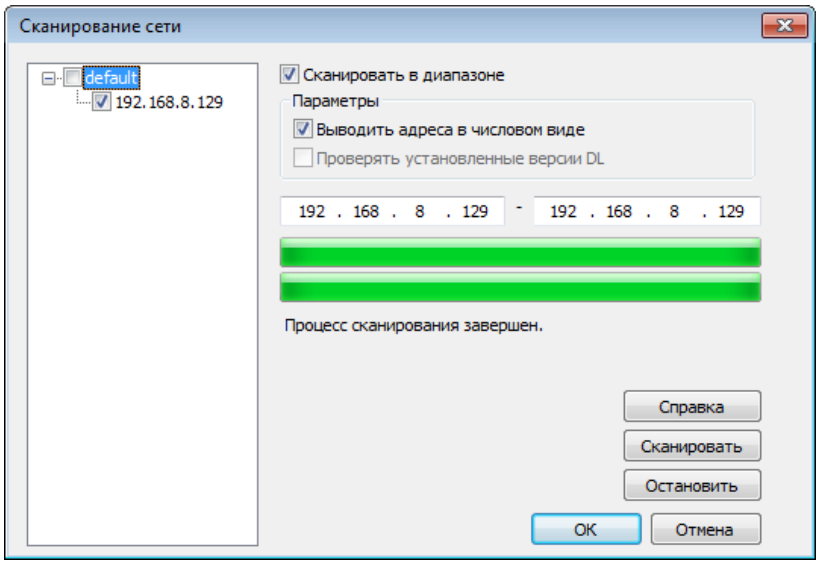


Рис. 488. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить».

5. Ввести логин и пароль администратора ОС на целевых клиентах (рис. 489).

Примечание. Необходимо установить флаг «Настройки клиентов требуют повышения привилегий» и заполнить учетные данные пользователя root. Для Ubuntu и Astra Linux флаг не устанавливать.

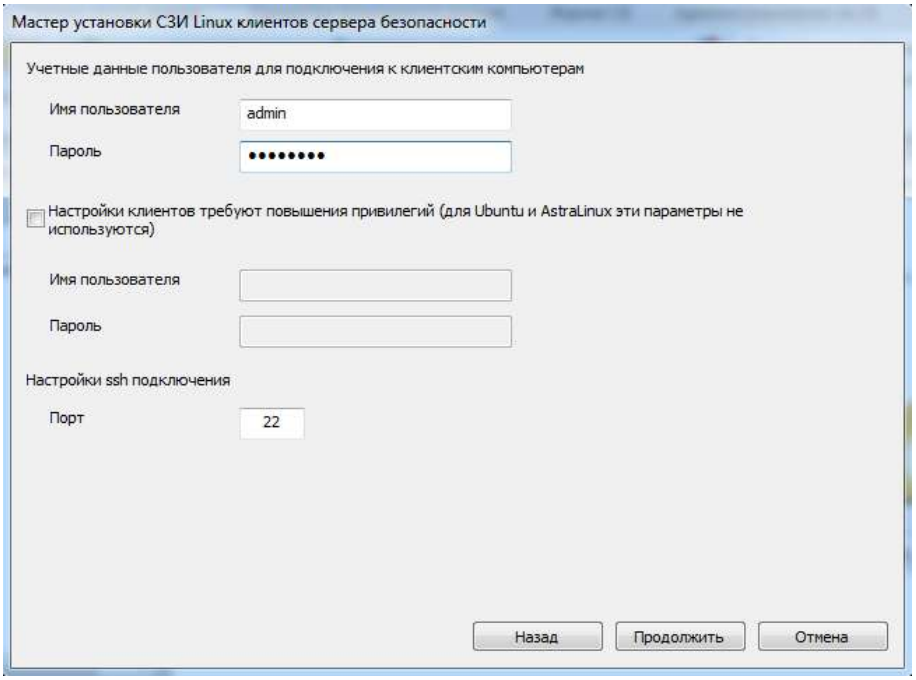


Рис. 489. Ввод учетных данных для подключения к Linux клиенту при централизованной установке

Для продолжения установки нажать кнопку «Продолжить».

6. Заполнить параметры установки, которые будут применены к клиентам в процессе активации Dallas Lock Linux (рис. 490):
   - номер лицензии и код технической поддержки, которые указаны на обложке футляра;
   - путь к папке с дистрибутивами Dallas Lock Linux.

В нижней части окна расположена информация о выбранных дистрибутивах для установки. Среди однотипных дистрибутивов выбирается самая новая версия.

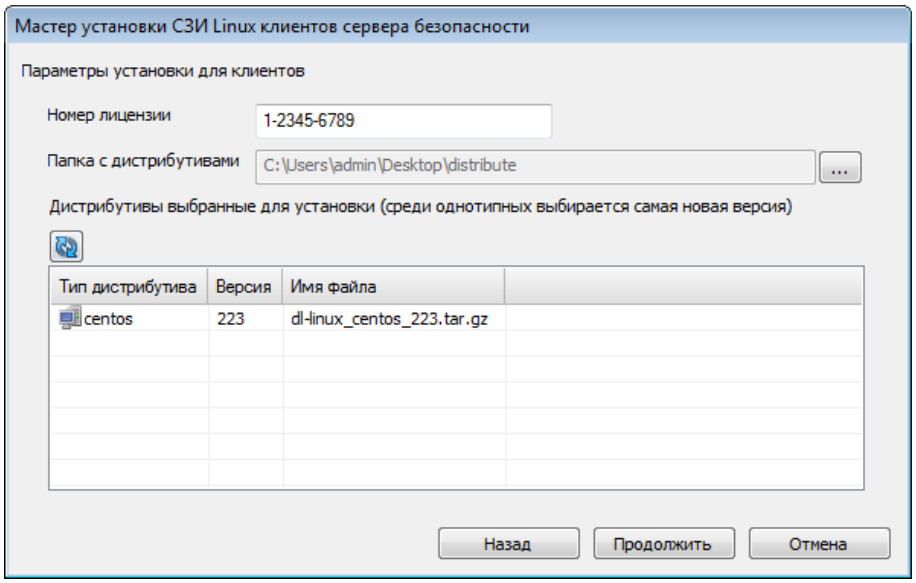


Рис. 490 Параметры установки для клиентов

Для продолжения установки нажать кнопку «Продолжить».

7. Далее можно просматривать состояние процесса установки для каждого клиента. Здесь же после централизованной установки появятся соответствующие комментарии удачного или не удачного завершения операции (рис. 491).

Примечание. Во время централизованной установки лог-файл процесса установки может быть переполнен. Прекращение ведения данного процесса не влияет на результат установки. В случае необходимости данный лог-файл можно найти на целевом клиенте.

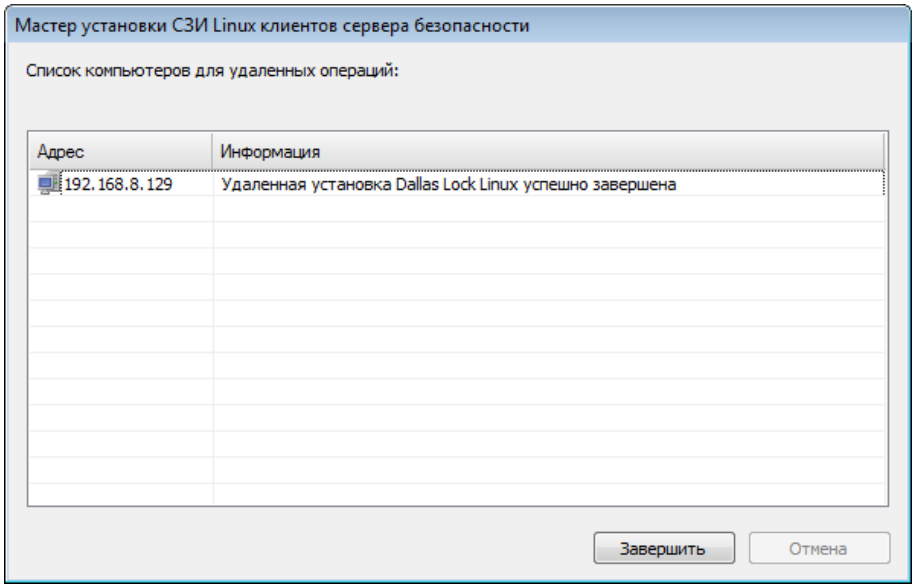


Рис. 491. Информация о ходе централизованной установки средствами КСБ

При выборе поля с комментарием в отдельном окне откроется список с историей событий в результате операции (рис. 492).

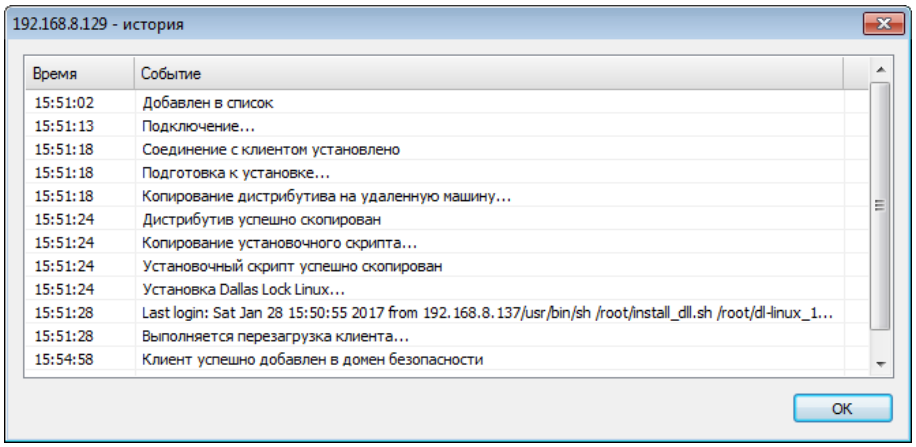


Рис. 492. Список событий в ходе централизованной установки

В дереве объектов КСБ появятся значки новых клиентов ДБ.

Централизованное удаление Dallas Lock Linux

Ряд предварительных настроек для централизованного удаления, аналогичны тем, что и в процессе централизованной установки (см. «Централизованная установка Dallas Lock 8.0 средствами СБ»)..

Для централизованного удаления необходимо выполнить следующие шаги:

1. Открыть вкладку «Состояние» на уровне СБ и нажать кнопку «Удалить СЗИ клиентов…».
2. Добавить клиентов для удаленных операций. Для этого доступны следующие операции:

 — добавить имя или IP-адрес клиента;

 — удалить имя или IP-адрес клиента;

 — добавить список клиентов из файла;

 — сохранить список клиентов в файл;

 — сканировать сеть;

 — удалить клиентов из списка.

При сканировании сети необходимо отметить клиентов и нажать кнопку «ОК» (рис. 493). Если отметить флагом «Сканирование в диапазоне», то становится доступным выбор диапазона IP-адресов, по которому будет произведен поиск клиентов. Для найденных клиентов в выбранном диапазоне возможно выводить адреса в числовом виде.

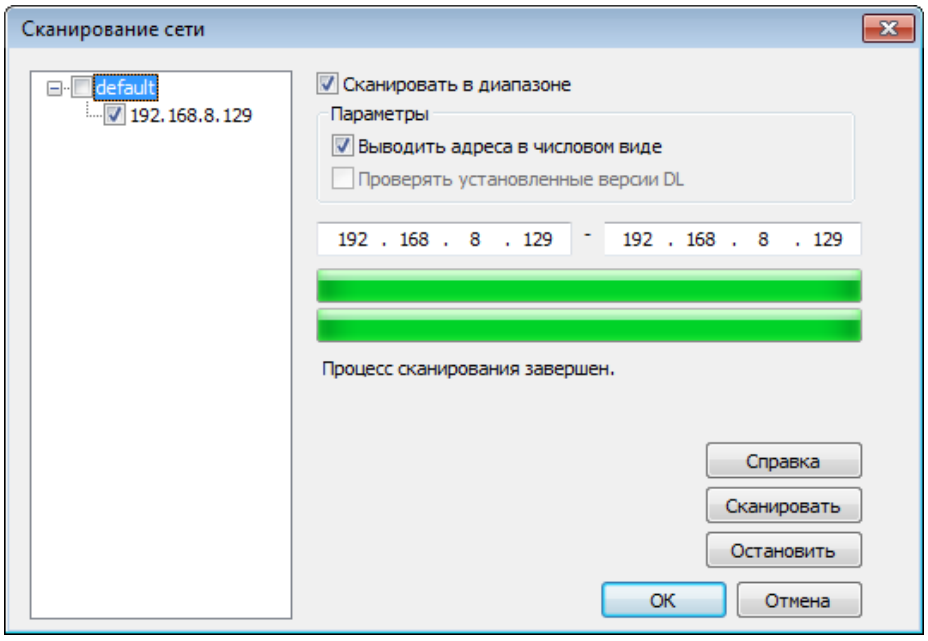


Рис. 493. Окно сканирования сети

После добавления клиентов необходимо нажать кнопку «Продолжить».

3. Ввести логин и пароль администратора Dallas Lock Linux на целевых клиентах.
4. Далее можно просматривать состояние процесса удаления для каждого клиента. Здесь же после централизованного удаления появятся соответствующие комментарии удачного или не удачного завершения операции (рис. 494).

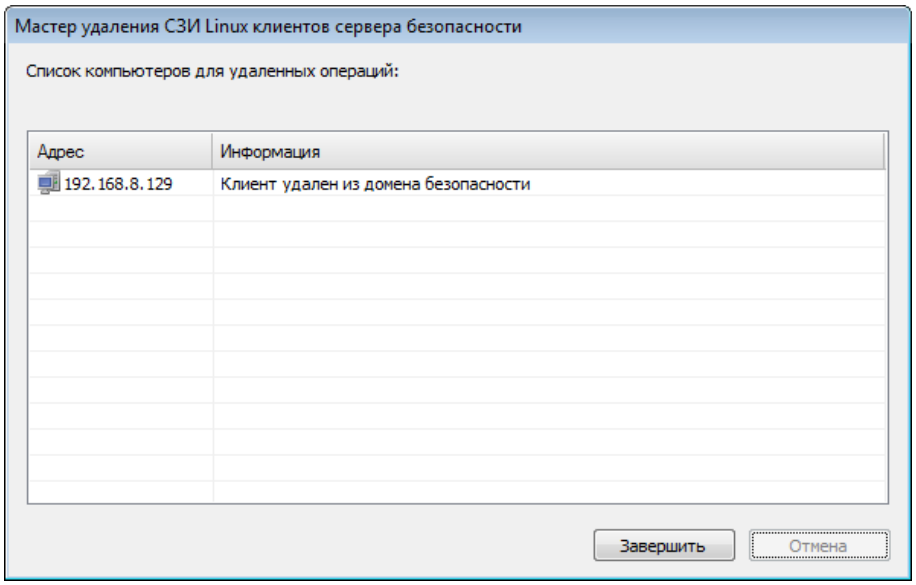


Рис. 494. Информация о ходе удаленного удаления средствами КСБ

При выборе поля с комментарием в отдельном окне откроется список с историей событий в результате операции (рис. 495).

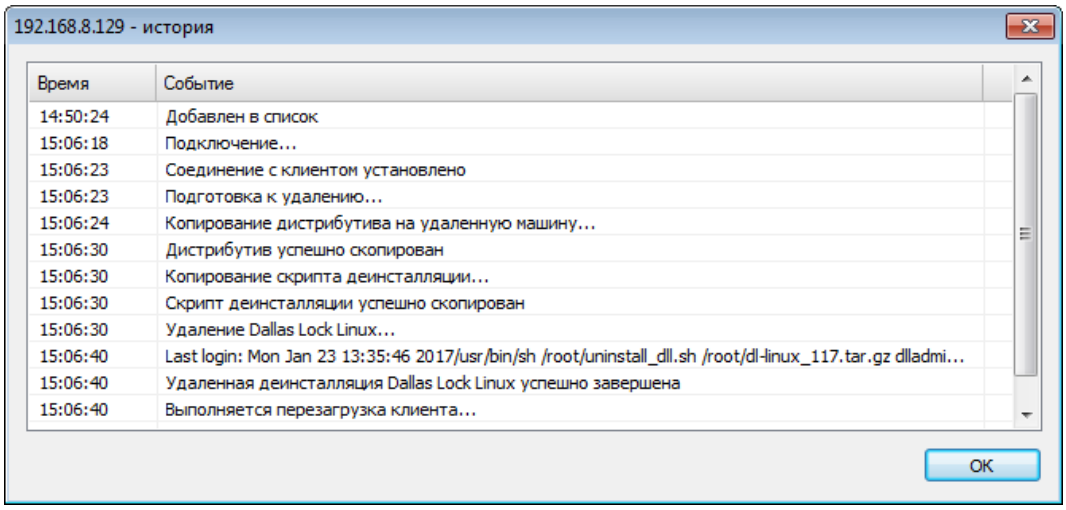


Рис. 495. Список событий в ходе удаленного удаления

В дереве объектов КСБ значок клиента удалится.

19.11.4 Параметры СБ для Linux клиентов

Для изменения параметров СБ необходимо открыть дополнительное меню КСБ → «Параметры сервера безопасности…» → «Linux».

Появится окно «Параметры сервера безопасности» для клиентов Linux (рис. 496).

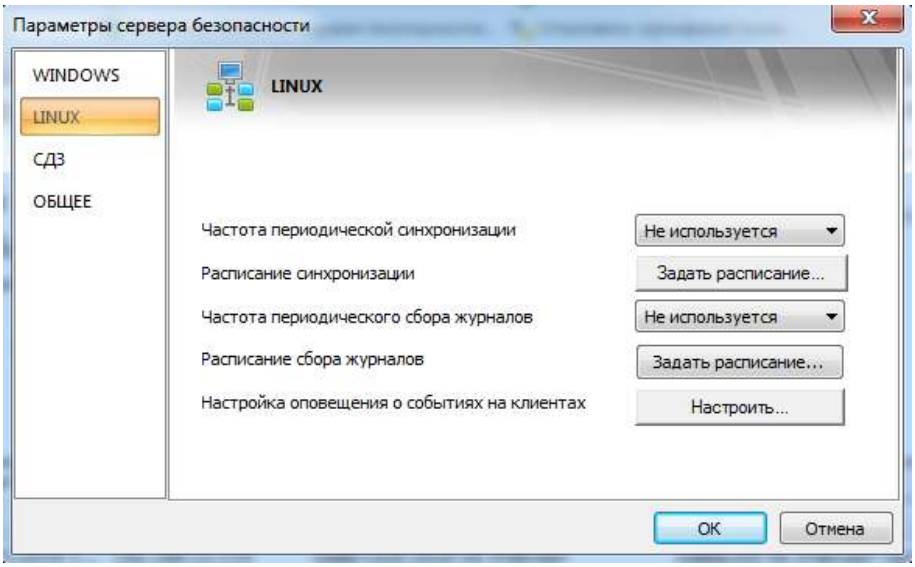


Рис. 496. Параметры СБ для Linux клиентов

Доступны следующие параметры.

Частота периодической синхронизации
Данный параметр позволяет производить автоматическую синхронизацию через указанный промежуток времени: от 10 минут до 24 часов (ежедневная синхронизация). Для отключения необходимо выбрать значение «Не используется».
Расписание синхронизации
Данный параметр позволяет настроить синхронизацию клиентов по гибкому расписанию. В окне настройки расписания необходимо включить контроль, поставив флаг в поле «Использовать расписание», и составить расписание.
Частота периодического сбора журналов
Данный параметр позволяет производить автоматический сбор журналов через указанный промежуток времени: от 5 минут до периода «ежемесячно». Для отключения необходимо выбрать значение «Не используется».

Расписание сбора журналов
Данный параметр позволяет настроить автоматический сбор журналов по гибкому расписанию. В окне настройки расписания необходимо включить контроль, поставив флаг в поле «Использовать расписание», и составить расписание.
Настройка оповещения о событиях на клиентах
Данный параметр позволяет настроить оповещения о событиях НСД на клиенте и почтовые уведомления (см. «Сигнализация об НСД»).

Сигнализация об НСД

Ситуации НСД на клиентах отслеживаются и сопровождаются сигнализацией на СБ. Сообщения о событиях НСД заносятся в журнал СБ. Сообщения о событиях клиента приходят на СБ пачками с интервалом (около 30 секунд), при этом время каждого события записывается фактическое, когда событие произошло на клиенте. На ПК с запущенной КСБ воспроизводится звуковой сигнал и выводится всплывающее сообщение на панели задач (рис. 497).

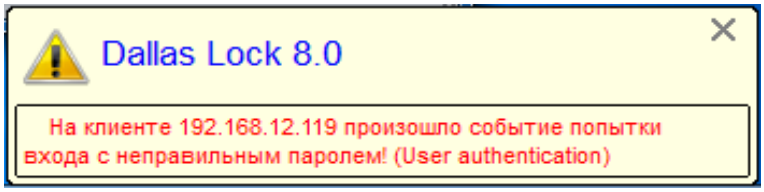


Рис. 497. Сигнализация на СБ

Для настройки оповещений и звукового сигнала необходимо открыть дополнительное меню КСБ  → «Параметры сервера безопасности…» → «Linux» → нажать кнопку «Настроить» для параметра «Настройка оповещения о событиях на клиентах».

Доступны следующие параметры.

Нарушение контроля целостности контролируемых объектов
При включении данного параметра осуществляется оповещение о нарушении контроля целостности объекта. Сигнализация при нарушении целостности происходит при ее проверке.
Попытка входа с неправильным паролем
При включении данного параметра осуществляется оповещение о попытке входа пользователя с неправильным паролем.
Пользователь блокирован после многократного ввода неправильного пароля
При включении данного параметра осуществляется оповещение о блокировке пользователя после многократного ввода неправильного пароля (настраивается параметром безопасности «Вход: максимальное количество ошибок ввода пароля»).
Попытка получения доступа к запрещенному устройству
При включении данного параметра осуществляется оповещение о попытке получения доступа к запрещенному устройству.
Dallas Lock на клиенте не отвечает
При включении данного параметра осуществляется оповещение о том, что система защиты Dallas Lock Linux клиента не отвечает СБ. Возможная причина — несанкционированная деактивация системы защиты. Клиент в дереве КСБ будет отображаться специальным знаком  .
Клиент недоступен долгое время
При включении данного параметра осуществляется оповещение об отсутствии связи клиента с СБ в течение длительного периода. Период определяется параметром «Оповещение при отсутствии связи с клиентом».
Оповещение при отсутствии связи с клиентом

Данным параметром устанавливается максимальный срок отсутствия связи клиента с СБ. По истечении установленного срока клиент в дереве КСБ будет отображаться специальным знаком  .
Звуковой сигнал при событии НСД
Данный параметр позволяет включить звуковой сигнал при регистрации события НСД. Звуковой сигнал воспроизводится на ПК с запущенной КСБ.
Подключить уведомления по почте
Данный параметр позволяет подключить автоматическую отправку уведомлений о событиях НСД на электронную почту (см. «Отправка почтовых уведомлений об НСД»).

События сигнализации отображаются в полученных с клиентов журналах, а также в интерфейсе КСБ на уровне клиента в категории «Состояние» → «События НСД».

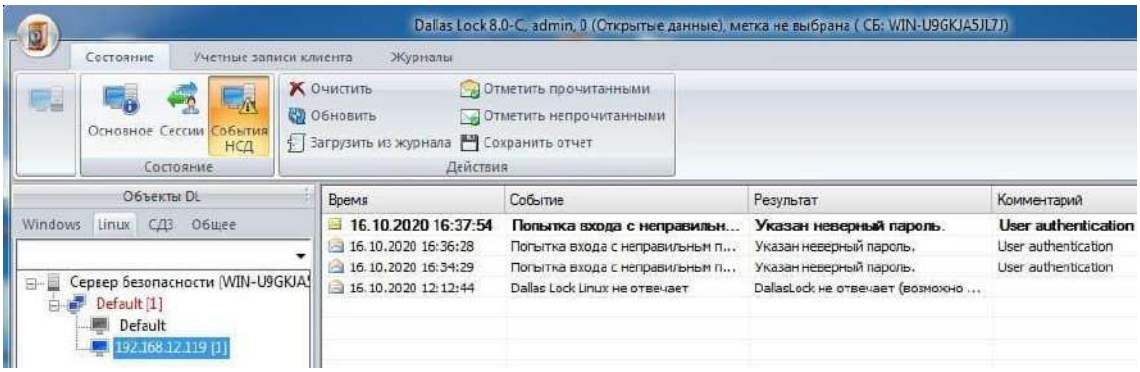


Рис. 498. Журнал событий сигнализации об НСД

Список событий НСД клиента собирается из журналов клиента.

С помощью панели действий для списка событий НСД возможно отметить все записи прочитанными или непрочитанными, обновить, очистить список и загрузить новый список НСД из журналов клиента. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

Общее состояние всего ДБ возможно узнать на уровне СБ в категории «Состояние» → «Основное» (см. «Основное»).

Также количество полученных новых (непрочитанных) сообщений дополнительно отображается в дереве объектов КСБ: после имени клиента и наименования группы (общее количество сообщений с клиентов данной группы), после имени СБ (общее количество сообщений с клиентов всего ДБ) (рис. 499).

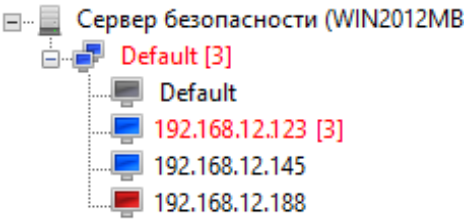


Рис. 499. Визуальное отображение оповещений о полученных событиях НСД

Операции с сообщениями НСД дополнительно доступны из контекстного меню выбранного объекта в дереве объектов КСБ.

Отправка почтовых уведомлений об НСД

Реализована возможность отправки почтовых уведомлений на e-mail (электронную почту) с СБ о событиях, связанных с НСД на клиентах ДБ.

Для настройки почтовых уведомлений об НСД необходимо открыть дополнительное меню КСБ  → «Параметры сервера безопасности…» → «Linux» → нажать кнопку «Настроить» для параметра «Настройка оповещения о событиях на клиентах». В окне «Настройка уведомлений сервера» отменить параметр «Подключить уведомления по почте» и нажать кнопку «Настроить уведомления по почте…».

Дальнейшая настройка выполняется аналогично тому, как это осуществляется для Windows

клиентов (см. «Отправка почтовых уведомлений об НСД»).

19.11.5 Настройка СБ для всего ДБ

На уровне СБ в верхней части консоли формируется набор вкладок для общей настройки параметров безопасности всего ДБ, всех клиентов данного СБ. При выборе определенной вкладки появляется возможность просматривать и редактировать параметры безопасности.

Состояние СБ

Вкладка «Состояние» на уровне СБ отображает общее состояние ДБ. Доступны следующие категории.

Основное

Для удобства работы возможно узнать общее состояние всего ДБ для Windows, Linux и СДЗ клиентов.

Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

Доступны следующие действия с ДБ:

- по команде синхронизировать клиентов с СБ;
- настроить сбор журналов;
- по команде собрать журналы с клиентов;
- добавить группу;
- включить клиента в ДБ;
- включить клиентов в ДБ;
- удалить клиентов из ДБ;
- установить сертификат (root) или (user);

Внимание! Смена сертификатов на СБ влечет необходимость смены сертификатов на всех клиентах ДБ.

- установить или удалить Dallas Lock Linux с клиентов.

Лицензии

Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Лицензии»).

Учетные записи домена

Вкладка «Учетные записи домена» на уровне СБ позволяет управлять учетными записями ДБ. На всех клиентах ДБ могут работать учетные записи только из списка учетных записей ДБ (рис. 500).

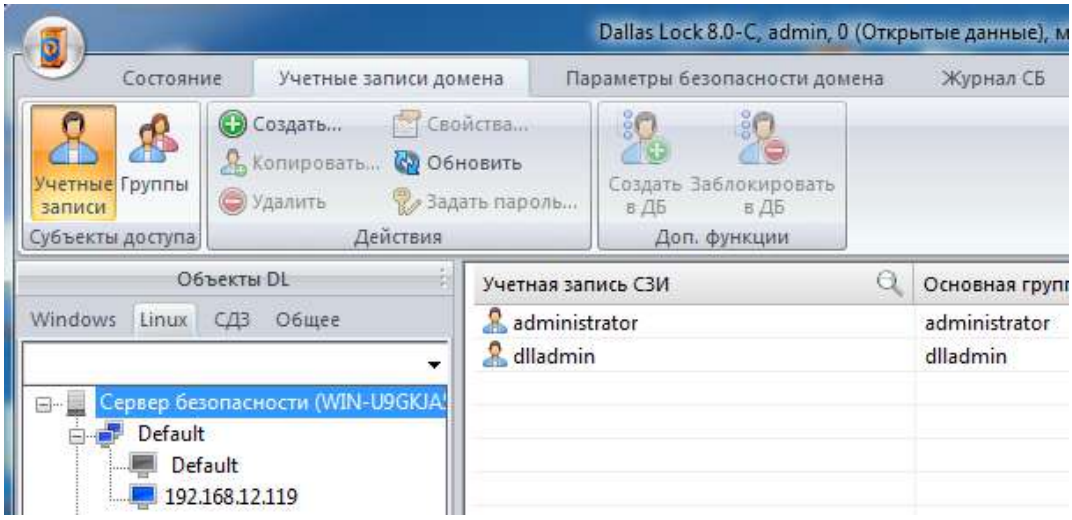


Рис. 500. Учетные записи Linux

Создание пользователей в ДБ

Для создания нового пользователя необходимо:

1. Нажать кнопку «Создать» на панели «Действия» или в контекстном меню, вызываемом щелчком правой кнопки мыши в рабочей области.
2. Выбрать размещение учетной записи и указать логин создаваемого пользователя (рис. 501).

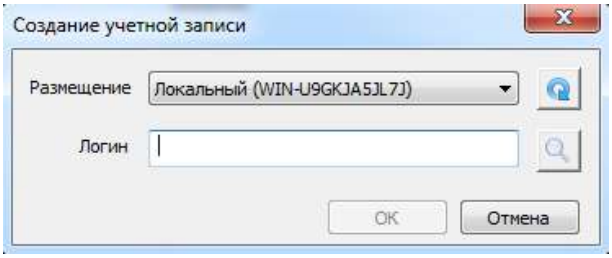


Рис. 501. Создание учетной записи

3. На экране появится окно изменения основных параметров пользователя (рис. 502).

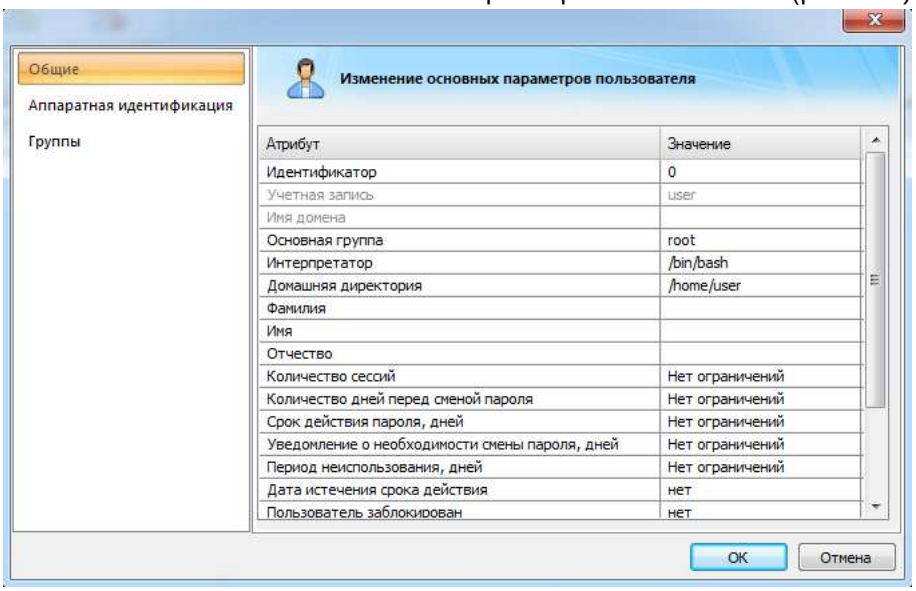


Рис. 502. Создание учетной записи Linux

4. На вкладке «Общие» предлагается заполнить следующие учетные данные и параметры:
   - «Идентификатор» — системный идентификатор учетной записи пользователя. Принимает значения от 0 до 65534. По умолчанию устанавливается и используется следующий доступный идентификатор в системе. Необязательный атрибут.
   - «Основная группа» является обязательным параметром. Наименование основной группы пользователя. При добавлении пользователя группа уже должна быть создана — необходимо выбрать ее из выпадающего списка.
   - «Интерпретатор» является обязательным параметром. В данном поле указывается полный путь к файлу. Указанный файл должен иметь права на чтение и запуск для всех пользователей.
   - «Домашняя директория» является обязательным параметром. Формат заполнения: /home/*имя учетной записи*.
   - Параметры «Фамилия», «Имя» и «Отчество» заполняются по мере необходимости.
   - «Количество сессий». Максимально допустимое значение сессий, создаваемое от имени учетной записи пользователя. Принимает значения от 0 до 10. По умолчанию, выставлено значение «Нет ограничений».
   - «Количество дней перед сменой пароля». Период (дней), после истечения срока действия пароля, в течение которого пользователь может входить в ОС, используя старый пароль, но будет выдаваться предупреждение о необходимости сменить пароль. Если период истек, учетная запись пользователя блокируется. Принимает значения от 0 до 180. По умолчанию выставлено значение «Нет ограничений».
   - «Срок действия пароля» в днях. После истечения срока действия пароля учетной записи система будет требовать смену пароля учетной записи пользователя. Принимает значения от 0 до 180. По умолчанию выставлено значение «Нет ограничений».
   - «Уведомление о необходимости смены пароля». Значение (в днях), после которого

пользователю будут выдаваться уведомление о необходимости смены пароля с указанием количества дней до истечения срока действия пароля. Принимает значения от 0 до 180. По умолчанию выставлено значение «Нет ограничений».

- «Период неиспользования». Принимает значения от 0 до 180 дней. Если период, в который под учетной записью не производился вход в систему, превышает выбранный допустимый период — учетная запись блокируется. По умолчанию выставлено значение «Нет ограничений».
- «Дата истечения срока действия». В поле «Дата» устанавливается флаг и указывается дата, когда данная учетная запись будет заблокирована системой. В этом случае поле «Дата» обязательно для заполнения. При пустом флаге — поле «Дата» неактивно. Время действия не ограничено.
- «Пользователь заблокирован». Если флаг «да» — учетная запись блокируется (учетная запись неактивна), вход в ОС на ЗАРМ запрещен. Для пользователей, в данный момент работающих в системе в момент блокировки учетной записи — сеанс не блокируется, блокируется следующий вход в систему. Если флаг «нет» — учетная запись активна, вход в ОС на ЗАРМ разрешен.
- «Смена пароля». Если флаг «да» — при входе в ОС, пользователю необходим сменить пароль. Если значение «нет» — требование изменения пароля отображено не будет;
- «Создать домашнюю директорию». Если при создании учетной записи пользователя не будет создана домашняя директория, то вход в систему для этой учетной записи будет невозможен.
- «Системный пользователь». Если флаг «да» — пользователь является системным. Если флаг «нет» — пользователь системным не является.
- «Роль администрирования». При нажатии на поле появляется выпадающий список доступных ролей для пользователя: администратор, аудитор, пользователь.

5. На вкладке «Аппаратная идентификация» пользователю назначается аппаратный идентификатор как это описано в подразделе «Назначение аппаратной идентификации».
6. На вкладке «Группы» возможно добавить пользователя в группу.
7. После всех произведенных настроек необходимо нажать кнопку «ОК» и в появившемся окне задать пользователю пароль. Нажать кнопку «ОК».

После создания учетных записей, они автоматически появляются в списках учетных записей объектов ДБ: каждой группы (подгруппы) клиентов и каждого клиента.

Для каждой группы (подгруппы) клиентов и для каждого клиента возможно индивидуально определить, какие учетные записи из списка смогут работать на данных клиентах, а какие нет.

Для того, чтобы отметить учетную запись для работы на клиентских ПК во всем ДБ, необходимо выделить учетную запись и нажать кнопку «Создать в ДБ (рис. 503). Созданная в ДБ учетная запись будет отмечена флагом для всех клиентов и групп клиентов. Для того, чтобы запретить доступ на всех клиентах ДБ, нужно выделить учетную запись и нажать «Заблокировать в ДБ».

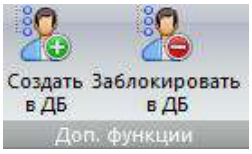


Рис. 503. Создание пользователя в ДБ

На всех клиентах, входящих в ДБ, параметры отмеченных пользователей будут идентичны.

Настройка учетных записей для групп и подгрупп клиентов описана в разделе «Учетные записи группы клиентов».

Настройка учетных записей для клиентов описана в разделе «Учетные записи клиента».

Создание группы пользователей ДБ

Список групп ДБ в категории «Учетные записи домена» → «Группы» формируется из групп, зарегистрированных через КСБ.

В процессе синхронизации списки групп пользователей клиента и ДБ сравниваются, из списка клиента удаляются группы, которых нет в списке ДБ, и добавляются новые, которые уже добавлены в список ДБ, но не добавлены в список групп пользователей клиента. Таким образом, на всех клиентах, будут одинаковые группы.

Для создания новой группы Linux необходимо:

1. Нажать кнопку «Создать».
2. Заполнить параметры новой группы: (рис. 504):
   - имя группы;

- опционально описание группы;
- поставленный флаг «Системная» означает, что информация по данной группе будет записана в файлы ОС на Linux клиенте.

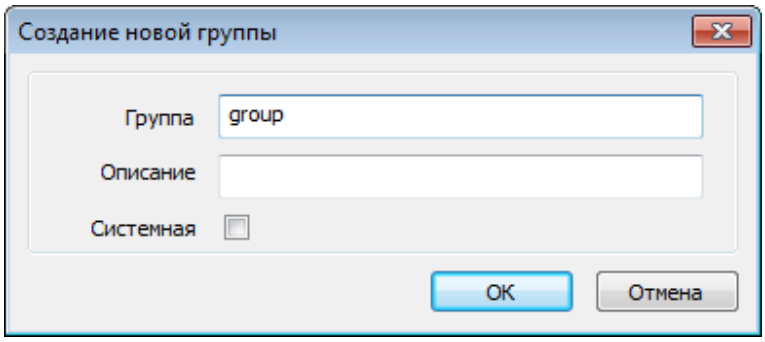


Рис. 504. Окно создания новой группы

3. Нажать кнопку «ОК».

Изменить описание группы можно, используя кнопку «Свойства» или выбрав данное действие из контекстного меню.

Для удаления группы необходимо выделить группу, которую следует удалить, нажать кнопку «Удалить» или выбрать данное действие в контекстном меню. На экране отобразится подтверждение на удаление.

Параметры безопасности домена

Доменные настройки пароля

Категория «Параметры безопасности домена» → «Вход» позволяет управлять настройками паролей, сессий, параметрами входа и домена на уровне всего ДБ (рис. 505). Для применения настроек на клиентах необходима синхронизация.

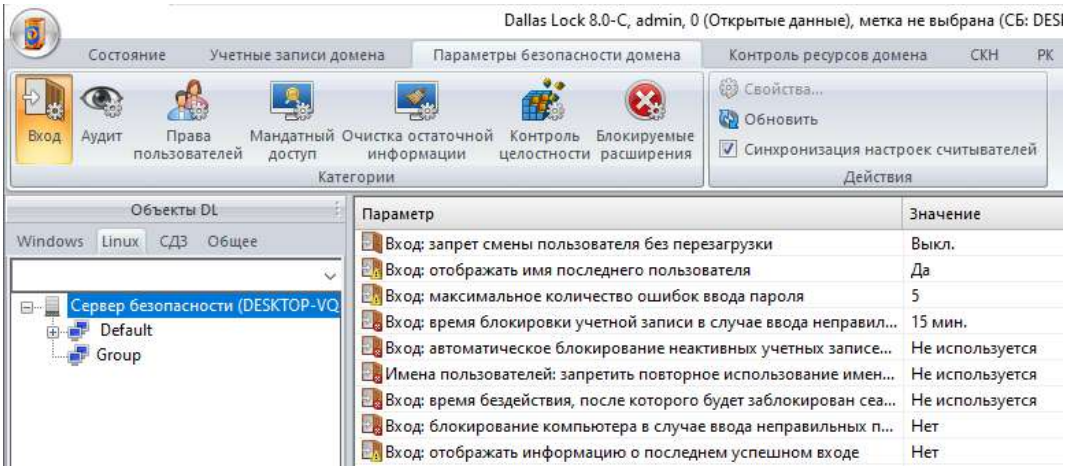


Рис. 505. Настройки параметров безопасности домена. Linux

Внимание! Максимальная допустимая длина пароля в СЗИ составляет 31 символ.

Доступны следующие параметры.

Пароли: минимальная длина
Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение. При выборе значения «Не используется» устанавливаемый пароль может иметь пустое значение. При регистрации нового пользователя и при изменении старого пароля система защиты контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «Пароль не соответствует текущим политикам Dallas Lock на сложность паролей. Введен слишком короткий пароль».

При этом новый пароль сохраняется, и учетная запись создается. По умолчанию минимальная длина пароля составляет 8 символов.
Пароли: необходимо наличие специальных символов
Если данный параметр включен, то при создании пароля в нем должны присутствовать специальные символы из следующего списка: «!», «@», «#», «$», «%», «&», «‘», «“», «)», «(», «*», «+», «,», «-», «.», «/», «;», «:», «<», «>», «?», «[», «]», «\», «^», «_», «{», «}», «~», «|», «=».
Пароли: необходимо наличие цифр
Если данный параметр включен, то при создании пароля в нем должны присутствовать цифры.
Пароли: необходимо наличие строчных и прописных букв
Если данный параметр включен, то при создании пароля в нем должны присутствовать строчные и прописные буквы.
Вход: максимальное количество ошибок ввода пароля
Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. В выпадающем списке можно выбрать число попыток от 1 до 10. Если при входе на АРМ или на этапе загрузки ОС пользователь ввел неверный пароль, то система выдаст предупреждение «Указан неверный пароль». Если число ошибок больше допустимого, учетная запись будет заблокирована и пользователь не сможет загрузить компьютер и ОС. По умолчанию минимальное количество попыток ввода неверного пароля составляет 3 ввода пароля. Если установлено значение «Не используется», то пользователь может вводить неверный пароль неограниченное число раз.
Максимальное количество сессий
Данный параметр позволяет задать максимальное количество разрешенных сессий на клиенте. Если установлено значение «Не используется», то параметр будет отключен.
Таймаут блокировки сессий
Данный параметр позволяет осуществлять автоматическую блокировку сессии учетной записи пользователя через определенное время неактивности данной учетной записи. Если установлено значение «Не используется», то параметр будет отключен.
Домен
При редактировании данного параметра вводится имя домена, для работы с которым настроено СЗИ НСД Dallas Lock Linux.
Разрешить авторизацию всем пользователям домена
Значение «Да» данного параметра разрешает авторизацию всем пользователям домена, для работы с которым настроено СЗИ НСД Dallas Lock Linux. По умолчанию значение данного параметра — «Нет».

Доменные настройки аудита

Категория «Параметры безопасности домена» → «Аудит» позволяет управлять настройками аудита на уровне всего ДБ (рис. 506). Для применения настроек на клиентах необходима синхронизация.

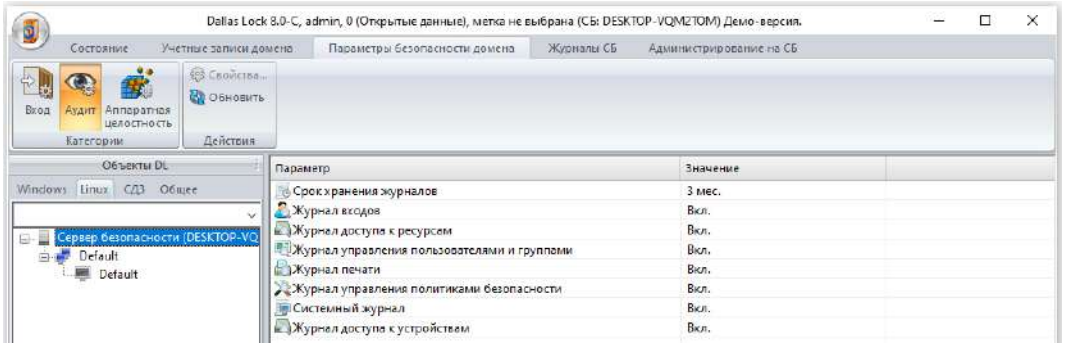


Рис. 506. Настройки аудита

Доступны следующие параметры.

Срок хранения журналов
Параметр устанавливает срок хранения журналов (в месяцах). По умолчанию 3 месяца.
Журнал входов
Включение журнала позволяет протоколировать в нем события аутентификации пользователей в ОС.
Журнал доступа к ресурсам
Включение журнала позволяет протоколировать в нем события, связанные с настройками правил разграничения доступа и обращения к защищаемым объектам доступа.
Журнал управления пользователями и группами
Включение журнала позволяет протоколировать в нем события, связанные с настройками и созданием учетных записей пользователей, групп учетных записей.
Журнал печати
Включение журнала позволяет протоколировать в нем события печати, выполненные с локальных печатающих устройств.
Журнал управления политиками безопасности
Включение журнала позволяет протоколировать в нем события изменения политик безопасности.
Системный журнал
Включение журнала позволяет протоколировать в нем события системного журнала ОС (SysLog).
Журнал доступа к устройствам
Включение журнала позволяет протоколировать в нем события, связанные настройками доступа к подключенным устройствам.

Доменные настройки аппаратной целостности

Категория «Параметры безопасности домена» → «Аппаратная целостность домена» позволяет управлять настройками аппаратной целостности на уровне всего ДБ (рис. 507). Для применения настроек на клиентах необходима синхронизация.

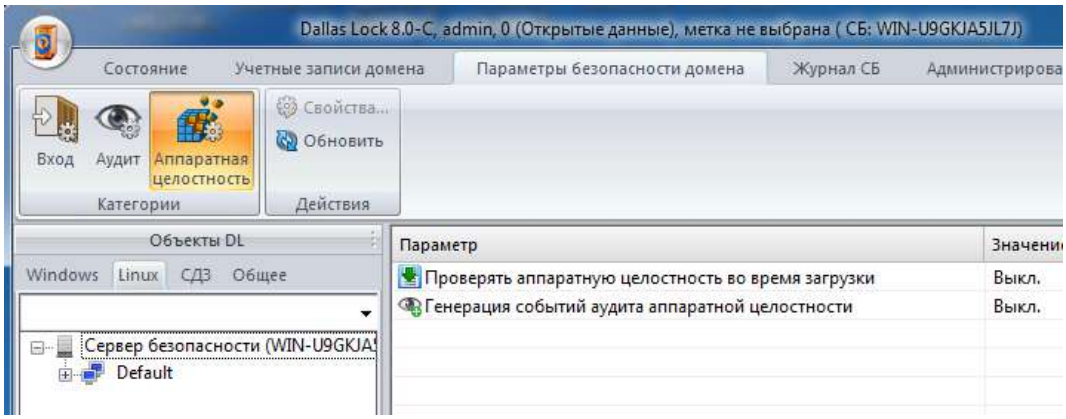


Рис. 507. Аппаратная целостность

Доступны следующие параметры.

Проверять аппаратную целостность во время загрузки
Параметра позволяет осуществлять автоматическую проверку целостности аппаратной среды при загрузке системы на клиенте.
Генерация событий аудита аппаратной целостности
Параметра включает протоколирование событий нарушения аппаратной целостности на клиенте DLL.

Журнал СБ

На вкладке «Журнал СБ» в категории «Журнал СБ» отображаются регистрируемые события, связанные непосредственно с работой СБ (рис. 508).

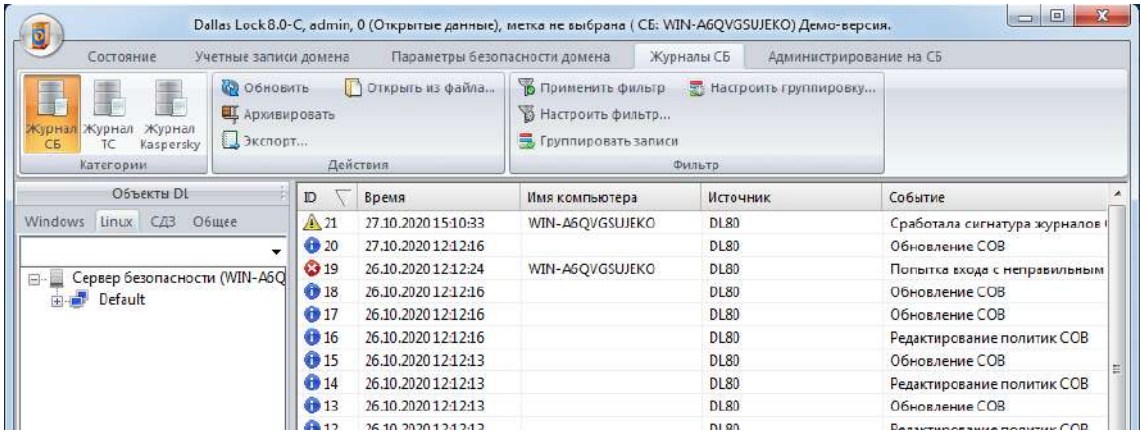


Рис. 508. Журнал СБ

Данный журнал един для всех клиентов ДБ: Windows, Linux и СДЗ. Подробнее о журнале СБ см. «Журнал СБ», подробнее о полученных с клиентов журналах см. «Журналы клиента СДЗ».

В категории «Журнал ТС» отображаются новостные сообщения от производителя (рис. 509).

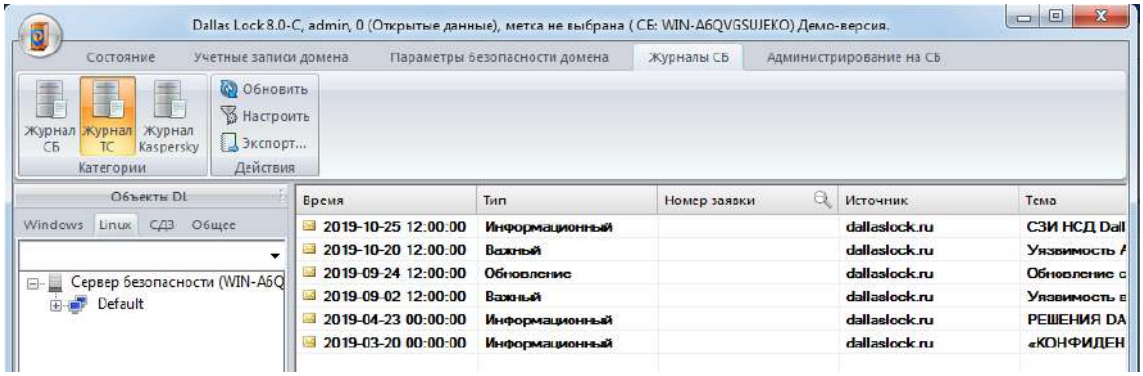


Рис. 509. Журнал ТС

Данный журнал един для всех клиентов ДБ: Windows, Linux и СДЗ. Подробнее о журнале СБ см. «Журнал СБ».

Для клиентов Linux можно настроить какие журналы необходимо собирать с клиентов, которые находятся под управлением СБ. На уровне СБ на вкладке «Состояние» на кнопке «Основное» на панели «Действия с доменом» есть кнопка «Настроить сбор журналов». При нажатии на эту кнопку появляется диалоговое окно «Политика сбора журналов» (Рис. 510). Следует отметить галочками, какие журналы следует собирать с клиента и нажать «ОК». Данные с выбранных журналов будут отображаться на вкладке «Журналы СБ».

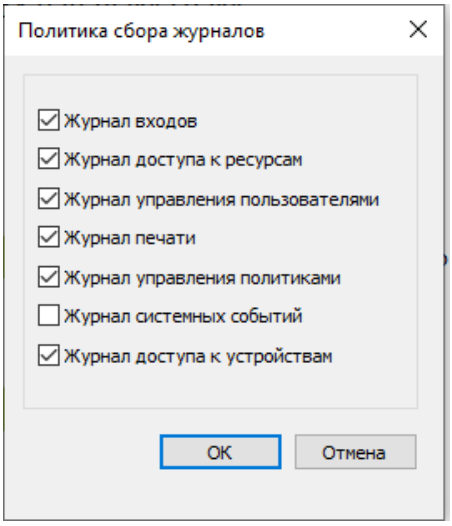


Рис. 510. Политика сбора журналов

Журналы ДБ

Вкладка «Журналы» доступна только при использовании базы данных MS SQL Server. Она позволяет просматривать собранные СБ журналы со всех Linux клиентов ДБ (рис. 511).

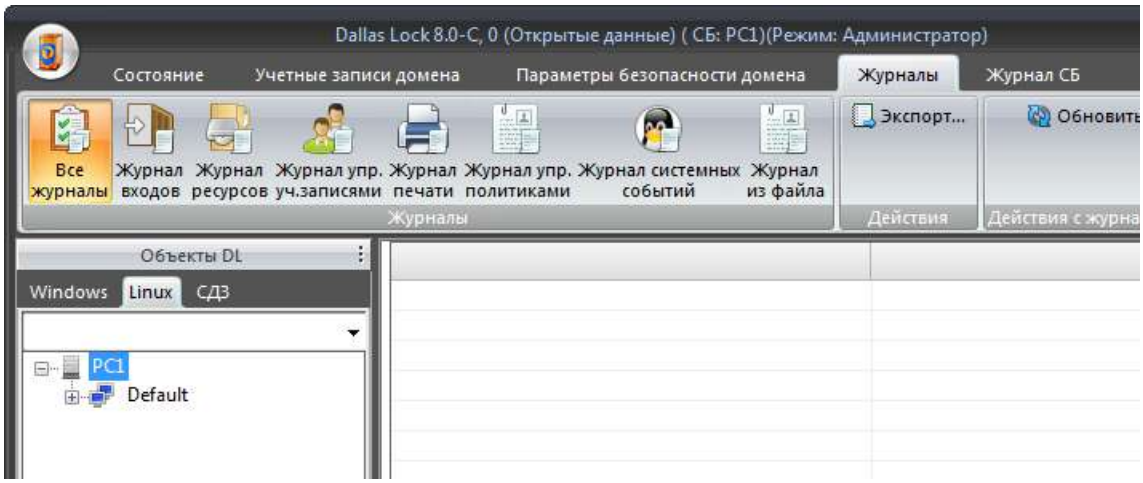


Рис. 511. Вкладка КСБ полученных с клиента журналов

В случае возникновении сбоя при сохранении данных аудита, собранные файлы журналов хранятся на СБ до тех пор, пока не будут загружены в БД. Зачистка файла журнала на клиенте выполняется только при успешной передаче файла СБ.

Формирование этих журналов и записей в них происходит на момент команды сбора журналов путем нажатия данной кнопки на вкладке «Состояние» клиента или на вкладке «Состояние» СБ, а также при настроенном периодическом сборе журналов в параметрах данного СБ.

Панель «Действия» аналогична той, что есть в оболочке администратора Dallas Lock 8.0: имеется возможность архивации записей, экспорта записей в файл в выбранном формате, настройка и применение фильтра, группировка записей (см. «Журналы»).

Примечание. С помощью клавиши «Delete» можно удалить файл журнала клиента в КСБ. Для этого выполнить следующее:

1. Выделить выбранный файл в журнале клиента и нажать клавишу «Delete».
2. Перед удалением файла из журнала пользователю выводится соответствующее сообщение.
3. При положительном ответе происходит удаление файла из журнала, при отрицательном операция будет отменена.

19.11.6 Клиенты и группы клиентов СБ

Группа Default и клиент Default

В дереве объектов КСБ всегда присутствуют группа «Default» и клиент «Default».

Примечание. При добавлении нового клиента в ДБ он всегда помещается в группу «Default» при следующих условиях:

1. Настройки безопасности для него копируются из настроек группы «Default».
2. Списки учетных записей и ключей преобразования копируются из списка клиента «Default».

Создание группы клиентов возможно, как на уровне родительского объекта «СБ», так и на уровне родительского объекта «группа», поэтому:

1. При создании в дереве объектов новой группы на уровне СБ («Состояние» → «Добавить группу…») для нее копируются параметры безопасности группы Default.
2. При создании новой группы как подгруппы (объект группы → «Добавить подгруппу…») для нее копируются параметры безопасности родительской группы.

В дальнейшем, администратор СБ ЗАРМ может перенести нового клиента в любую другую группу, а также любую группу в качестве подгруппы в другую группу. Для этого можно воспользоваться контекстным меню («Переместить») или перетащить значок нужного объекта кнопкой мыши в поле другого значка («Drag-and-drop»).

При выборе каждой группы (подгруппы) и каждого клиента КСБ будет иметь типовой набор вкладок управления параметрами.

Внимание! В группе «Default» нельзя создавать подгруппы. Группу и клиента «Default» нельзя перемещать в какие-либо созданные администратором группы.

Настройка групп клиентов

При создании группы потребуется ввести ее наименование, которое можно впоследствии изменить. Удалить существующую группу можно с помощью кнопки «Удалить группу» на панели инструментов или воспользовавшись контекстным меню.

Каждая группа (подгруппа) в дереве объектов КСБ содержит одинаковые вкладки для индивидуальной настройки параметров для клиентов и подгрупп в составе данной группы.

Состояние группы клиентов

Вкладка «Состояние» для выбранной группы в дереве объектов отображает общее состояние клиентов, входящих в группу.

Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

Доступны следующие действия с группой клиентов:

1. По команде синхронизировать с СБ клиентов, входящих в данную группу (подгруппу).
2. Добавить в состав группы (подгруппы) новую подгруппу.
3. Удалить группу из ДБ. Есть возможность удалить только ту группу, в которой нет клиентов. Группу «Default» удалить невозможно.
4. Переименовать группу.

Учетные записи группы клиентов

Вкладка «Учетные записи группы» на уровне группы содержит список учетных записей ДБ и

отмеченных флагом для работы на клиентах в составе группы (подгруппы) (рис. 512) (см. «Создание пользователей Домена безопасности»).

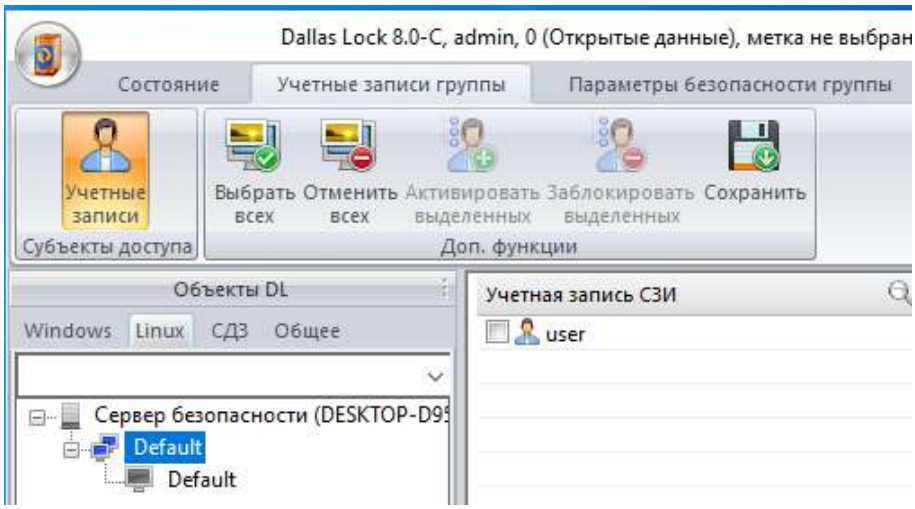


Рис. 512. Список учетных записей группы клиентов СБ

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для группы необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

У клиентов ДБ существует также свой список учетных записей, в котором также можно выбрать необходимые для доступа к работе на клиенте.

Поэтому, особенностью списка учетных записей для группы клиентов является то, что после дополнительного формирования списка на самих клиентах, состояние отмеченных записей в списке группы (подгруппы) принимает вид:

- — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на всех клиентах группы (подгруппы);
- — затемненное поле означает неопределенность, запись включена на одних и выключена на других клиентах группы (подгруппы);
- — пустое поле означает, что запись отключена для работы на всех клиентах группы (подгруппы).

Параметры безопасности группы

Вкладка «Параметры безопасности группы» на уровне группы позволяет редактировать параметры безопасности для группы (подгруппы) (рис. 513).

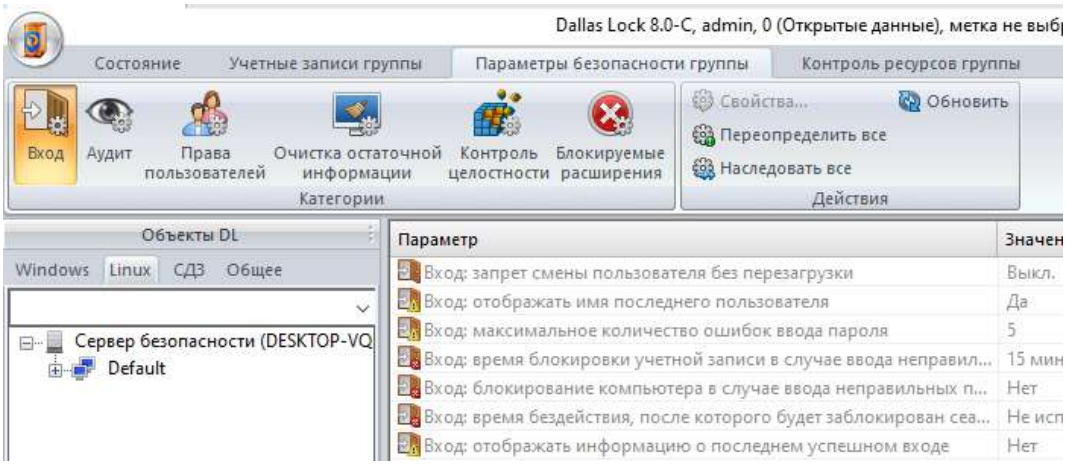


Рис. 513. Параметры безопасности для групп клиентов СБ

Настройка параметров безопасности для группы производится аналогично настройке параметров безопасности для ДБ (см. «Параметры безопасности домена»). Для применения параметров на клиентах необходима синхронизация.

Параметры могут наследовать установленные настройки (от СБ или от группы, в состав которой входит данная группа) или принимать индивидуальные значения следующим образом:

1. Параметры, для которых отмечено наследование, примут значения, установленные для

родительского объекта в дереве объектов КСБ: значения для СБ или группы. В этом случае параметры будут отображаться нечетким серым цветом.

2. Параметры, для которых выбраны и установлены оригинальные настройки, будут отображаться четким черным цветом.

Для того, чтобы установить или снять наследование настроек, имеются следующие возможности:

1. Для того, чтобы все параметры наследовали значения, установленные для родительского объекта дерева, необходимо на панели действий выбрать «Наследовать все».
2. Если на панели действий выбрать «Переопределить все», то все параметры одновременно будут обозначены как индивидуально настроенные.
3. Для отдельно выбранного параметра имеется возможность выбрать оригинальное значение нажав кнопку «Оригинальные настройки для выбранного параметра.
4. Для отдельно выбранного параметра имеется возможность выбрать оригинальное значение нажав кнопку «Наследовать настройки для выбранного параметра.

Настройка клиентов

Состояние клиента

Вкладка «Состояние» на уровне клиента отображает общее состояние клиента (рис. 514).

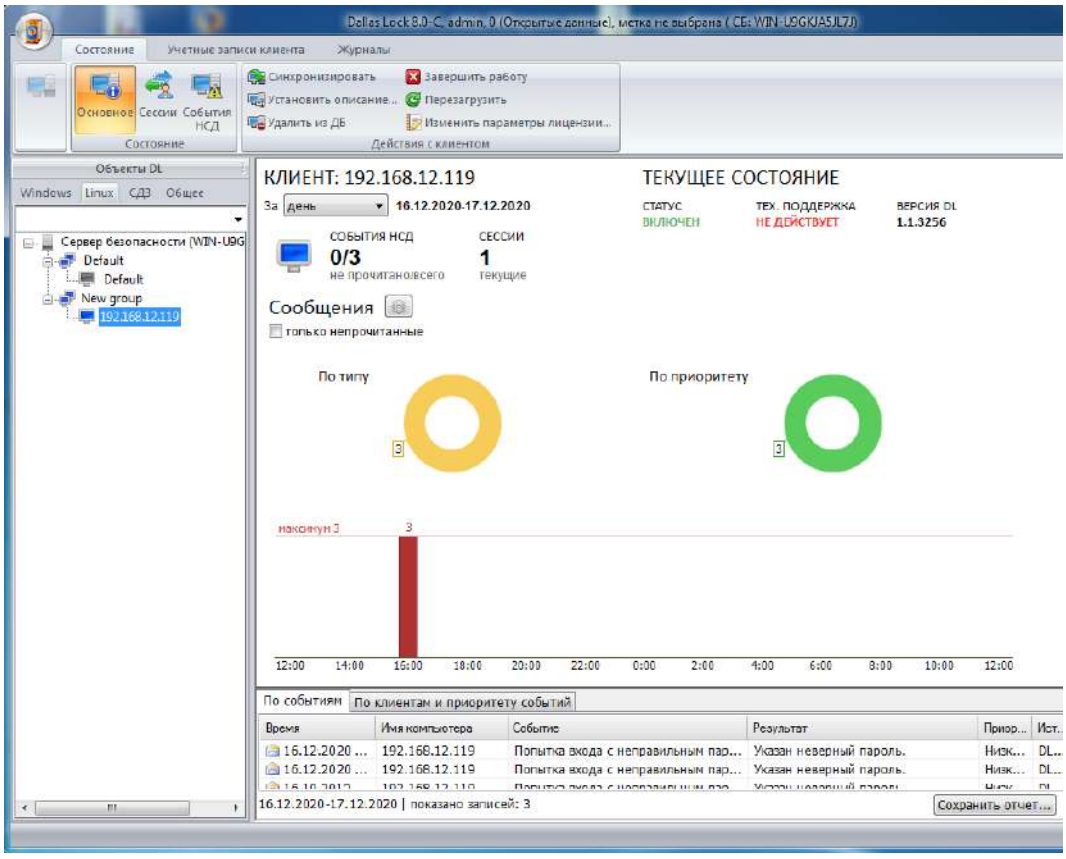


Рис. 514. Выбор клиента СБ

Доступны следующие категории.

Основное

В верхней части информационной панели отображается следующая информация:

- имя клиента;
- количество событий НСД на клиенте за выбранный период времени;
- количество текущих сессий (интерактивных) на клиенте.
- текущее состояние клиента:
  - статус клиента,
  - статус технической поддержки,
  - версия Dallas Lock Linux.

Управление данной категорией аналогично управлению категории «Состояние» → «Основное» на уровне СБ (см. «Основное»).

Доступны следующие действия с клиентом (некоторые действия доступны только при подключении к клиенту): • по команде синхронизировать клиента с СБ; • установить краткое описание, которое будет добавлено к имени клиента в списке объектов; • удалить клиента из ДБ (Dallas Lock Linux при этом не удаляется); • завершить работу клиента; • перезагрузить клиент; • изменить номер лицензии и код технической поддержки на клиенте.
Сессии
Отображаются текущие (интерактивные) сессии на данном клиенте. Имеется возможность завершить или заблокировать определенную сессию.
События НСД
Отображается список событий НСД клиента. События, регистрируемые как НСД, настраиваются через параметры СБ (см. «Сигнализация об НСД»). Данный список формируется из журналов клиента. С помощью панели действий можно: отметить все записи прочитанными или непрочитанными; обновить, загрузить новый или очистить список. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

Учетные записи клиента

Вкладка «Учетные записи клиента» на уровне клиента содержит список учетных записей ДБ и отмеченных флагом для работы на клиенте (рис. 515) (см. «Создание пользователей в ДБ»).

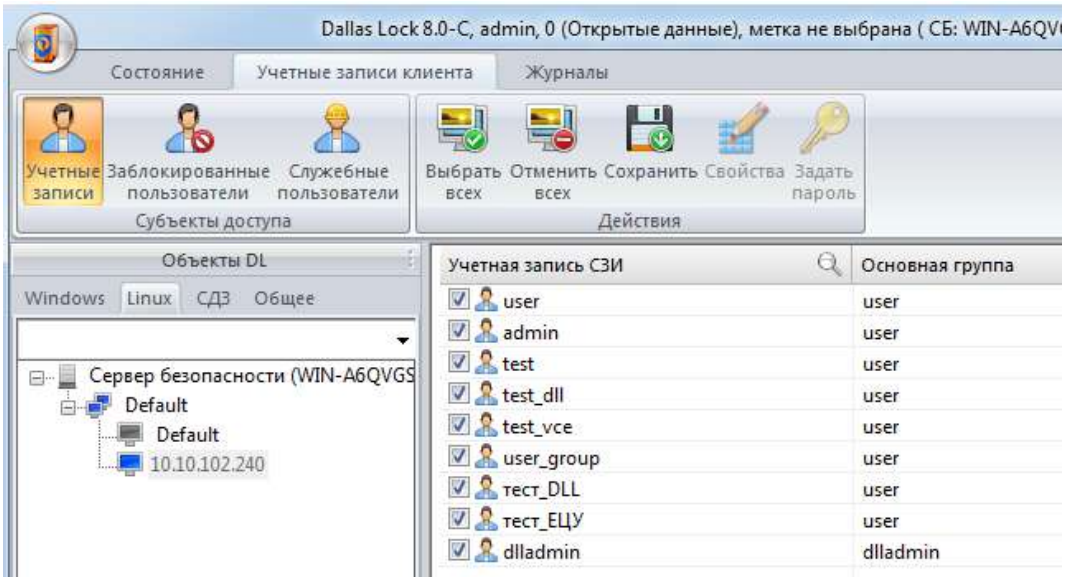


Рис. 515. Список учетных записей клиента Linux

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для клиента необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

Так как все учетные записи клиентов управляются с СБ, следует учесть, что:

1. Если на клиенте в оболочке администратора созданы учетные записи, но не продублированы на СБ, то в процессе синхронизации они будут отключены (отображается соответствующим значком в оболочке администратора).
2. Не отмеченные учетные записи ДБ (снят флаг) после синхронизации будут отключены на клиенте.

Категория «Заблокированные пользователи» в КСБ формирует список учетных записей, которые заблокированы для работы на данном ПК с СБ. Для каждого клиента при его подключении осуществляется формирование своего списка с заблокированными для работы на клиенте пользователями, если таковые имеются.

Управление служебными пользователями происходит способом, аналогичным управлению обычными пользователями СБ. Чтобы создать группу, нужно нажать кнопку «Создать». Чтобы

удалить существующую группу, необходимо выделить ее и нажать «Удалить».

Журналы клиента

Вкладка «Журналы» на уровне клиента позволяет выбрать и открыть собранные СБ журналы с клиента (рис. 516).

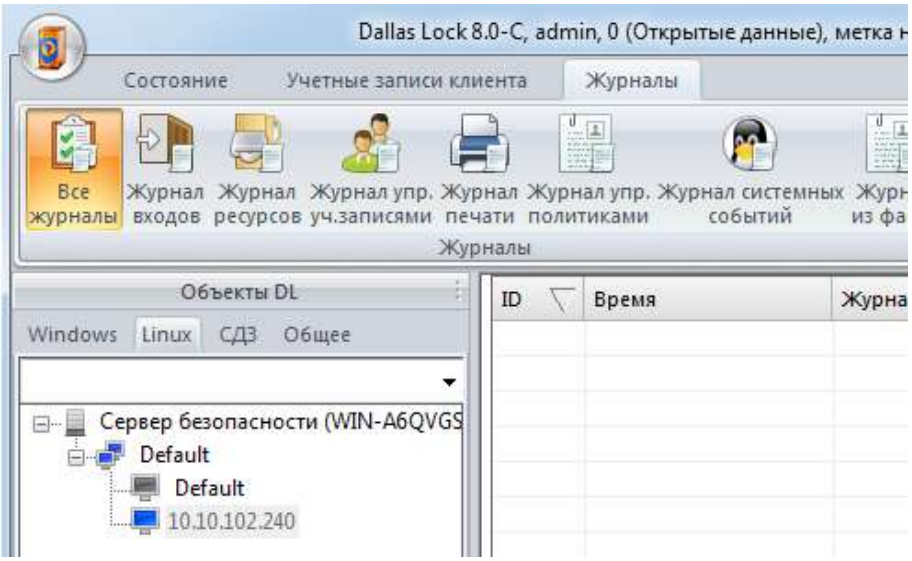


Рис. 516. Вкладка КСБ полученных с клиента журналов

Формирование этих журналов и записей в них происходит на момент команды сбора журналов путем нажатия данной кнопки на вкладке «Состояние» клиента или на вкладке «Состояние» СБ, а также при настроенном периодическом сборе журналов в параметрах СБ.

Принцип ведения журналов клиентов на СБ следующий. На СБ в момент получения журналов с клиента происходит объединение записей журналов одного типа с предыдущими. Объединение новых записей в процессе сбора журналов происходит до тех пор, пока не достигается максимальный размер (20000 записей). Далее журнал архивируется и начинает вестись заново.

В правой части окна формируется список всех полученных журналов и их размер в байтах, а в центральной — списки записей выбранного журнала.

Панель «Действия» аналогична той, что есть в оболочке администратора Dallas Lock 8.0: имеется возможность архивации записей, экспорта записей в файл в выбранном формате, настройка и применение фильтра, группировка записей (см. «Журналы»).

Примечание. С помощью клавиши «Delete» можно удалить файл журнала клиента в КСБ. Для этого выполнить следующее:

1. Выделить выбранный файл в журнале клиента и нажать клавишу «Delete».
2. Перед удалением файла из журнала пользователю выводится соответствующее сообщение.
3. При положительном ответе происходит удаление файла из журнала, при отрицательном операция будет отменена.

19.12 Клиенты СДЗ

Для управления клиентами средства доверенной загрузки необходимо в списке клиентов СБ выбрать вкладку «СДЗ» (рис. 517).

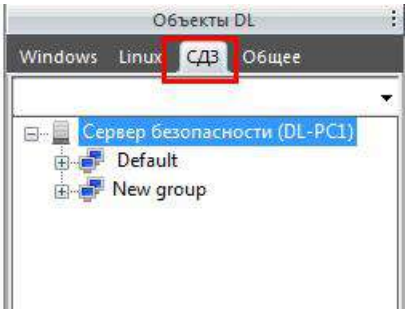


Рис. 517. Клиенты СДЗ

19.12.1 Ввод СДЗ клиента в ДБ

Для ввода СДЗ клиента в ДБ, должны быть соблюдены следующие условия:

1. В ЛВС должен быть работающий СБ.
2. На СБ должны быть открыты TCP/IP порты 17494 и 17501, используемые для обмена данными с клиентами СДЗ.

Для ввода СДЗ клиента в ДБ необходимо:

1. Включить ПК, в котором установлена аппаратная плата СДЗ.
2. Ввести авторизационные данные пользователя категории «Администратор». Нажать кнопку «ОК».
3. Перейти в категорию «Параметры» → «Параметры сети», настроить сеть, выбрать тип сервера «Сервер Безопасности» и заполнить следующие поля (рис. 518):
   - Имя клиента, которое будет отображаться в дереве КСБ.
   - Имя компьютера в сети или IP-адрес, на котором установлен СБ.
   - Ключ доступа к СБ. По умолчанию ключ доступа — пустой.

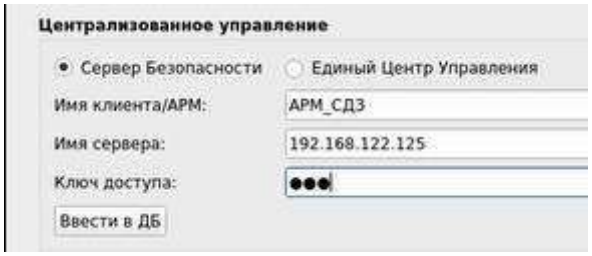


Рис. 518. Настройки ДБ для ввода клиента СДЗ

4. Клиент СДЗ будет введен в ДБ, появится сообщения об успешном вводе клиента (рис. 519). Для завершения операции и перезагрузки клиента СДЗ необходимо нажать кнопку «ОК».

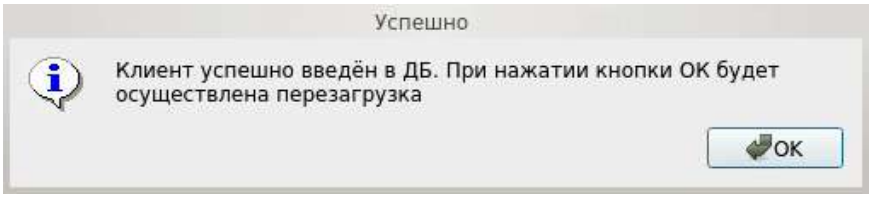


Рис. 519. Клиент СДЗ успешно введен в ДБ

В дереве объектов КСБ появятся новый клиент СДЗ.

19.12.2 Вывод клиента из ДБ

Для вывода клиента через КСБ необходимо выбрать клиента в дереве объектов КСБ и нажать кнопку «Удалить из ДБ» на вкладке «Состояние» или выбрать соответствующую кнопку из контекстного меню, нажав правую кнопку мыши по клиенту в дереве объектов КСБ (рис. 520).

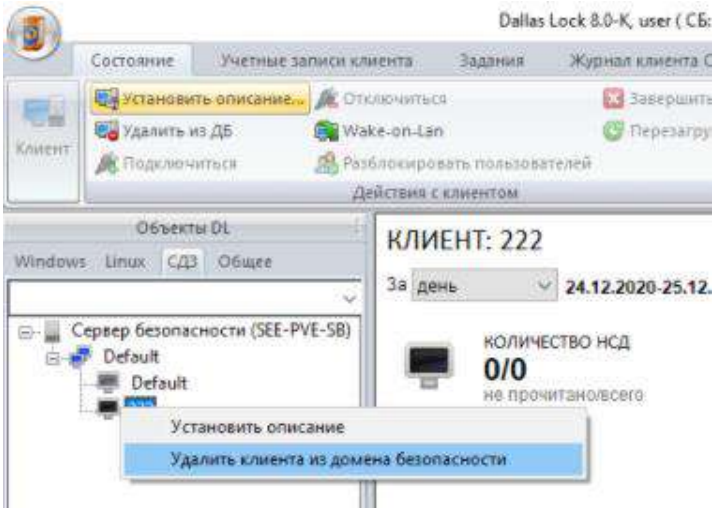


Рис. 520. Удаление клиента из ДБ в КСБ

Для локального вывода СДЗ клиента из ДБ необходимо:

1. Включить ПК, в котором установлена аппаратная плата СДЗ.
2. Ввести авторизационные данные пользователя категории «Администратор». Выбрать сценарий сессий «Администрирование». Нажать кнопку «ОК».
3. Перейти в категорию «Параметры» → «Параметры сети» и нажать кнопку «Вывести из ДБ» (Рис. 521).

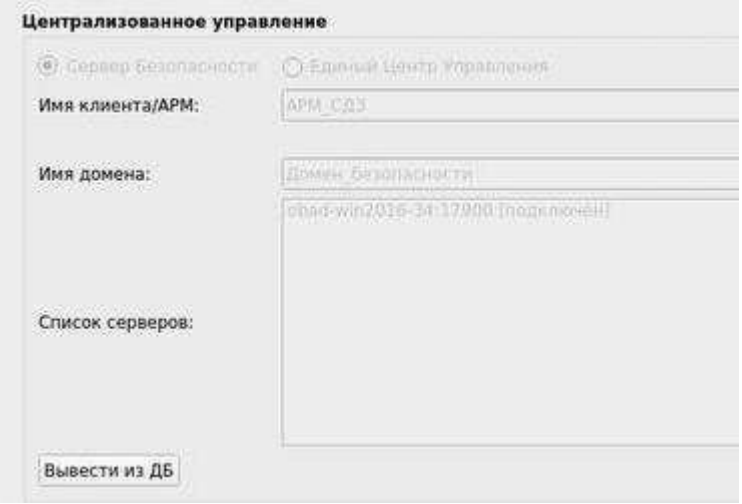


Рис. 521. Вывод клиента СДЗ из ДБ

4. Клиент СДЗ будет выведен из ДБ, появится сообщения об успешном выводе клиента (Рис. 522). Для завершения операции и перезагрузки клиента СДЗ необходимо нажать кнопку «ОК».

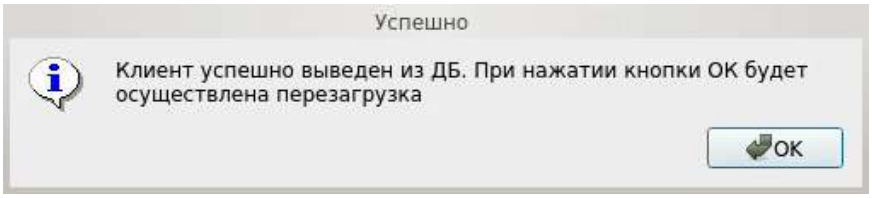


Рис. 522. Клиент СДЗ успешно введен в ДБ

19.12.3 Параметры СБ для СДЗ клиентов

Для изменения параметров СБ необходимо открыть дополнительное меню КСБ  → «Параметры Сервера безопасности…» → «СДЗ».

Появится окно «Параметры Сервера безопасности» для клиентов СДЗ (рис. 523).

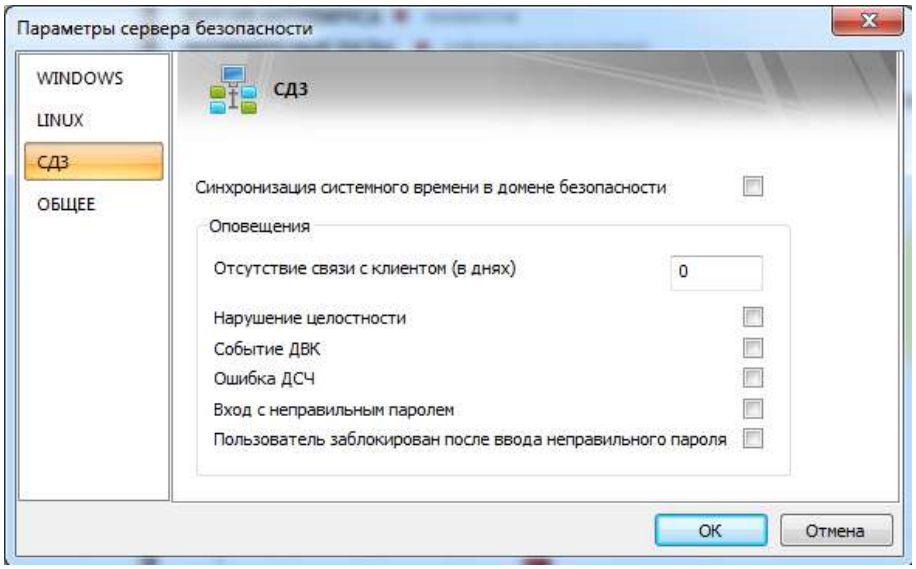


Рис. 523. Параметры СБ

Доступны следующие параметры.

Синхронизация системного времени в домене безопасности
При включении данного параметра осуществляется синхронизация системного времени клиентов СДЗ с системным временем СБ.
Отсутствие связи с клиентом (в днях)
Данным параметром устанавливается максимальный срок отсутствия связи клиента с СБ. По истечении установленного срока клиент в дереве КСБ будет отображаться специальным знаком  . Если установлено значение «0», то данный параметр будет отключен.
Нарушение целостности
При включении данного параметра осуществляется оповещение о нарушении контроля целостности объекта.
События ДВК
При включении данного параметра осуществляется оповещение от датчика вскрытия корпуса.
Ошибка ДСЧ
При включении данного параметра осуществляется оповещение об ошибке от датчика случайных чисел.
Вход с неправильным паролем
При включении данного параметра осуществляется оповещение о попытке входа с неправильным паролем.
Пользователь заблокирован после ввода неправильного пароля
При включении данного параметра осуществляется оповещение о блокировке пользователя после многократного ввода неправильного пароля (настраивается параметром безопасности «Вход: максимальное количество ошибок ввода пароля»).

Значки объектов, обозначающие клиентов СДЗ в дереве КСБ, в зависимости от состояния клиента могут принимать следующий вид:

 — клиент недоступен, либо клиент находится в режиме работы ШОС и в ШОС не установлен Агент, либо нет соединения между Агентом ШОС и СБ Dallas Lock;

 — связь с клиентом отсутствует свыше заданного на СБ времени, которое определяется параметром «Оповещение при отсутствии связи с клиентом» (при условии, что настроено оповещение об отсутствии связи с клиентом);

 — существует возможность подключиться к клиенту в режиме ОУ;

 — клиент находится на связи с СБ посредством установленного на клиенте Агента ШОС.

19.12.4 Настройка СБ для всего ДБ

При выборе в дереве объектов КСБ СБ в верхней части консоли формируется набор вкладок для общей настройки параметров безопасности всего ДБ, всех клиентов данного СБ. При выборе определенной вкладки появляется возможность просматривать и редактировать параметры безопасности.

Состояние СБ

Для удобства работы на вкладке «Состояние» возможно узнать общее состояние всего ДБ для Windows, Linux и СДЗ клиентов. Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

С помощью данной вкладки можно добавить группу в дерево КСБ.

Учетные записи домена

Вкладка «Учетные записи домена» на уровне СБ позволяет управлять учетными записями ДБ. На всех клиентах ДБ могут работать учетные записи только из списка учетных записей ДБ (рис. 524).

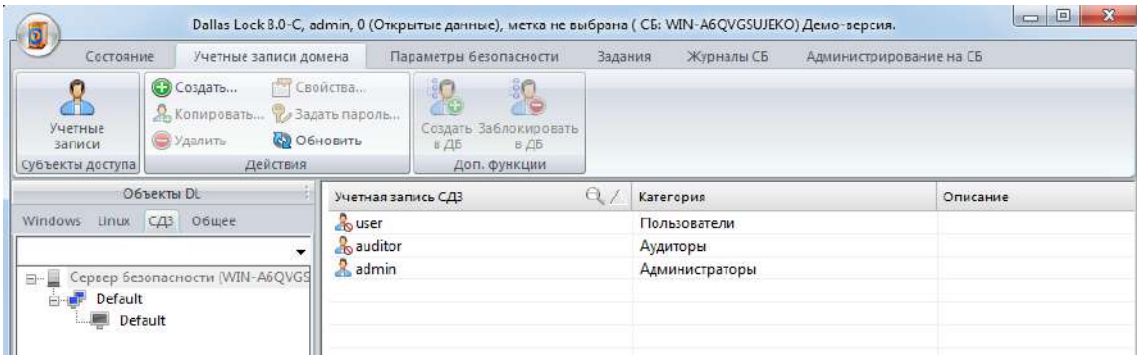


Рис. 524. Учетные записи СДЗ

Список учетных записей ДБ в категории «Учетные записи домена» → «Учетные записи» формируется из учетных записей по умолчанию и зарегистрированных через КСБ.

После создания учетных записей, они автоматически появляются в списках учетных записей объектов ДБ: каждой группы (подгруппы) клиентов и каждого клиента.

Для каждой группы (подгруппы) клиентов и для каждого клиента возможно индивидуально определить, какие учетные записи из списка смогут работать на данных клиентах, а какие нет.

На всех клиентах, входящих в ДБ, параметры отмеченных пользователей будут идентичны.

Установка учетных записей для групп и подгрупп клиентов описана в разделе «Учетные записи группы клиентов».

Установка учетных записей для клиентов описана в разделе «Учетные записи клиента».

Создание пользователей СДЗ в ДБ

Создание учетных записей с помощью КСБ имеет тот же механизм, что и в оболочке администратора Dallas Lock 8.0. Однако следует учитывать, что свойства учетной записи СДЗ имеет отличия от свойств учетной записи Windows.

Для создания нового пользователя СДЗ необходимо:

1. Нажать кнопку «Создать».
2. На экране появится окно создания новой учетной записи (Рис. 525).

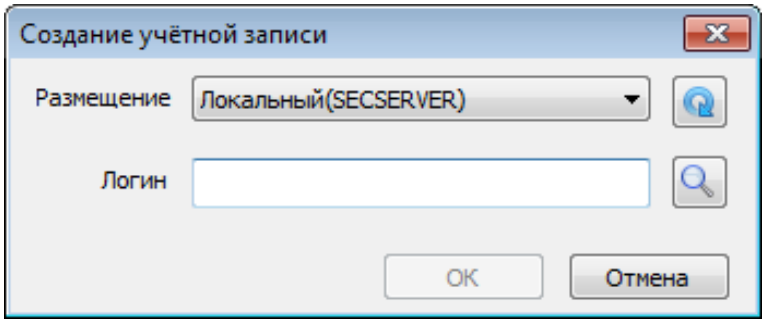


Рис. 525. Окно создания учетной записи

3. В поле «Размещение» выбрать значение «Локальный».
4. В поле «Логин» ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:
   - максимальная длина имени — 20 символов;
   - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ *);
   - разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть прописные и строчные буквы воспринимаются как одинаковые (*User* и *user* являются одинаковыми именами).

   Кнопка поиска, расположенная рядом с полем логина, разворачивает список учетных записей пользователей, зарегистрированных в ОС данного ПК, и позволяет выбрать пользователя из уже существующих (рис. 526).

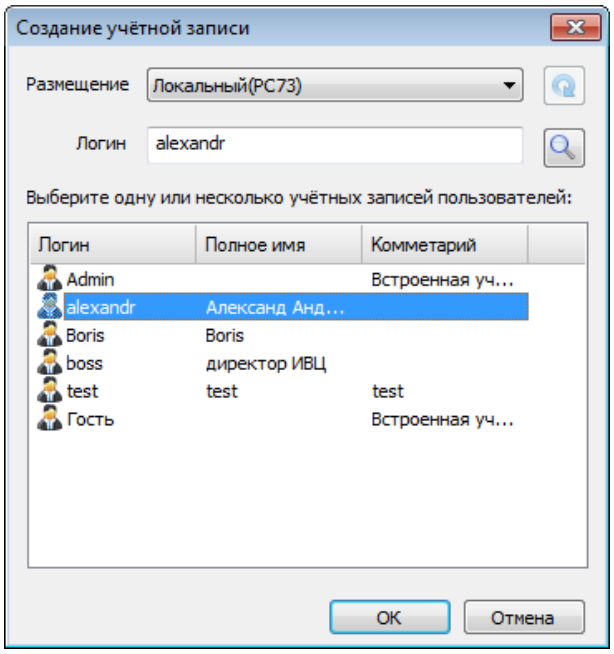


Рис. 526. Учетные записи, зарегистрированные в ОС компьютера

Также можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.

5. После нажатия кнопки «ОК» на экране появится окно изменения основных параметров пользователя (рис. 527).

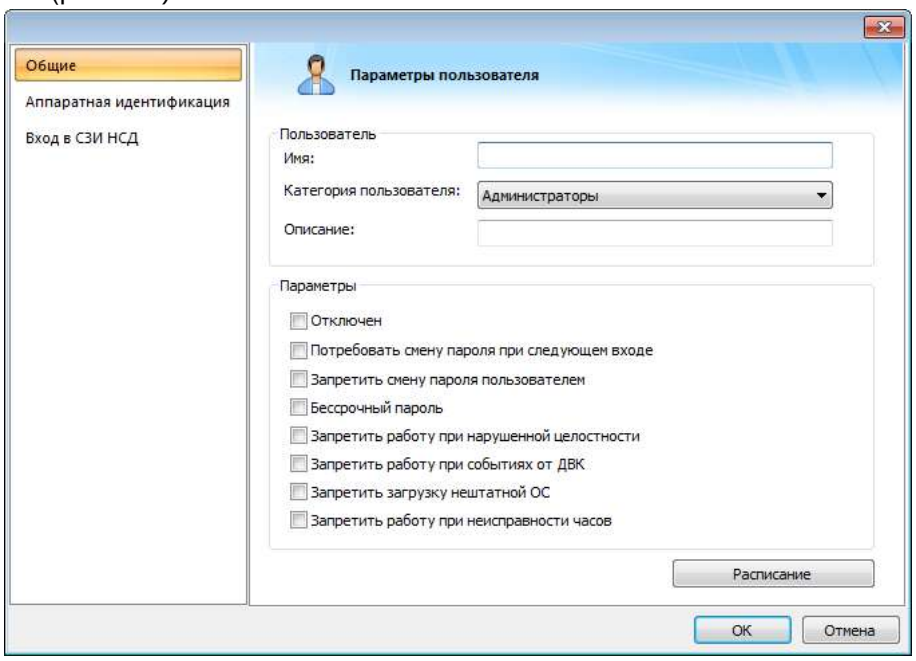


Рис. 527. Создание учетной записи СДЗ

На вкладке «Общие» предлагается заполнить следующие учетные данные и параметры:

- «Имя» пользователя. Данное поле остается без возможности изменения после создания пользователя.
- «Категория пользователя». Штатные пользователи, допущенные к работе на ЗАРМ, не должны иметь категорию «Администратор» или «Аудитор».
- «Описание». Предназначено для текстового описания учетной записи. Длина комментария не более 95 символов. Вводить описание не обязательно.
- «Отключен». Администратор имеет возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на ЗАРМ до тех пор, пока администратор не деактивирует эту опцию.
- «Потребовать смену пароля при следующем входе». При входе пользователя в систему принудительно запускается диалоговое окно смены текущего пароля.
- «Запретить смену пароля пользователем». Запрет для пользователя на смену своего

пароля, в т. ч. и по истечении срока действия.

- «Бессрочный пароль». На учетную запись пользователя не распространяется действие политики безопасности, которая устанавливает максимальный срок действия пароля. Установка данного атрибута не запрещает смену пароля учетной записи пользователем в любое время.
- «Запретить работу при нарушении целостности». Вход в систему пользователем при неуспешном прохождении процедуры контроля целостности объектов и компонентов ПК запрещается.
- «Запретить работу при событиях от ДВК». Вход в систему блокируется при срабатывании датчика вскрытия корпуса. На экране приглашения в систему отображается соответствующее сообщение.
- «Запретить загрузку нештатной ОС». Запрет на загрузку ОС с носителя отличного от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора.
- «Запретить работу при неактивности часов». вход в систему блокируется при неисправности часов. На экране приглашения в систему отображается соответствующее сообщение.
- «Расписание». Задается период времени работы пользователя. Вне указанного периода пользователь не сможет зайти на АРМ.

6. На вкладке «Аппаратная идентификация» возможно назначить аппаратные идентификаторы для пользователя (рис. 528).

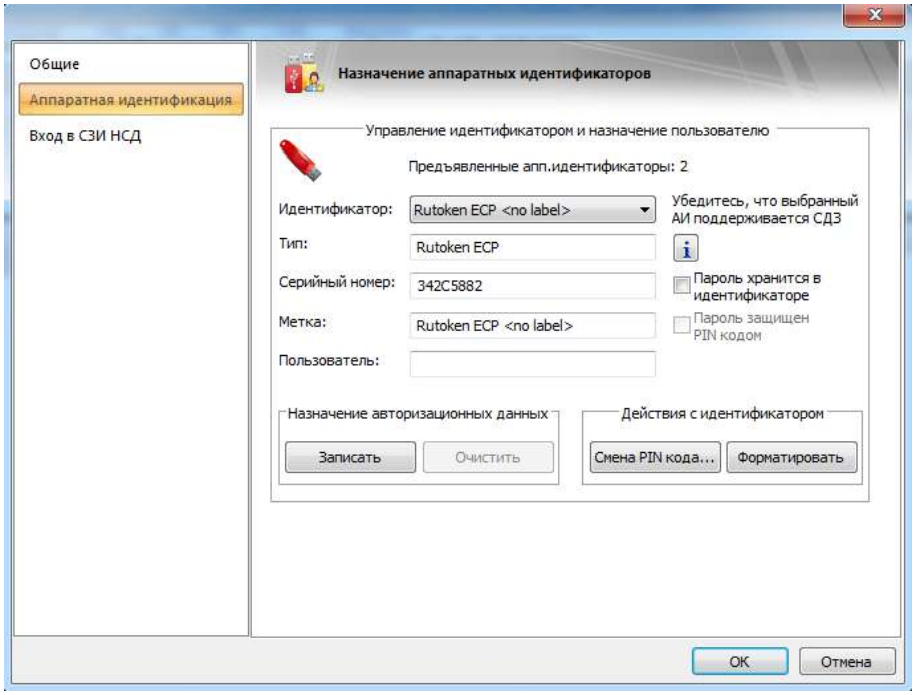


Рис. 528. Назначение аппаратного идентификатора

Внимание! При назначении аппаратного идентификатора администратор должен предварительно убедиться, что выбранный аппаратный идентификатор поддерживается клиентом СДЗ.

7. На вкладке «Вход в СЗИ» возможно настроить автовход в СЗИ Dallas Lock 8.0.
8. Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки «ОК» (рис. 529).

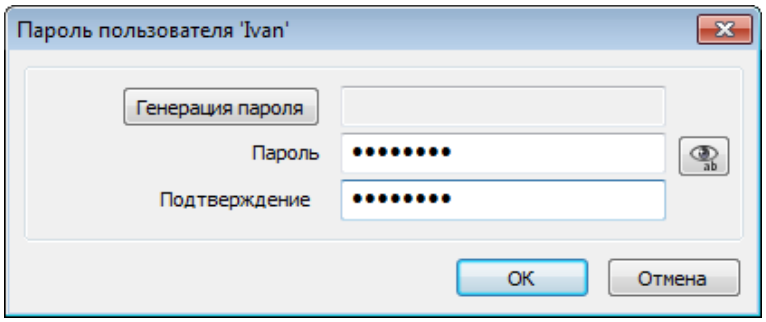


Рис. 529. Форма ввода пароля

Пароль должен соответствовать политике паролей (см. «Доменные политики паролей»).

Регистрация доменных пользователей в ДБ

Для регистрации доменных пользователей необходимо:

1. Нажать кнопку «Создать».
2. На экране появится окно создания новой учетной записи (рис. 530).

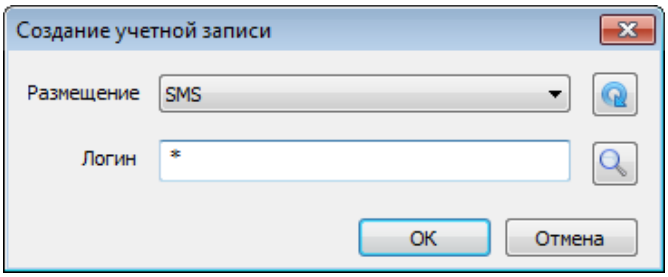


Рис. 530. Окно создания учетной записи

3. В поле «Размещение» выбрать имя домена.
4. Для получения списка учетных записей домена необходимо дополнительно ввести авторизационные данные администратора домена. После авторизации появится список пользователей, зарегистрированных на контроллере домена. Для поиска необходимой записи можно воспользоваться сортировкой или ввести первые буквы и нажать кнопку поиска  .
5. Выбрать учетную запись пользователя и нажать «OK». Можно выделить несколько учетных записей, имеющихся в ОС, и зарегистрировать их одновременно.
6. Последующие действия аналогичны действиям при создании пользователя СДЗ в ДБ.

Возможна регистрация доменных учетных записей с использованием масок, по символу «*» (см. «Регистрация доменных учетных записей по маске»).

Параметры безопасности домена

Доменные политики авторизации

Вкладка «Политики авторизации» позволяет управлять настройками авторизации для клиентов ДБ (рис. 531).

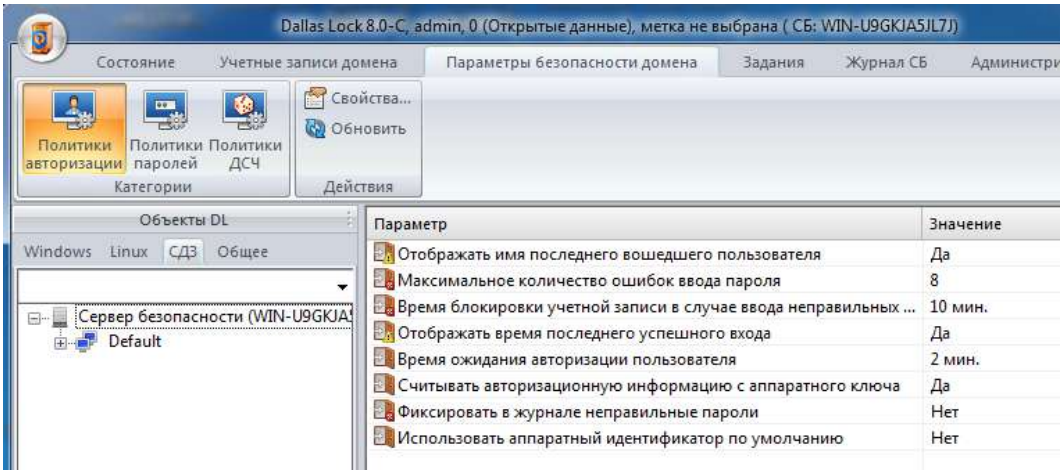


Рис. 531. Политики авторизации

Доступны следующие параметры.

Отображать имя последнего вошедшего пользователя
Возможное значение параметра: «Да/Нет». При значении «Да» в окне авторизации поле «Пользователь» заполняется именем учетной записи пользователя, осуществившего последний успешный вход. При значении «Нет» поле остается пустым.
Максимальное количество ошибок ввода пароля
Установленное значение регламентирует количество попыток ввода значений пароля. В случае ввода неверного пароля появляется предупреждение. По достижении установленного значения — учетная запись пользователя блокируется на определенное время, устанавливаемое параметром «Время блокировки учетной записи в случае ввода неправильных паролей». Возможное значение параметра: от 1 до 15 и «Не используется» — количество попыток ввода пароля неограниченно.
Время блокировки учетной записи в случае ввода неправильных паролей
Установленное значение регламентирует время блокировки учетной записи после ввода неверного пароля более допустимого числа раз (определяется параметром «Максимальное количество ошибок ввода пароля»). В данный интервал времени вход невозможен даже при верном вводе пароля. Возможное значение параметра: от 1 мин до 5 ч и «Не используется» — в таком случае разблокировка возможна только администратором.
Отображать время последнего успешного входа
Возможное значение параметра: «Да/Нет». При значении «Да» при очередном входе пользователя во вовремя выполнения процедуры контроля целостности объектов отображается дата и время последнего успешного входа данного пользователя. При значении «Нет» — не отображается.
Время ожидания авторизации пользователя
Время, отводимое на ввод пользователем авторизационных данных (от начала набора данных, до нажатия кнопки «ОК»). Если пользователь не успел завершить ввод авторизационных данных, уже введенные данные очищаются. Возможное значение параметра: от 1 мин до 10 мин и «Не используется» — время ожидания ввода авторизационных данных неограниченно.
Считывать авторизационную информацию с аппаратного ключа
Возможное значение параметра: «Да/Нет». При значении «Нет» авторизационная информация вводится пользователем с клавиатуры. При значении «Да» авторизационная информация считывается с памяти аппаратного идентификатора в соответствии с настройками учетной записи пользователя, указанными в разделе «Аппаратная идентификация».
Фиксировать в журнале неправильные пароли
Возможное значение параметра: «Да/Нет». При значении «Да» неверный пароль, введенный пользователем, отображается в журнале в столбце «Неверный пароль». При значении «Нет» — не отображается.  **Внимание!** При значении параметра «Да» возникает риск использования информации, содержащейся в столбце «Неверный пароль», для скрытой компрометации паролей пользователей. Ошибки пользователей при вводе пароля неминуемо приведут к раскрытию части пароля, что может значительно облегчить для злоумышленника задачу его подбора.
Использовать аппаратный идентификатор по умолчанию
Возможное значение параметра: «Да/Нет». При значении «Да» во время авторизации для поле «Аппаратный идентификатор» автоматически выберется подключенный аппаратный идентификатор. При значении «Нет» поле остается пустым.

Доменные политики паролей

Вкладка «Политики паролей» позволяет управлять политиками паролей ДБ (рис. 532).

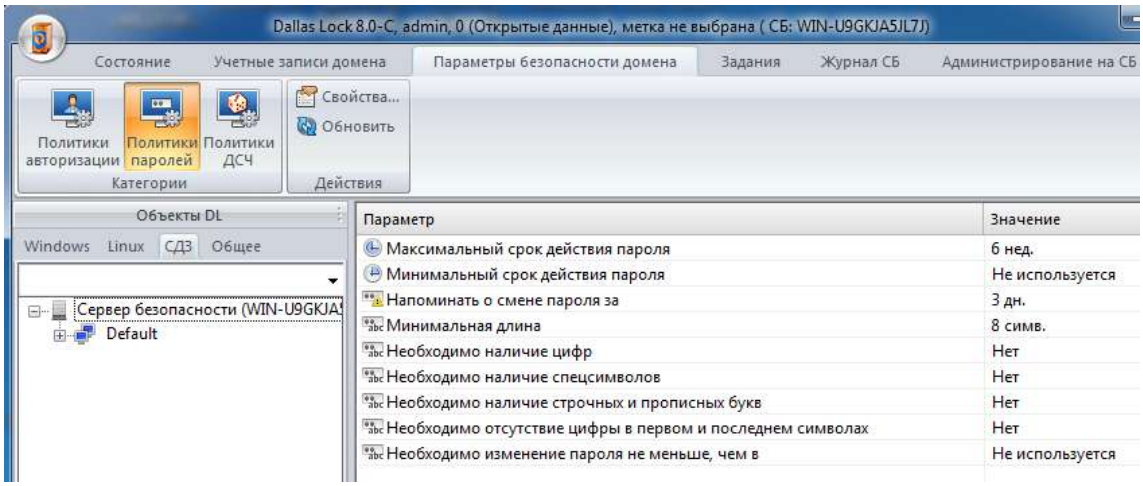


Рис. 532. Политики паролей

Доступны следующие параметры.

Максимальный срок действия пароля
Параметр устанавливает максимальный срок действия пароля пользователей. По истечении срока действия пользователю автоматически будет предложено сменить пароль. Не распространяется на учетные записи пользователей с установленным атрибутом «Бессрочный пароль». Возможное значение параметра: от 1 дня до 25 недель и «Не используется» — максимальный срок действия пароля не установлен.
Минимальный срок действия пароля
Параметр определяет минимальный срок действия пароля. Если этот срок еще не истек, смена пароля пользователем запрещена.
Напоминать о смене пароля за
Параметр задает период до установленного максимального срока действия пароля, в который пользователю будет выводиться сообщение о необходимости смены пароля. Возможное значение параметра: от 1 дня до 2 недель и «Не используется» — сообщение выводиться не будет.
Минимальная длина
Параметр устанавливает ограничение на минимальную длину пароля. Возможное значение параметра: от 1 до 14 и «Не используется» — устанавливаемый пароль может иметь пустое значение.
Необходимо наличие цифр
Если данный параметр включен, то при создании пароля в нем должны присутствовать цифры. Возможное значение параметра: «Да/Нет».
Необходимо наличие спецсимволов
Если данный параметр включен, то при создании пароля в него должны быть включены специальные символы, такие как "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/", "=" и т. д. Возможное значение параметра: «Да/Нет».
Необходимо наличие строчных и прописных букв
Если данный параметр включен, то при создании пароля в него должны быть включены как строчные, так и прописные буквы.

Возможное значение параметра: «Да/Нет».
Необходимо отсутствие цифры в первом и последнем символах
Если данный параметр включен, то при создании пароля его первый и последний символ не должны являться цифрами. Возможное значение параметра: «Да/Нет».
Необходимо изменение пароля не меньше, чем в
Возможное значение параметра: от 1 до 10 и «Не используется» — проверки на отличие старого пароля от нового не происходит.

Доменные политики ДСЧ

Вкладка «Политики ДСЧ» позволяет управлять политиками датчика случайных чисел для всего ДБ (рис. 533).

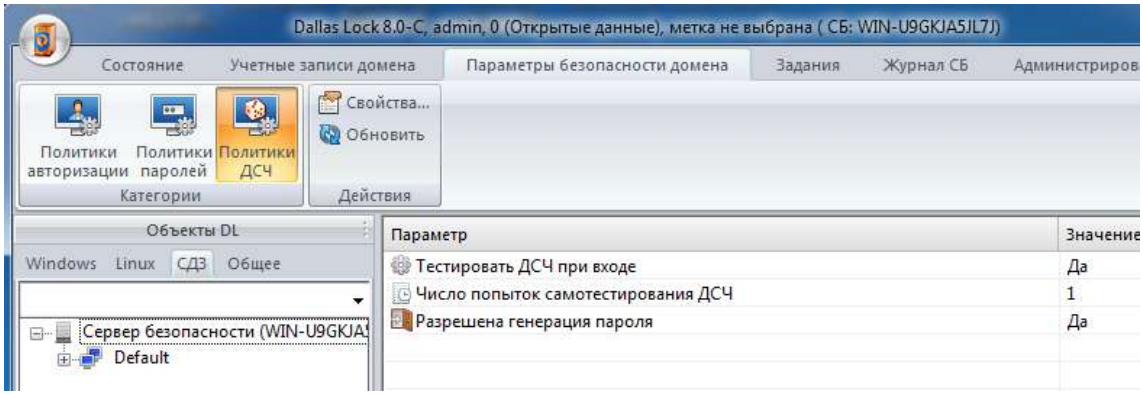


Рис. 533. Политики ДСЧ

Доступны следующие параметры.

Тестировать ДСЧ при входе
Возможное значение параметра: «Да/Нет». При значении «Да» осуществляется тестирование ДСЧ при входе. При значении «Нет» тестирование ДСЧ при входе отключено.
Число попыток самотестирования ДСЧ
Установленное значение регламентирует число попыток самотестирования ДСЧ. Возможное значение параметра: от 1 до 3.
Разрешена генерация пароля
Возможное значение параметра: «Да/Нет». При значении «Да» для пользователя разрешена генерация пароля. При значении «Нет» для пользователя запрещена генерация пароля.

Задания

Использование мастера добавления задач позволяет гибко настраивать однотипные задания для нескольких объектов дерева СДЗ КСБ (рис. 534).

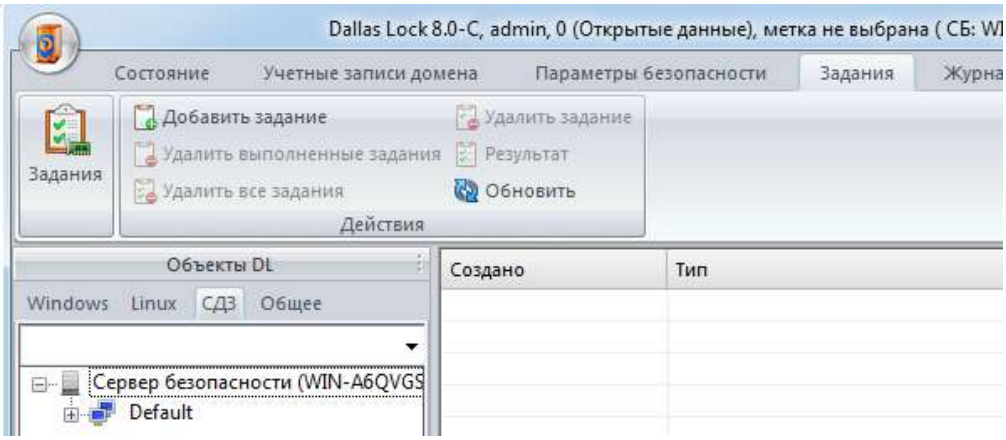


Рис. 534. Задания СДЗ

Централизованное управление файлами конфигурации и отчетами СДЗ DL обеспечивает следующие возможности:

- для файлов конфигурации:
  - получение файлов конфигурации с клиентов на СБ по запросу администратора,
  - хранение и удаление файлов конфигурации в базе данных СБ,
  - применение файлов конфигурации на клиенте СДЗ при синхронизации СБ;
- для отчетов:
  - получение отчетов клиентов с помощью СБ,
  - просмотр отчетов на СБ,
  - хранение и удаление отчетов в базе данных СБ.

Задания для всего ДБ отображаются на вкладке «Задания» на уровне СБ и передаются при синхронизации клиента СДЗ.

Есть возможность удалить все задания или одно определенное, а также удалить только выполненные задания.

Получение отчета

Для того, чтобы создать задание на получение отчета, необходимо:

1. Нажать кнопку «Добавить задание».
2. Выбрать в выпадающем меню «Получение отчета» и нажать кнопку «ОК» (рис. 535).

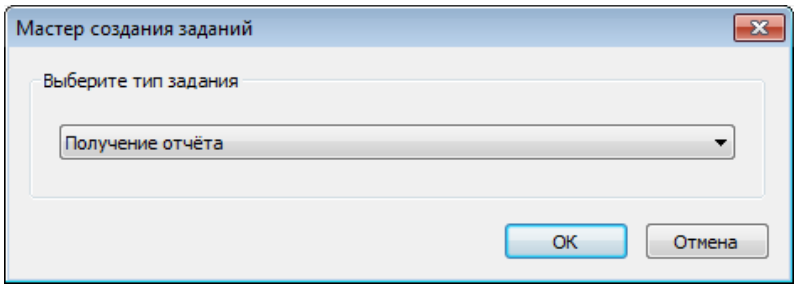


Рис. 535. Выбор типа задания

3. Вв категории «Клиенты» выбрать объект или несколько объектов дерева СДЗ КСБ и нажать кнопку «ОК».

После синхронизации клиенту будет передано задание. Если задание успешно выполнено, то в таблице в графе «Статус» появится соответствующий комментарий. Чтобы открыть отчет необходимо выделить выполненное задание и нажать на кнопку «Результат». Появится детальный отчет, полученный в результате выполнения задания. Для сохранения отчета в файл необходимо нажать кнопку «Сохранить» и выбрать путь сохранения файла.

Получение конфигурации

Для того, чтобы создать задание на получение конфигурации, необходимо:

1. Нажать кнопку «Добавить задание».
2. Выбрать в выпадающем меню «Получение конфигурации» и нажать кнопку «ОК» (рис. 536).

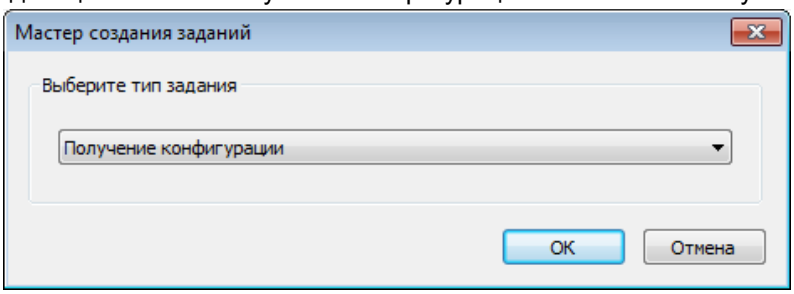


Рис. 536. Выбор типа задания

3. В категории «Клиенты» выбрать объект или несколько объектов дерева СДЗ КСБ и нажать кнопку «ОК».

После синхронизации клиенту будет передано задание. Если задание успешно выполнено, то в таблице в графе «Статус» появится соответствующий комментарий. Чтобы сохранить файл конфигурации необходимо выделить выполненное задание и нажать на кнопку «Результат» и выбрать путь сохранения файла.

Применение конфигурации

Для того, чтобы создать задание на применение конфигурации, необходимо:

1. Нажать кнопку «Добавить задание».
2. Выбрать в выпадающем меню «Применить конфигурацию» и нажать кнопку «ОК» (рис. 537).

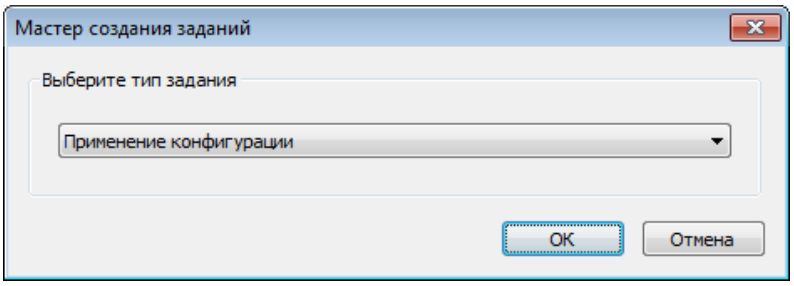


Рис. 537. Выбор типа задания

3. В категории «Файл конфигурации» выбрать файл конфигурации СДЗ.
4. В категории «Клиенты» выбрать объект или несколько объектов дерева СДЗ КСБ и нажать кнопку «ОК».

После синхронизации клиенту будет передано задание. Если задание успешно выполнено, то в таблице в графе «Статус» появится соответствующий комментарий.

Журнал СБ

Вкладка «Журнал СБ» позволяет просматривать регистрируемые события, связанные непосредственно с работой СБ (рис. 538).

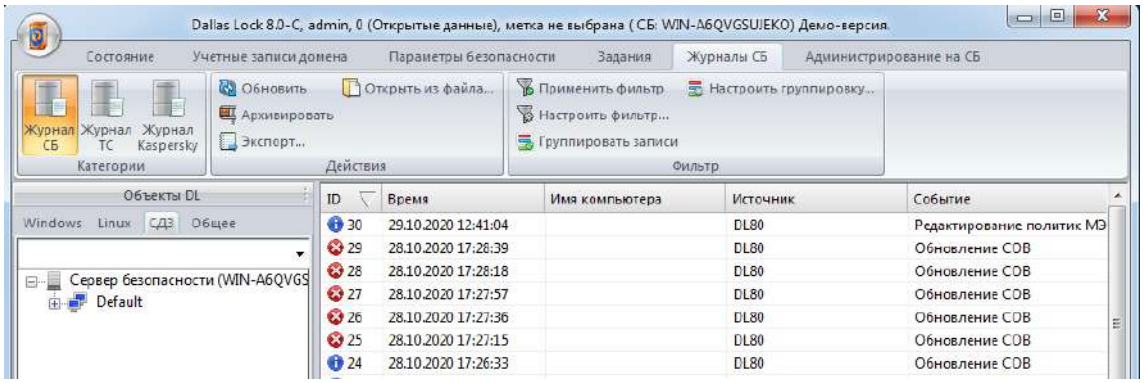


Рис. 538. Журнал СБ

Данный журнал един для всех клиентов ДБ: Windows, Linux и СДЗ. Подробнее о журнале СБ см. «Журнал СБ», подробнее о полученных с клиентов журналах см. «Журналы клиента СДЗ».

19.12.5 Клиенты и группы клиентов СБ

Группа Default и клиент Default

В дереве объектов КСБ всегда присутствуют группа «Default» и клиент «Default».

Примечание. При добавлении нового клиента в ДБ он всегда помещается в группу «Default» при следующих условиях:

1. Настройки безопасности для него копируются из настроек группы «Default».
2. Списки учетных записей копируются из списка клиента «Default».

Создание группы клиентов возможно или на уровне родительского объекта «СБ» или на уровне родительского объекта «группа», поэтому:

1. При создании в дереве объектов новой группы на уровне СБ («Сервер безопасности» → «Добавить группу») для нее копируются параметры безопасности группы Default.
2. При создании новой группы как подгруппы (объект группы → «Добавить подгруппу») для нее копируются параметры безопасности родительской группы.

В дальнейшем администратор СБ ЗАРМ может перенести нового клиента в любую другую группу, а также любую группу в качестве подгруппы в другую группу. Для этого можно воспользоваться

контекстным меню («Переместить») или перетащить значок нужного объекта кнопкой мыши в поле другого значка («Drag-and-drop»).

При выборе каждой группы (подгруппы) и каждого клиента КСБ будет иметь типовой набор вкладок управления параметрами.

Внимание! В группе «Default» нельзя создавать подгруппы. Группу и клиента «Default» нельзя перемещать в какие-либо созданные администратором группы.

Настройка групп клиентов

При создании группы потребуется ввести ее наименование, которое можно впоследствии изменить. Удалить существующую группу можно с помощью кнопки «Удалить группу» на панели инструментов или, воспользовавшись контекстным меню.

Каждая группа (подгруппа) в дереве объектов КСБ содержит одинаковые вкладки для индивидуальной настройки параметров для клиентов и подгрупп в составе данной группы.

Состояние группы клиентов

Вкладка «Состояние» для выбранной группы в дереве объектов отображает общее состояние клиентов, входящих в группу.

Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

Доступы следующие действия с группой клиентов:

1. Добавить в состав группы (подгруппы) новую подгруппу.
2. Удалить группу из ДБ. Есть возможность удалить только ту группу, в которой нет клиентов. Группу «Default» удалить невозможно.
3. Переименовать группу.

Учетные записи группы клиентов

Вкладка «Учетные записи группы» на уровне группы содержит список учетных записей ДБ и отмеченных флагом для работы на клиентах в составе группы (подгруппы) (Рис. 539) (см. «Создание пользователей СДЗ в ДБ»).

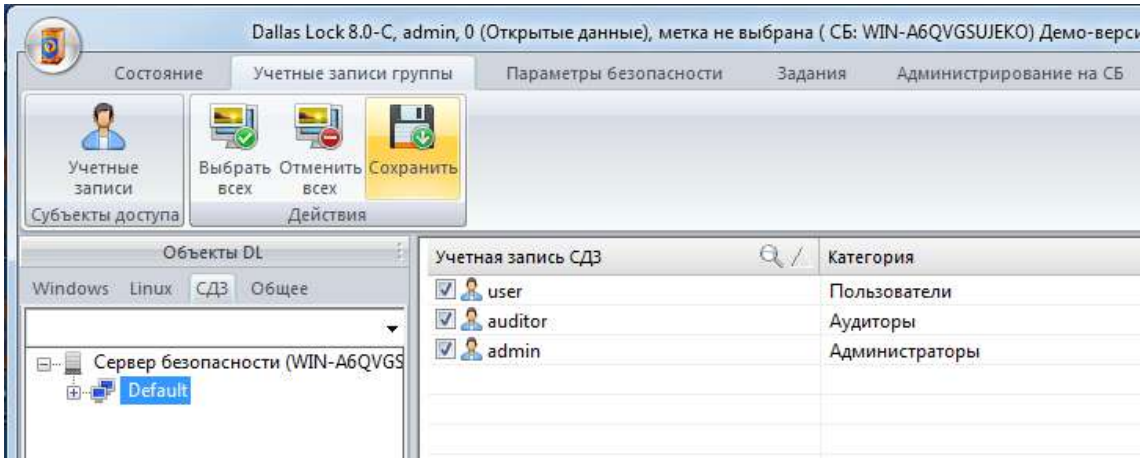


Рис. 539. Список учетных записей группы клиентов СБ

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для группы необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

У клиентов ДБ существует также свой список учетных записей, в котором также можно выбрать необходимые для доступа к работе на клиенте.

Поэтому, особенностью списка учетных записей для группы клиентов является то, что после дополнительного формирования списка на самих клиентах, состояние отмеченных записей в списке группы (подгруппы) принимает вид:

☑ — отмеченное флагом поле означает, что данная учетная запись пользователя имеет доступ на всех клиентах группы (подгруппы);

- — затемненное поле означает неопределенность, запись включена на одних и выключена на других клиентах группы (подгруппы);
- — пустое поле означает, что запись отключена для работы на всех клиентах группы (подгруппы).

Параметры безопасности группы

Вкладка «Параметры безопасности группы» на уровне группы позволяет редактировать параметры безопасности для группы (подгруппы) клиентов (Рис. 540).

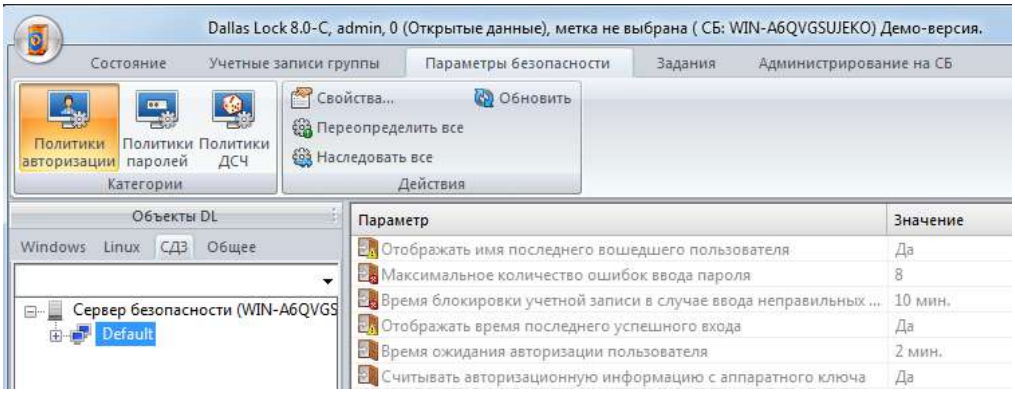


Рис. 540. Параметры безопасности для групп клиентов СБ

Настройка параметров безопасности для группы производится аналогично настройке параметров безопасности для ДБ (см. «Параметры безопасности домена»). Для применения параметров на клиентах необходима синхронизация.

Параметры могут наследовать установленные настройки (от СБ или от группы, в состав которой входит данная группа) или принимать индивидуальные значения следующим образом:

1. Параметры, для которых отмечено наследование, примут значения, установленные для родительского объекта в дереве объектов КСБ: значения для СБ или группы. В этом случае параметры будут отображаться нечетким серым цветом.
2. Параметры, для которых выбраны и установлены оригинальные настройки, будут отображаться четким черным цветом.

Задания

Вкладка «Задания» на уровне группы позволяет управлять заданиями группы (подгруппы) клиентов (Рис. 541).

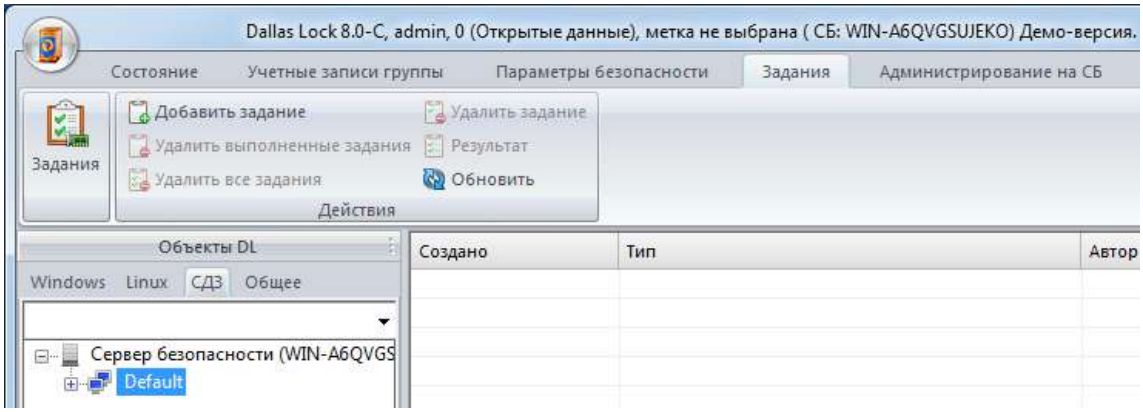


Рис. 541. Задания СДЗ группы клиентов

Управление заданиями группы клиентов выполняется аналогично тому, как это осуществляется для заданий всего ДБ (см. «Задания»).

Настройка клиентов

Состояние клиента

При выборе клиента в дереве объектов КСБ автоматически откроется вкладка основного состояния данной клиентской рабочей станции (рис. 542):

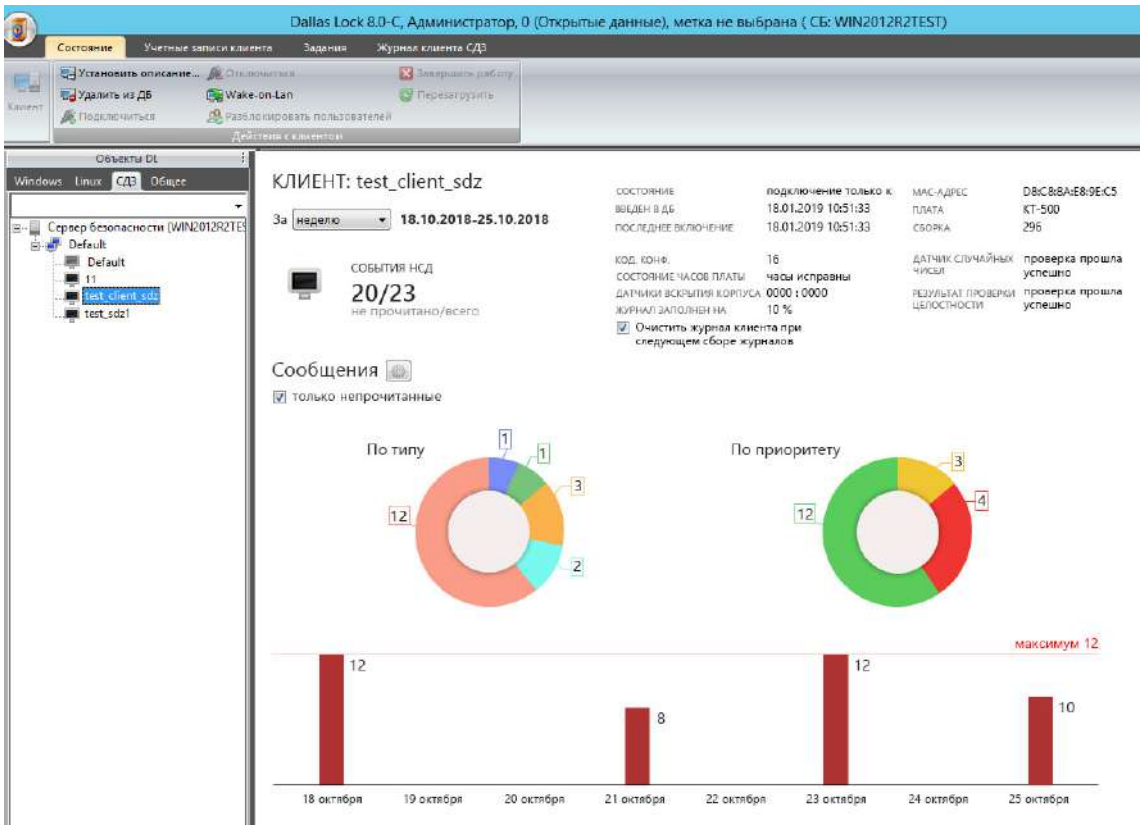


Рис. 542. Выбор клиента СБ

В верхней части информационной панели отображается следующая информация:

- имя клиента,
- состояние клиента,
- дата и время ввода клиента в ДБ,
- дата и время последнего включена клиента,
- MAC-адрес клиента,
- тип платы СДЗ,
- номер прошивки платы СДЗ,
- код конфигурации,
- состояние датчика вскрытия корпуса,
- состояние часов платы,
- состояние датчика случайных чисел,
- результат проверки целостности,
- состояние журнала.

Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

Доступны следующие действия с клиентом (некоторые действия доступны только при подключении к клиенту):

- установить краткое описание, которое будет добавлено к имени клиента в списке объектов;
- удалить клиента из ДБ;
- подключиться (отключиться) к клиенту для ОУ;
- отправить команду «Wake-on-Lan», чтобы включить клиента СДЗ;
- завершить работу клиента СДЗ (действие доступно, если клиент находится на связи с СБ — либо клиент доступен, то есть включен и находится в окне авторизации —);
- перезагрузить клиент СДЗ (действие доступно, если клиент находится на связи с СБ — либо клиент доступен, то есть включен и находится в окне авторизации —);
- разблокировать пользователей клиента.

Использование ОУ через VNC позволяет управлять платой СДЗ аналогично локальной настройке непосредственно самой платы, установленной в ТС. ОУ VNC осуществляется после нажатия кнопки

«Подключиться» и возможно только тогда, когда на клиенте СДЗ Dallas Lock открыто окно авторизации.

После осуществления успешного подключения отображается графическая оболочка администратора СДЗ, в которой возможно выполнять следующие действия:

- просматривать журналы регистрации событий безопасности и управлять ими;
- устанавливать контроль целостности для категорий: «Файловая система», «Реестр», «Области диска», «BIOS CMOS», а также осуществлять операции удаления, обновления и перерасчета;
- осуществлять проверку прошивки платы СДЗ (через сервисную утилиту KtService);
- выполнять настройку часов платы (если плата не оснащена часами или часы неисправны, используется время системной платы) (через сервисную утилиту KtService);
- для сторожевого таймера возможно устанавливать/изменять время срабатывания в секундах (через сервисную утилиту KtService);
- обновлять и обнулять результат ДВК, если зафиксировано вскрытие корпуса (только если плата оснащена ДВК) (через сервисную утилиту KtService);
- запускать тестирование ДСЧ (через сервисную утилиту KtService);
- выбирать конкретное загрузочное устройство, с которого будет возможна загрузка штатной операционной системы (можно установить пункт «Любое устройство» — загрузка штатной операционной системы будет возможна с произвольного устройства) (через сервисную утилиту KtService).

Учетные записи клиента

Вкладка «Учетные записи клиента» на уровне клиента содержит список учетных записей ДБ и отмеченных флагом для работы на клиенте (рис. 543) (см. «Создание пользователей СДЗ в ДБ»).

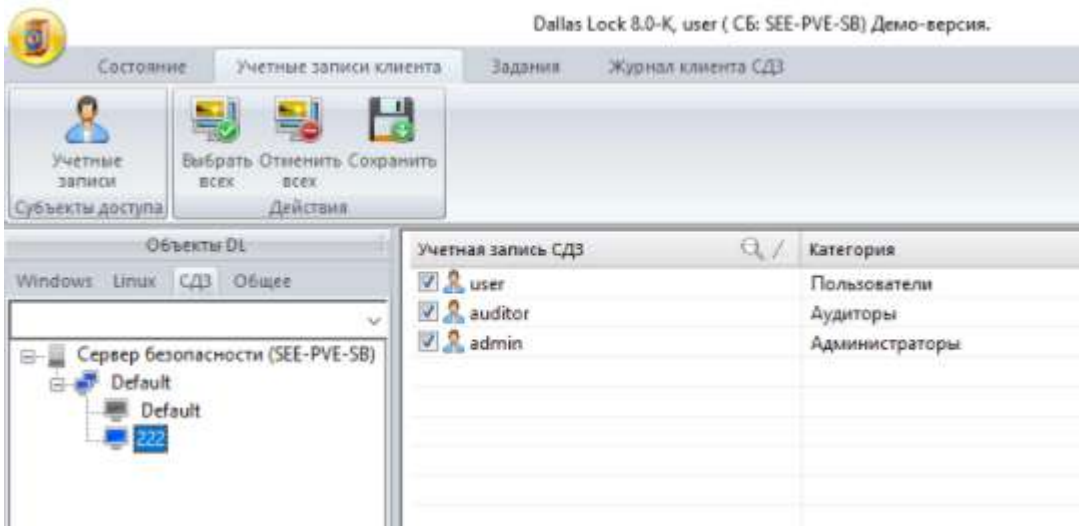


Рис. 543. Список учетных записей клиента СДЗ

Вспомогательные кнопки помогают одновременно отметить все учетные записи.

После формирования списка учетных записей для клиента необходимо нажать «Сохранить». Для применения списка учетных записей на клиентах необходима синхронизация.

Так как все учетные записи клиентов управляются с СБ, следует учесть, что:

1. Если на клиенте в оболочке администратора созданы учетные записи, но не продублированы на СБ, то в процессе синхронизации они будут отключены.
2. Не отмеченные учетные записи ДБ (снят флаг) после синхронизации будут отключены на клиенте.

Журналы клиента СДЗ

Вкладка «Журнал» на уровне клиента позволяет выбрать и открыть собранные СБ журналы с клиента (рис. 544).

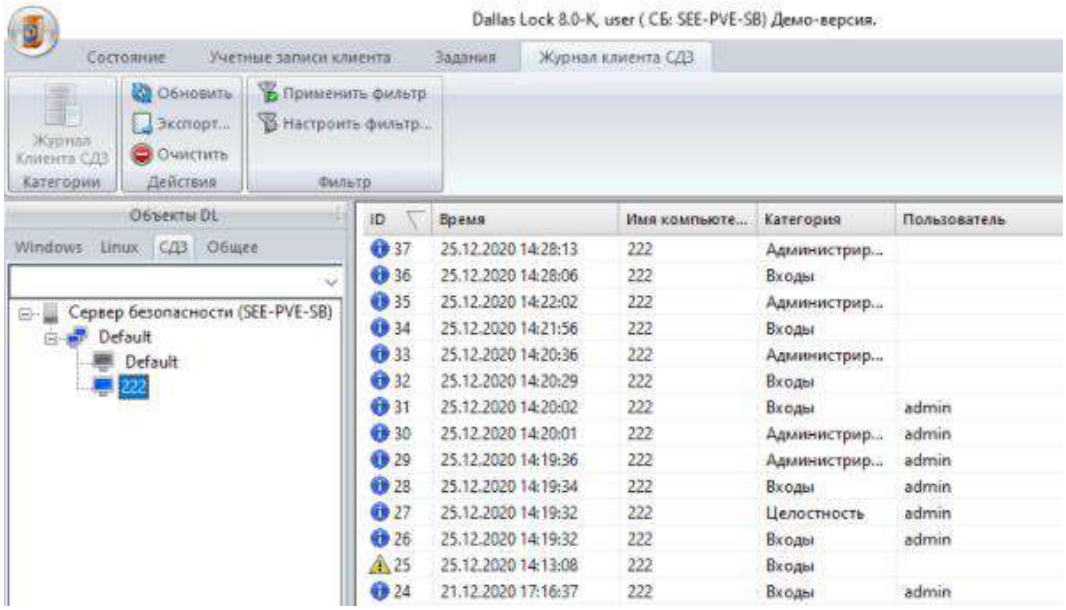


Рис. 544. Вкладка КСБ полученных с клиента журналов

Формирование этого журнала и записей в нем происходит на момент сбора журналов с клиента СДЗ. СБ производит сбор журналов при каждом включении клиента. Если в момент включения клиента СБ недоступен, в журнал событий клиента в категорию «Входы» заносится сообщение об отсутствии связи с СБ.

Имеется возможность очистки журнала, экспорта записей в файл в выбранном формате, открытие журнала из файла, настройка и применение фильтра, группировка записей.

Примечание. С помощью клавиши «Delete» можно удалить файл журнала клиента в КСБ. Для этого выполнить следующее:

1. Выделить выбранный файл в журнале клиента и нажать клавишу «Delete».
2. Перед удалением файла из журнала пользователю выводится соответствующее сообщение.
3. При положительном ответе происходит удаление файла из журнала, при отрицательном операция будет отменена.

Задания

Вкладка «Задания» на уровне клиента позволяет управлять заданиями клиента (рис. 545).

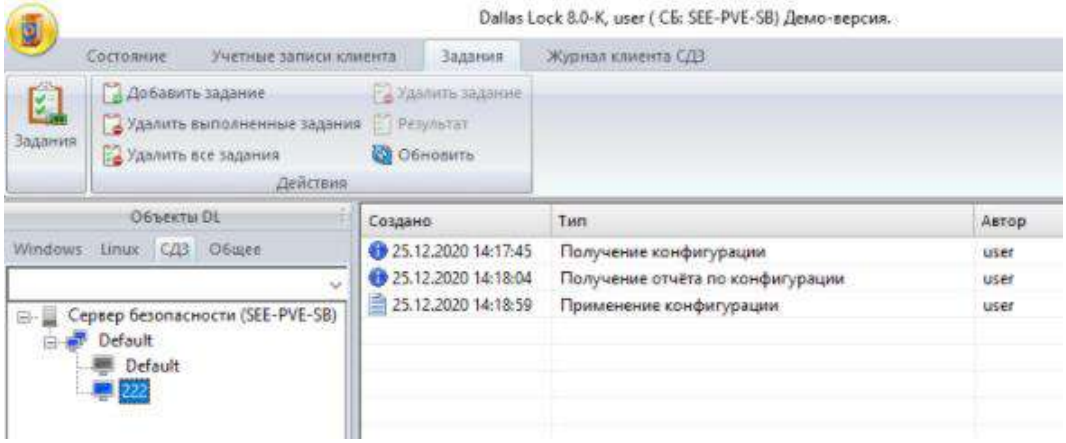


Рис. 545. Задания СДЗ клиента

Управление заданиями клиента выполняется аналогично тому, как это осуществляется для заданий всего ДБ (см. «Задания»).

19.13 Общее

Для управления всеми клиентами СБ необходимо в списке объектов DL выбрать вкладку «Общее» (рис. 546).

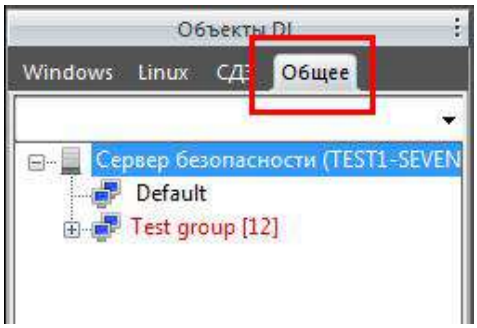


Рис. 546. Общие объекты DL

Для удобства работы на вкладке «Состояние» возможно увидеть объединенную информацию о состоянии всего ДБ для Windows, Linux и СДЗ клиентов с унифицированной возможностью обработки для каждого узла или группы узлов (вне зависимости от типа узла). Управление выполняется аналогично тому, как это осуществляется для Windows клиентов (см. «Основное»).

С помощью данной вкладки можно добавить группу в дерево КСБ.

Значки объектов, обозначающие клиентов СБ (только на вкладке «Общее»), могут принимать следующий вид:

 — клиент Windows;

 — клиент Windows с установленным ПО KES;

 — клиент Linux;

 — клиент СДЗ.

19.13.1 Общие параметры СБ

Для изменения параметров СБ необходимо открыть дополнительное меню КСБ  → «Параметры сервера безопасности…» → «Общее».

Появится окно «Параметры сервера безопасности» (рис. 547).

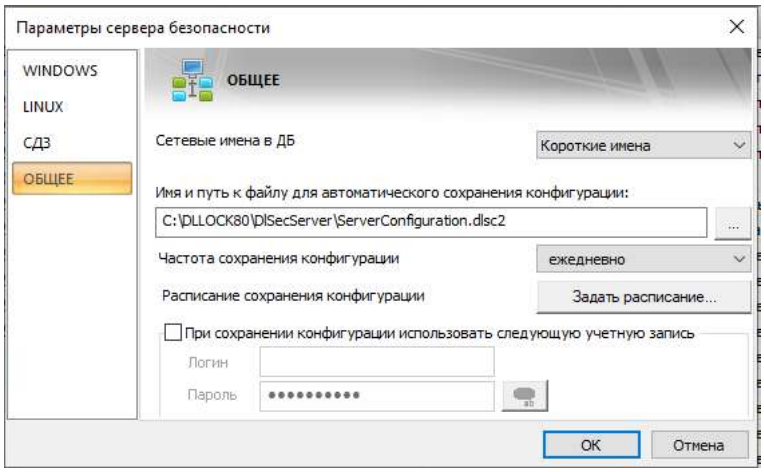


Рис. 547. Параметры СБ

Доступны следующие параметры:

Сетевые имена в ДБ
Данным параметром определяется схема идентификации клиентов в ДБ. Доступны три возможных значения параметра: «Короткие имена», «Полные доменные имена» и «IP-адреса».

Примечание. Схема идентификации клиентов в ДБ должна быть выбрана однократно до введения клиентов в ДБ.

Имя и путь к файлу для автоматического сохранения конфигурации
Данный параметр позволяет задать путь сохранения файла конфигурации СЗИ на жестком диске, сетевом диске или съемном носителе и имя для него. По умолчанию указан путь «C:\DLLOCK80\DlSecServer\ServerConfiguration.dlsc2». **Примечание.** Пока данному параметру не присвоено значение, «Частота сохранения конфигурации» и «Расписание сохранения конфигурации» недоступны.
Частота сохранения конфигурации
Данный параметр позволяет настроить частоту сохранения файла конфигурации. Параметр становится доступен после выбора пути и указания допустимого имени для файла конфигурации. Параметру можно присвоить значение в диапазоне от «5 мин» до «ежемесячно». По умолчанию параметр имеет значение «Ежедневно».
Расписание сохранения конфигурации
Данный параметр позволяет производить настройку расписания сохранения конфигурации СЗИ. По умолчанию расписание не используется. Если для сохранения конфигурации указывается сетевой путь, необходимо установить флаг в поле «При сохранении конфигурации использовать следующую учетную запись» и ввести данные учетной записи пользователя, из-под которого необходимо выполнять сохранение конфигурации. При этом указываемый пользователь должен быть зарегистрирован на СБ.

После задания значений параметров на экране появляется оповещение об успешном сохранении.

19.14 Менеджер серверов безопасности

Если информационная сеть сильно распределена, например, по территориальному признаку, или в ней очень много рабочих станций, то имеет смысл включить защищенные СЗИ Dallas Lock 8.0 компьютеры не в один ДБ, а в несколько.

По аналогии с терминологией, применяемой корпорацией Microsoft, совокупность доменов безопасности образует ЛБ. Для управления ЛБ служит МСБ. МСБ должен быть установлен на любой защищенный Dallas Lock 8.0 компьютер, который имеет сетевой доступ ко всем СБ, которые необходимо включить в ЛБ.

МСБ Dallas Lock 8.0 может объединять СБ Dallas Lock 8.0 редакциях «К» и «С».

МСБ — вспомогательная программа, которая позволяет:

- собирать журналы с конкретного ДБ, либо со всех ДБ, входящих в данный ЛБ;
- централизованно применять политики безопасности к конкретному ДБ, либо ко всем ДБ, входящим в данный ЛБ;
- начинать сессию администрирования любого СБ, входящего в ЛБ (может использоваться как КСБ, так и сетевое администрирование);
- начинать сессию терминального доступа СБ.

Примечание. В контексте МСБ термины «Сервер безопасности» и «Домен безопасности» эквивалентны. МСБ взаимодействует только с СБ, который для него олицетворяет весь ДБ. Непосредственное взаимодействие с клиентами СБ в МСБ не предусмотрено.

Используя клиентские рабочие станции, защищенные Dallas Lock 8.0, работающие под управлением СБ и МСБ, можно создавать трехуровневую модель централизованного управления защиты информации (Рис. 548).

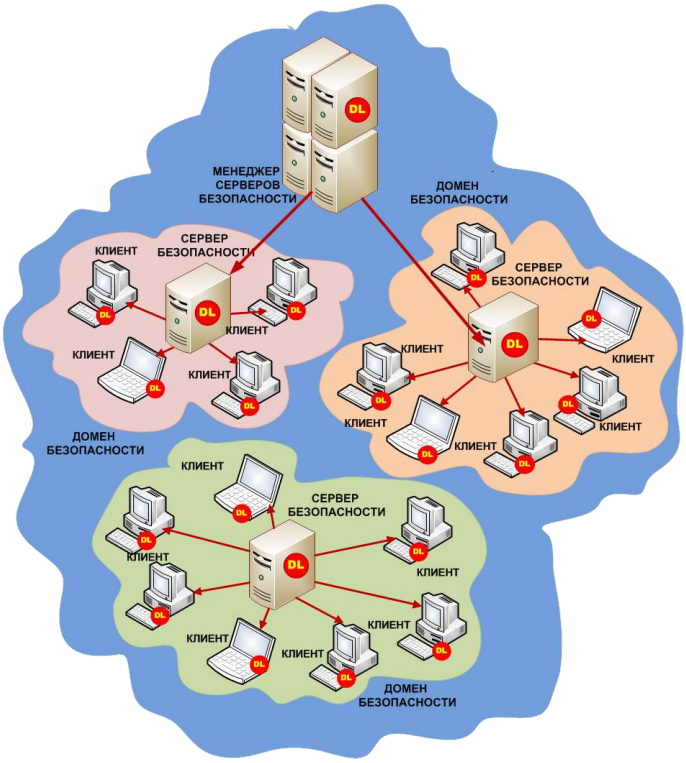


Рис. 548. Модель централизованного управления Dallas Lock

19.14.1 Системные требования

МСБ может работать на любом компьютере, работающем под управлением следующих ОС:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter) (см. Формуляр RU.48957919.501410-02 30 п. 3.3.4);
- Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter) (см. Формуляр RU.48957919.501410-02 30 п. 3.3.4);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

19.14.2 Установка Менеджера серверов безопасности

Чтобы установить МСБ, необходимо запустить установочный файл DL80.SecServManager.msi и дождаться завершения копирования файлов.

Процесс установки МСБ будет сопровождаться соответствующими окнами программы установки (Рис. 549).

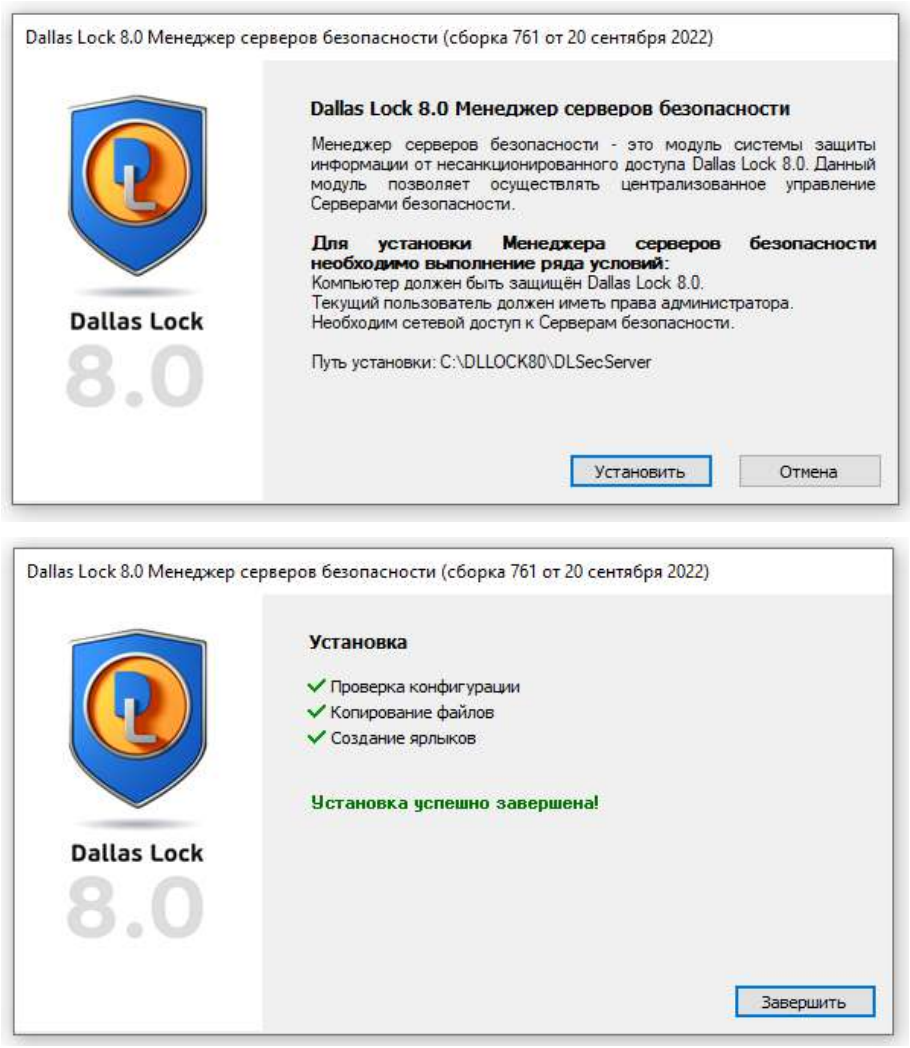


Рис. 549. Установка МСБ

Сразу же после установки МСБ готов к работе. В меню «Пуск» после установки появится значок МСБ. При необходимости ярлык МСБ можно отправить на рабочий стол самостоятельно.

Для уточнения информации об используемой лицензии Dallas Lock 8.0 МСБ нажать на кнопку «О программе» (Рис. 550Рис. 549).

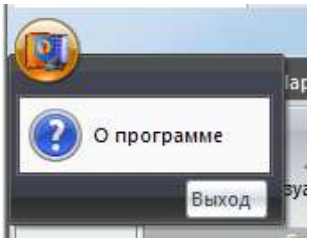


Рис. 550. О программе МСБ

В появившимся окне появится информация о номере сборки, о дате сборки, о номере лицензии, о коде технической поддержки и т.д. Dallas Lock 8.0 МСБ (Рис. 551).

Рис. 551. Окно «О программе»

При нажатии на кнопку «Проверить обновление» выводится окно о наличии обновлений Dallas Lock 8.0 МСБ. Нажмите «ОК» (Рис. 552).

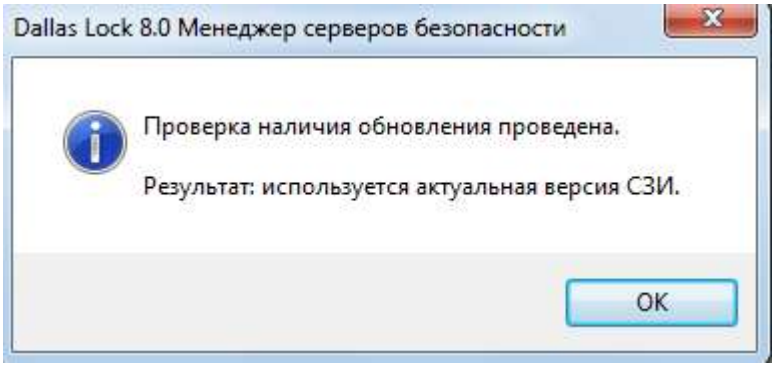


Рис. 552. Обновление СЗИ

Для смены номера лицензии необходимо нажать на кнопку «Сменить номер лицензии» и ввести действующий номер лицензии и код технической поддержки, нажать «ОК» (Рис. 553).

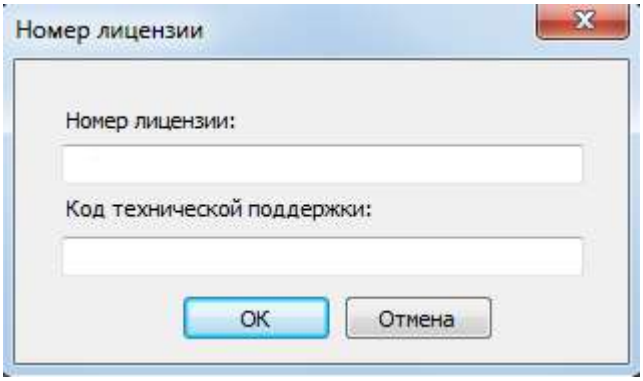


Рис. 553. Смена лицензии

Появится окно об успешной смене номера лицензии (Рис. 554).

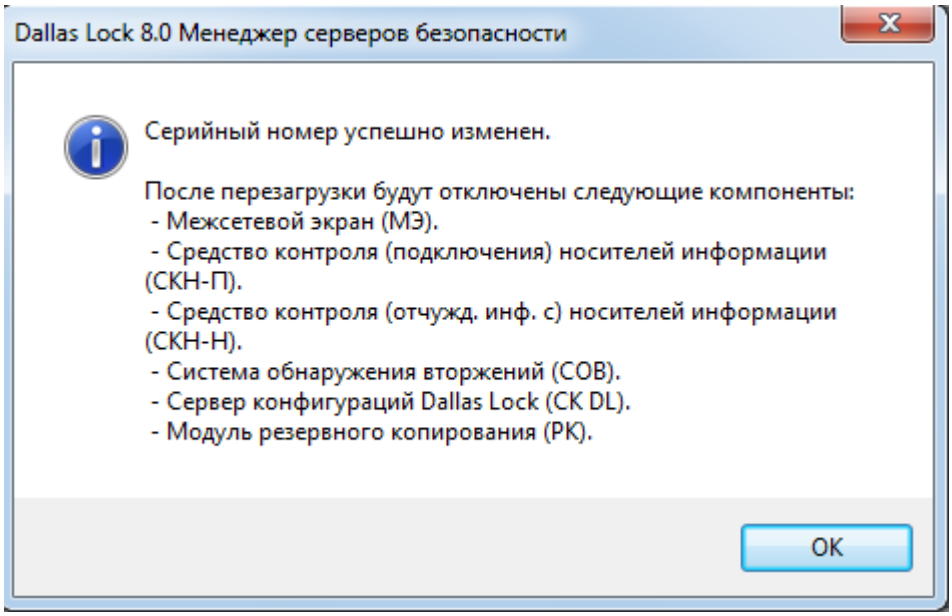


Рис. 554. Обновление номера лицензии

Примечание. На компьютере, где установлена КСБ, смена номера лицензии невозможна в МСБ, только через КСБ.

Примечание. Для использования функции сбора журналов с ДБ необходимо настроить СБ на локальное хранение журналов.

Для выхода из окна «О программе» нажмите «ОК».

19.14.3 Удаление Менеджера серверов безопасности

Удаление МСБ производится с помощью Мастера установок. В разных операционных системах удаление программ может осуществляться по-разному.

В ОС Windows 10 необходимо вызвать пункт «Параметры», выбрать пункт «Приложения». В появившемся окне два раза нажать на СБ и выбрать действие «Удалить», подтвердить удаление (Рис. 555).

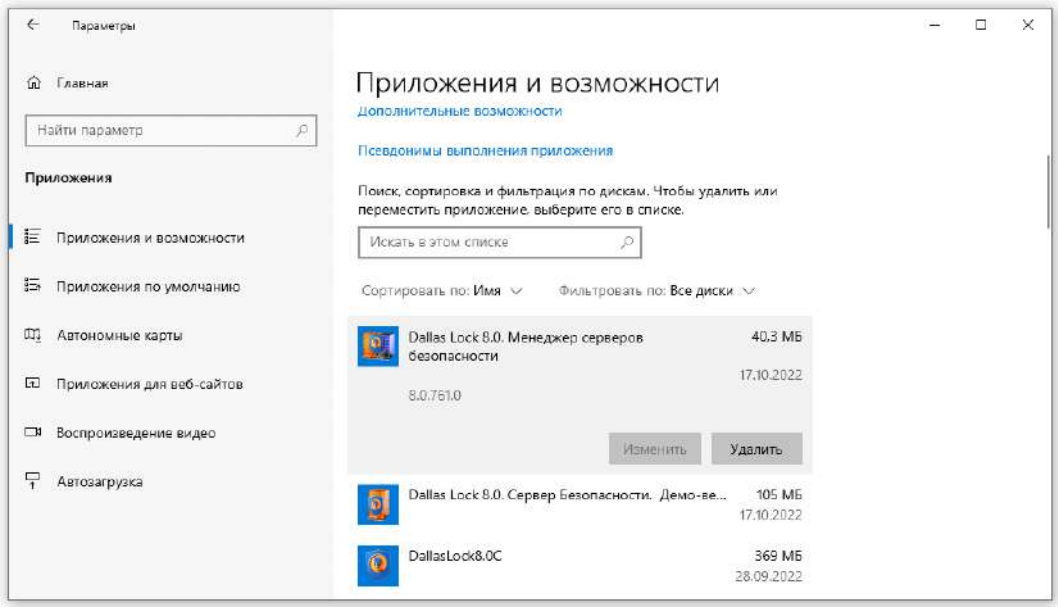


Рис. 555. Удаление МСБ

19.14.4 Параметры Менеджера серверов безопасности

19.14.4.1 Работа с ЛБ

Главное окно программы МСБ состоит из: заголовка, основного меню, дополнительного меню, дерева объектов, входящих в данный ЛБ и рабочей области (Рис. 556).

Дерево объектов состоит из корневого объекта ЛБ и имен СБ, добавленных в ЛБ. В зависимости от выбранного объекта содержимое правой части, список закладок окна будет меняться.

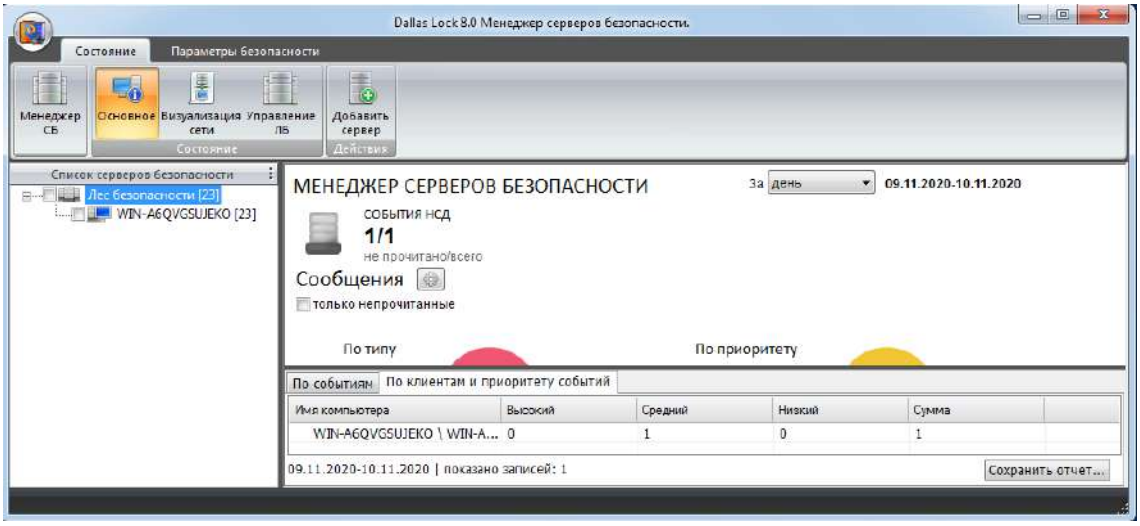


Рис. 556. Окно МСБ

По умолчанию в дереве объектов выбран корневой ЛБ, для которого доступны вкладки «Состояние» и «Параметры безопасности».

Состояние ЛБ

Для добавления СБ к списку существующих объектов необходимо в пункте «Действия» нажать «Добавить сервер». Откроется окно для заполнения параметров СБ (Рис. 557).

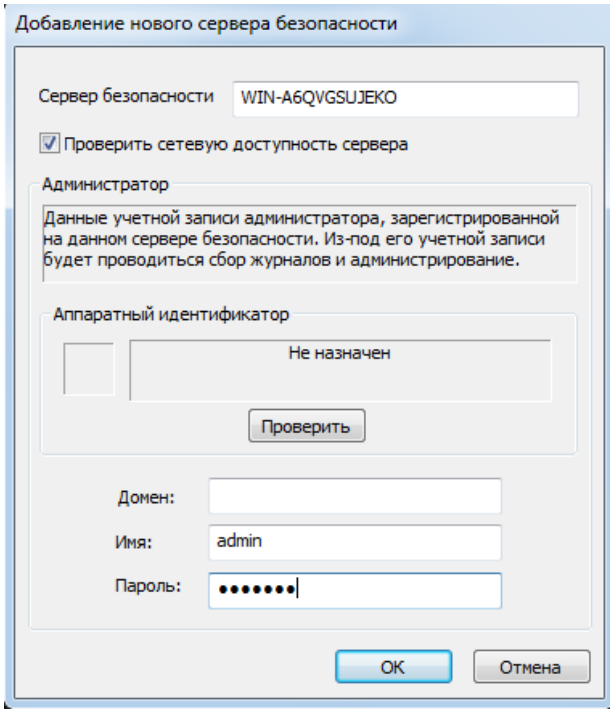


Рис. 557. Данные для добавления СБ в ЛБ

В появившемся окне необходимо ввести имя СБ и авторизационные данные, используя которые МСБ будет подключаться к данному СБ. Эти авторизационные данные должны принадлежать пользователю, зарегистрированному на данном СБ с правами суперадминистратора СБ Dallas Lock.

Примечание. Проверка введенных авторизационных данных осуществляется при подключении к СБ. Если были введены неверные данные, их возможно изменить при дальнейшей настройке.

Если будет установлен флаг «Проверять сетевую доступность сервера», то после нажатия кнопки «ОК», перед добавлением сервера в список, будет произведена попытка подключиться к данному серверу.

В дереве МСБ статусы СБ отображаются следующим образом:

— ПК с СБ выключен.

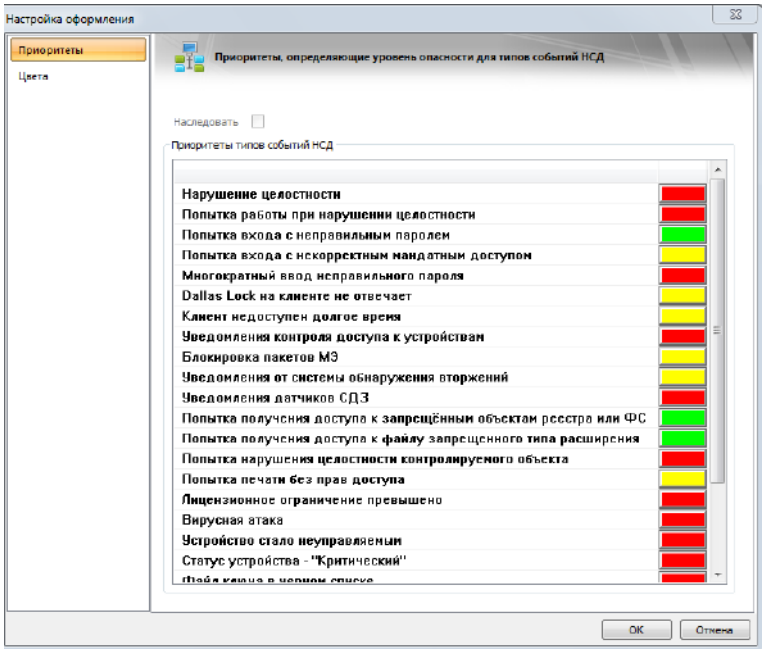
— ПК с СБ включен и функционирует.

— ПК с СБ включен, но служба СБ не реагирует на тестовый запрос. Вероятно, служба СБ на этом ПК остановлена.

Также в имени Сервера отображается число непрочитанных сообщений о событиях НСД. Через контекстное меню объекта в дереве серверов МСБ можно обрабатывать сообщения аналогично тому, как это делается в КСБ (обновить, очистить, загрузить из журнала, отметить прочитанными\непрочитанными).

В пункте «Основное» категории «Состояние» отображается суммарное количество событий НСД во всем ЛБ за выбранный период времени. При нажатии на определенный столбец гистограммы в таблице ниже отображаются все события НСД за выбранный интервал времени. Под таблицей расположена кнопка «Сохранить отчет» для возможности сохранения отфильтрованных записей таблицы в выбранную папку в выбранном формате файла (TXT, CSV, HTML, XML). В получившемся файле представлена информация из всех столбцов таблицы (рис. 8).

Для настройки рабочей области вкладки «Состояние» на уровне ЛБ необходимо нажать на кнопку , которая расположена рядом с заголовком «Сообщения». Появится окно «Настройка оформления», в котором настраивается приоритет появляющихся сообщений и выбор цвета на данные сообщения (Рис. 558).



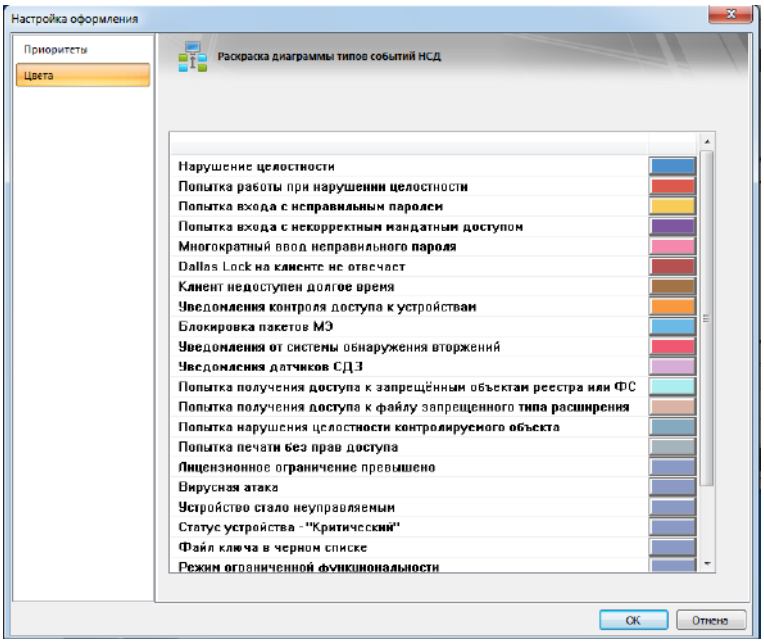


Рис. 558. Настройка оформления

Для построения топологии ДБ в категории «Состояние» нажать «Визуализация сети» (Рис. 559).

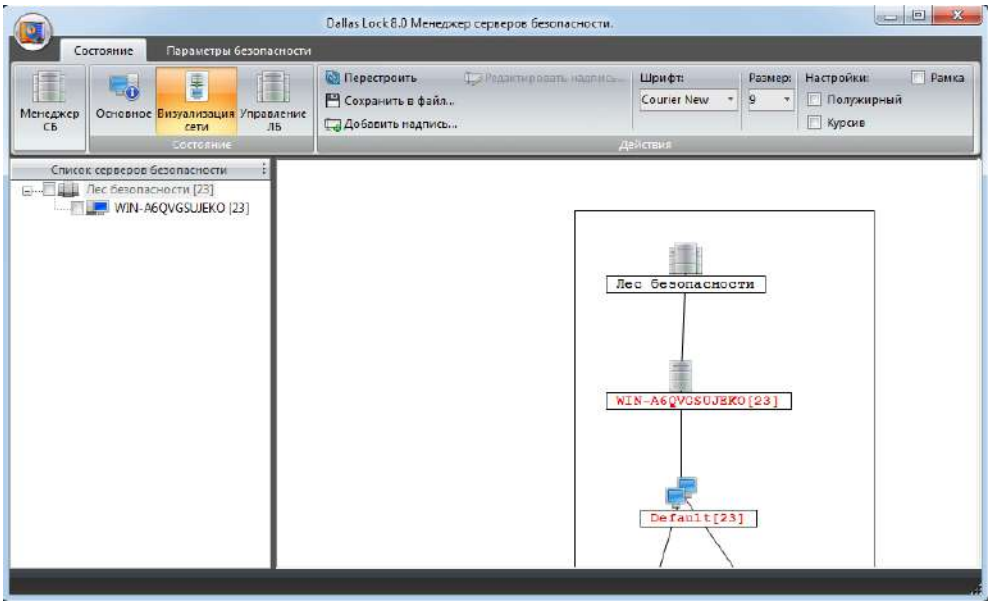


Рис. 559. Топология ДБ

Примечание. Построение топологии ДБ может занять несколько минут. Для обновления топологии ДБ нажать на кнопку «Перестроить» в категории «Действия».

Для сбора журналов со всего ЛБ необходимо отметить флагами объекты СБ или сам ЛБ и в категории «Состояние», нажать на пункт «Управление ЛБ». Откроется окно с кнопкой «Собрать все журналы», МСБ по очереди подключится к выбранным СБ и заберет с них все имеющиеся журналы (журналы СБ и клиентов). В окне будут отображаться записи процессов МСБ (Рис. 560).

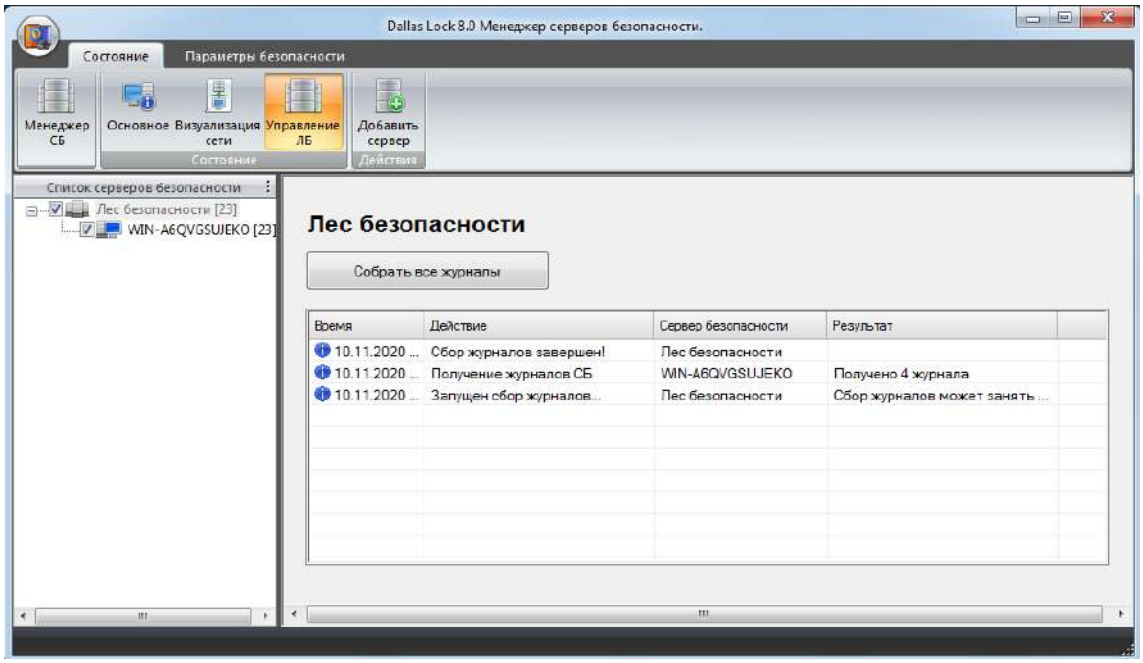


Рис. 560. Управление ЛБ

Параметры безопасности ЛБ

Вкладка «Параметры безопасности» ЛБ в дереве объектов МСБ позволяет назначать и изменять параметры безопасности во всем ЛБ, т. е. на каждом СБ, входящем в ЛБ.

На вкладке «Параметры безопасности» все политики разделены на 8 типов — политики входа и паролей, политики аудита, политики очистки остаточной информации, политики контроля целостности, политики блокируемых расширений, политики настройки МЭ и политики параметров СОВ (Рис. 561).

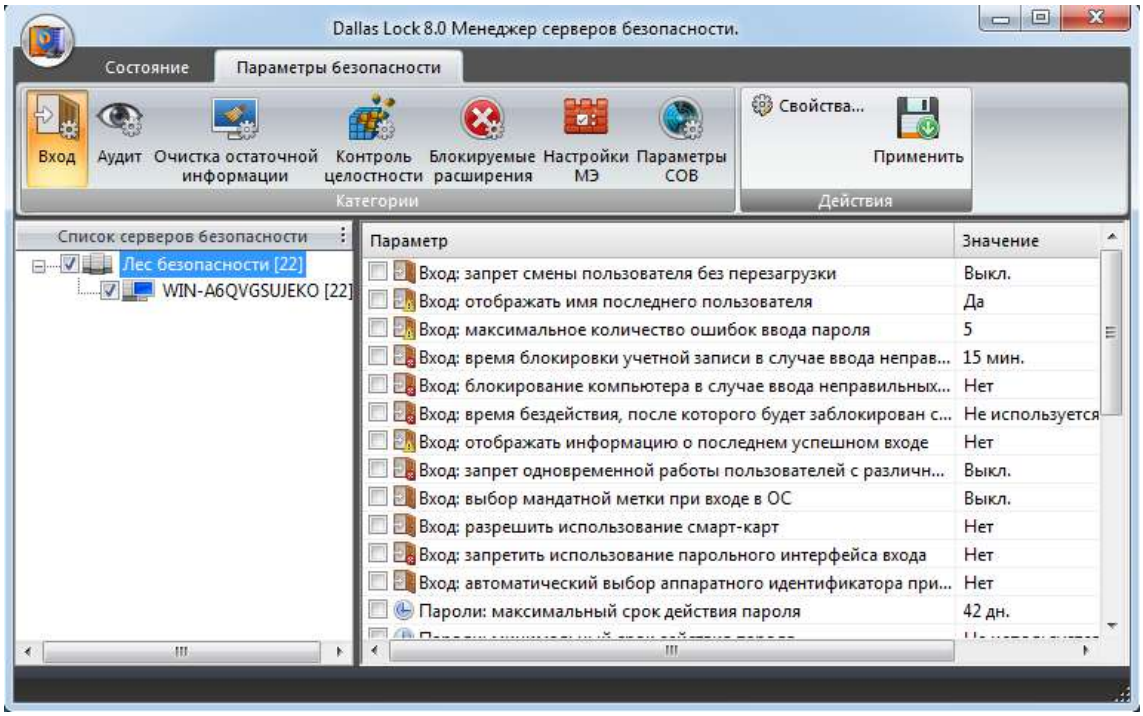


Рис. 561. Выбор параметров безопасности в МСБ

Механизм централизованного назначения параметров безопасности в ЛБ:

1. Для выбора параметров нужного типа необходимо выбрать соответствующую категорию. Откроется рабочая область со списком параметров.
2. Далее необходимо отметить флагами те параметры, которые необходимо изменить, и указать (изменить) их значения в окне свойств, нажать «ОК».

3. Затем необходимо в дереве объектов МСБ отметить флагами СБ, для которых нужно применить параметры, или сам ЛБ.
4. После того, как будут установлены значения параметров и выбраны объекты, следует нажать кнопку «Применить» на панели действий.

МСБ по очереди подключится к каждому СБ и изменит на нем значения соответствующих параметров. Неотмеченные параметры останутся неизмененными. В логе будет отображен ход процесса. Установка политики на СБ означает, что политика установится на СБ и во всех группах клиентов данного СБ. На клиенте политика будет установлена в процессе следующей синхронизации.

Параметры безопасности каждой категории, которые могут быть централизованно применены для всего ЛБ или отдельно взятого Сервера, входящего в данный ЛБ, подробно описаны в разделах данного документа, соответствующих настройкам локального администрирования с помощью оболочки администратора:

- настройки, касающиеся входа в систему и установки атрибутов пароля;
- настройки аудита;
- настройки параметров очистки остаточной информации;
- настройки осуществления контроля целостности;
- установка блокируемых расширений;
- настройки МЭ;
- параметры СОВ.

Примечание. Список блокируемых расширений, в отличие от списка других параметров, может быть применен к ЛБ или отдельному СБ только полностью.

19.14.4.2 Работа с ЛБ

Если в дереве объектов МСБ выбран какой-либо СБ, то для него становятся доступны вкладки «Состояние» и «Журналы».

Состояние СБ

Вкладка «Состояние» в категории «Основное» объекта СБ в дереве объектов МСБ отображает общее состояние клиентов, входящих в группу (Рис. 562).

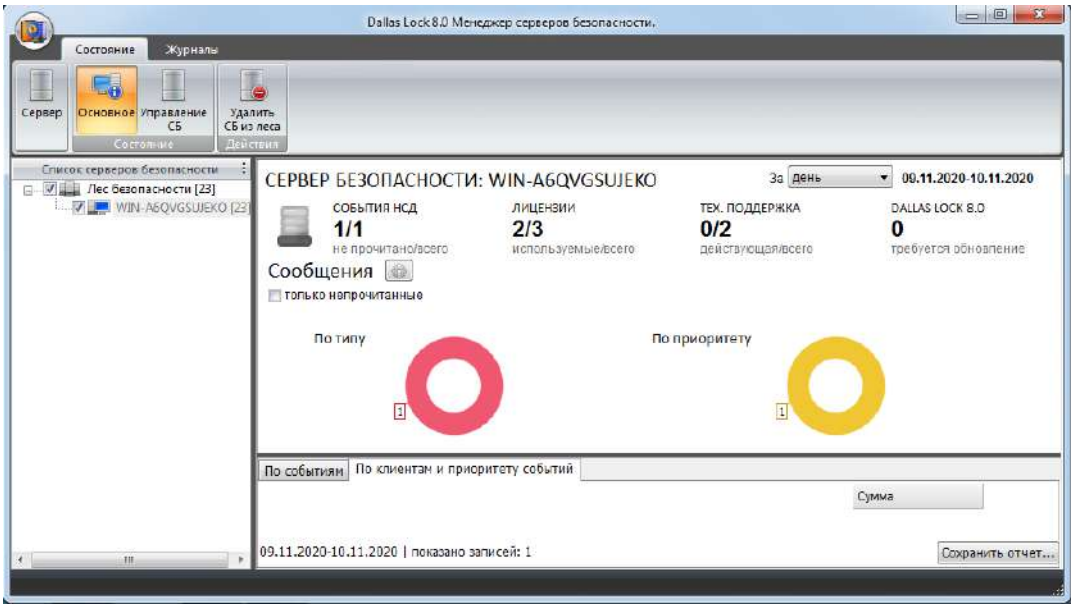


Рис. 562. Просмотр состояния объекта МСБ

В окне «Основное» для СБ отображается:

- Суммарное количество событий НСД за выбранный период времени.
- Количество включенных лицензий клиентов СБ.

- Количество клиентов СБ, на которых осуществляется техническая поддержка лицензий клиентов.
- Информация об актуальности версий СЗИ НСД DL 8.0.

При нажатии на определенный столбец гистограммы в таблице ниже отображаются вся информация за выбранный интервал времени. Под таблицей расположена кнопка «Сохранить отчет» для возможности сохранения отфильтрованных записей таблицы в выбранную папку в выбранном формате файла (TXT, CSV, HTML, XML). В получившемся файле представлена информация из всех столбцов таблицы.

Для настройки рабочей области вкладки «Состояние» на уровне СБ необходимо нажать на кнопку  , которая расположена рядом с заголовком «Сообщения». Появится окно «Настройка оформления» в котором доступен раздел «Приоритеты», с доступным чекбоксом «Наследовать». При включенном чекбоксе настройки приоритетов будут наследоваться у вышестоящего уровня. Указанные настройки учитываются при отображении кольцевых диаграмм и при формировании отчета (Рис. 563).

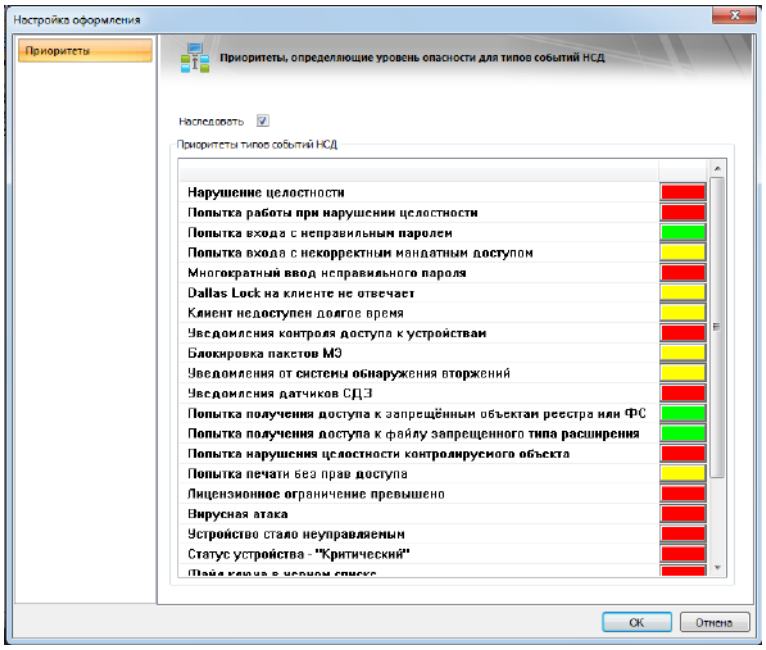


Рис. 563. Настройка оформления СБ

В категории «Состояние» при нажатии «Управление СБ» осуществляется переход на информационную панель СБ (Рис. 564).

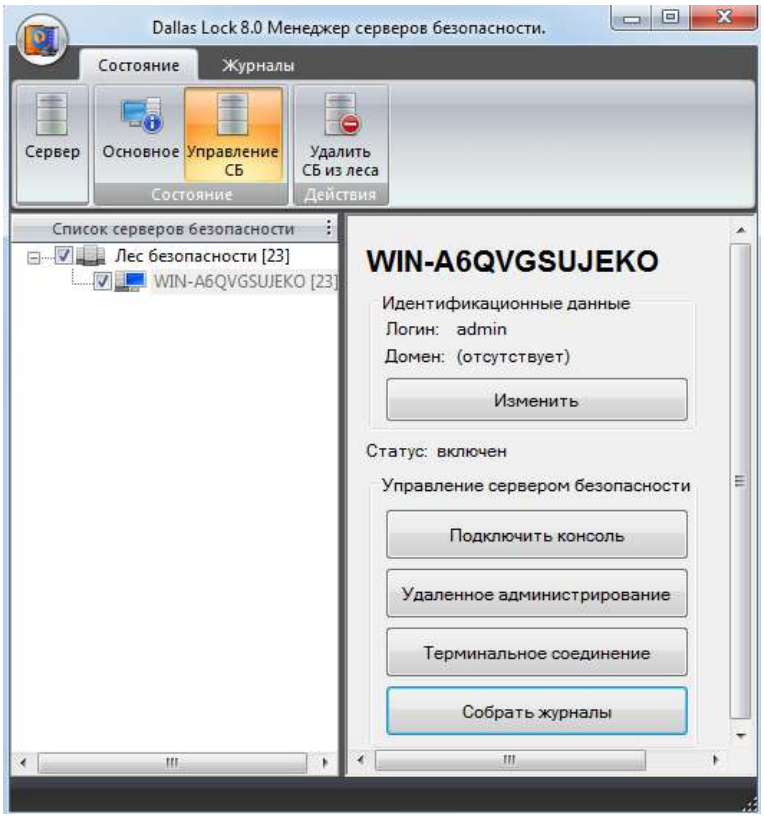


Рис. 564. Просмотр состояния объекта МСБ

Для каждого СБ МСБ позволяет:

- Изменить авторизационные данные, введенные при добавлении данного СБ в ЛБ (кнопка «Изменить»).
- Подключиться к КСБ на ПК с СБ для удаленного администрирования СБ. Обязательным условием является установка КСБ на данном ПК, с которого происходит подключение (кнопка «Подключить консоль»).
- Подключиться к оболочке администратора на ПК с СБ для удаленного администрирования (кнопка «Удаленное администрирование»).
- Подключиться к ПК с установленным СБ с помощью кнопки «Терминальное соединение».
- Собрать журналы с данного СБ. Эта операция аналогична сбору журналов со всего ЛБ за исключением, того что сбор будет происходить с одного СБ (кнопка «Собрать журналы»).

В категории «Действия» при нажатии «Удалить СБ из леса» появится информационное окно для подтверждения удаления СБ из ЛБ (Рис. 565).

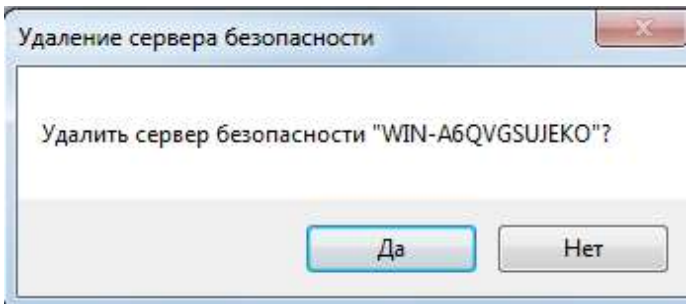


Рис. 565. Удаление СБ

Журналы СБ

Вкладка «Журналы» СБ состоит из следующих журналов:

1. Журнал входов.
2. Журнал управления учетными записями.
3. Журнал ресурсов.
4. Журнал печати.
5. Журнал управления политиками.

6. Журнал процессов.
7. Журнал резервного копирования.
8. Журнал пакетов МЭ.
9. Журнал соединений МЭ.
10. Журнал событий ОС.
11. Журнал трафика.
12. Журнал контроля приложений.
13. Журнал сервера безопасности.

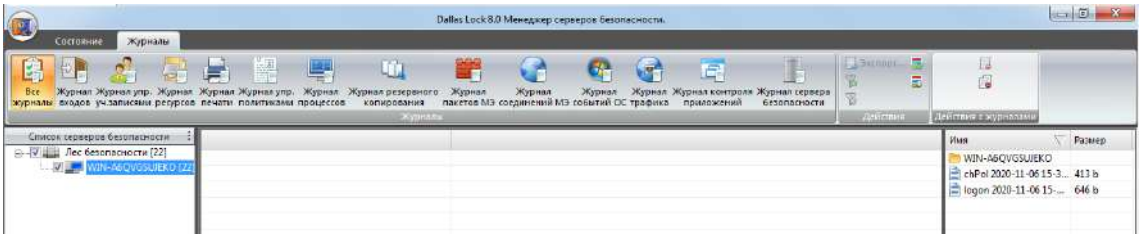


Рис. 566. Журналы СБ в окне программы МСБ

В верхней части окна можно выбрать тип журнала, в правой части рабочей области можно выбрать папку с журналами определенного клиента и конкретный журнал.

Двойной щелчок по корневой папке журналов позволяет вернуться на уровень вверх.

Панель кнопок «Действия» используется для задания параметров отбора событий, отображаемых в выбранном журнале. Действия для журналов в МСБ аналогичны действиям с журналами в оболочке администратора Dallas Lock 8.0.

Журналы формируются по принципу объединения записей полученных журналов одного типа с предыдущими до максимального размера журнала (20000 записей). Далее журнал архивируется в папку и начинает вестись заново).

20 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Для реализации централизованного управления различными модулями на клиентах необходимо использовать Единый центр управления Dallas Lock (ЕЦУ Dallas Lock), управление которым осуществляется отдельным приложением «Консоль ЕЦУ».

ЕЦУ Dallas Lock 8.0 позволяет осуществлять централизованное управление такими модулями клиентов, как СЗИ Dallas Lock 8.0 редакций «К» и «С» (включая компоненты МЭ и СОВ), СЗИ НСД Dallas Lock Linux, СЗИ ВИ Dallas Lock, СДЗ Dallas Lock и шлюз безопасности WAF Dallas Lock.

При работе с модулями СЗИ Dallas Lock 8.0 редакций «К» и «С» доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- удаленное развертывание модуля на АРМ;
- управление пользователями и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
  - сохранение конфигурации;
  - применение конфигурации;
  - изменение параметров лицензии и технической поддержки;
  - проверку целостности контролируемых объектов;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- настройка неактивного режима работы модуля;
- управление мандатными метками (только для Dallas Lock 8.0 редакции «С»);
- настройка аппаратных идентификаторов.

Некоторые параметры безопасности могут быть настроены сразу для всего ДБ, некоторые — для отдельных клиентов.

ЕЦУ предназначен для использования на ТС, таких как: персональные компьютеры, портативные компьютеры (ноутбуки, планшеты), серверы и ТС с поддержкой виртуальных сред (по технологии VMware и пр.) и технологии Windows To Go[16], работающих на 64-битной архитектуре процессоров под управлением операционных систем семейства Windows:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows 8 (Core, Pro, Enterprise);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Home, Pro, Enterprise);
- Windows Server 2022;

и семейства GNU Linux:

- Debian 10;
- Debian 11;
- CentOS 7;
- Red Hat Enterprise Linux Server 7;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6;
- Astra Linux Special Edition (Смоленск) 1.7;
- Альт Сервер 9;
- Альт Сервер 10;
- Альт Рабочая Станция 9.0;
- Альт Рабочая Станция 9.1;

[16] Поддержка технологии Windows To Go осуществляется только для Консоли ЕЦУ Dallas Lock.

- Альт Рабочая Станция 9.2;
- Альт Рабочая Станция 10.0;
- Альт Рабочая Станция К 10.0;
- РЕД ОС 7.3 Муром.

Примечание. Для обработки обращений от ЕЦУ должны быть открыты TCP/IP порты 17901 и 17903.

С подробным описанием ЕЦУ Dallas Lock можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock RU.48957919.501410-02 И6.

21 СЕРВЕР КОНФИГУРАЦИЙ

СК выполнен в виде отдельного программного продукта.

Модуль предназначен для централизованного управления процессами контроля за изменением состава ПО и контроля целостности файлов ПО, установленного на клиентских ПК, составления и утверждения Паспортов ПО.

Паспорт ПО представляет собой заверенную информацию о состоянии программной среды и фиксирует эталонное состояние программной среды.

При создании Проекта паспорта ПО в СК производится сканирование файлов контролируемых каталогов с целью вычисления хэш-суммы по алгоритму ГОСТ Р 34.11-94, а также сохраняются сведения о расположении файлов и метаданные.

Проект паспорта ПО отличается от Паспорта ПО отсутствием подписи.

В состав модуля входят следующие компоненты:

- серверная часть СК, которая осуществляет взаимодействие с клиентскими компонентами, сбор и обработку данных о состоянии программной среды контролируемых ПК, хранение данных в БД программного модуля, регистрацию событий;
- консоль СК, которая представляет собой пользовательский интерфейс для управления функциональными возможностями СК;
- клиентская часть, которая входит в состав СЗИ Dallas Lock 8.0.

СК предназначен для работы на ТС, работающих под управлением следующих ОС:

- Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
- Windows Server 2008 R2 (Foundation, Standard, Web, Enterprise, Datacenter);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012;
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Home, Pro, Enterprise, Education);
- Windows Server 2016;
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Enterprise, Education, Pro, Home);
- Windows Server 2022 (Standard, Datacenter).

СК позволяет:

- выполнять сбор по сети информации о ПО ПК с установленным СЗИ Dallas Lock 8.0;
- отслеживать изменения в установленном ПО на клиентах;
- выполнять контроль и фиксацию состояния программной среды;
- формировать Проект паспорта ПО, Паспорт ПО;
- утверждать Паспорт ПО с помощью установки простой электронной подписи;
- создавать и редактировать права учетных записей СК.

С подробным описанием СК можно ознакомиться в Инструкции по использованию сервера конфигураций RU.48957919.501410-02 И4.

Для просмотра Паспортов ПО, их обработки и редактирования параметров СК пользователь должен быть указан в значении параметров «СК DL: просмотр паспортов ПО», «СК DL: обработка паспортов ПО» и «СК DL: редактирование параметров» категории «Права пользователей» оболочки администратора Dallas Lock 8.0 либо состоять в группе, указанной в данном параметре.

22 ВОССТАНОВЛЕНИЕ КОМПЬЮТЕРА ПРИ СБОЕ СИСТЕМЫ ЗАЩИТЫ

В некоторых случаях возможны ситуации, когда по каким-либо причинам доступ на ЗАРМ осуществить невозможно. Невозможно загрузить ОС предположительно из-за сбоя работы системы защиты Dallas Lock 8.0.

В этом случае можно воспользоваться аварийным отключением системы защиты. Аварийное отключение может производиться в ручном режиме или в автоматическом с помощью диска восстановления.

Примечание. В ситуациях, когда вход в ОС осуществляется, необходимо воспользоваться штатной функцией удаления (раздел «Удаление системы защиты»).

Если Windows не загружается, однако модуль загрузчика DL работает корректно, значит, нет поврежденных зон преобразования, и дальнейшее аварийное восстановление имеет смысл.

Общий порядок аварийного отключения следующий:

1. Восстановление преобразованных областей жесткого диска (данный этап не выполняется, если диски не были преобразованы) (для Dallas Lock 8.0-C) и отключение модуля загрузчика DL.
2. Отключение модуля интерактивного входа и подмена системных файлов Dallas Lock 8.0 (подмена библиотек Dallas Lock 8.0 на библиотеки Windows) вручную или с помощью загрузочного диска восстановления.
3. Редактирование реестра вручную или с помощью специальной утилиты.

22.1 Обратное преобразование жесткого диска в аварийном режиме

Данный параметр доступен только для Dallas Lock 8.0 редакции «С».

Обратное преобразование областей жесткого диска в аварийном режиме выполняется, если диски были преобразованы. Обратное преобразование следует произвести с помощью модуля загрузчика DL. Если модуль загрузчика DL работает корректно, то есть возможность вызвать аварийное обратное преобразование дисков прямо из загрузчика.

Для этого необходимо ввести в поле авторизации загрузчика PIN-код администратора и выбрать действие: Аварийное восстановление (рис. 567), нажав F2.

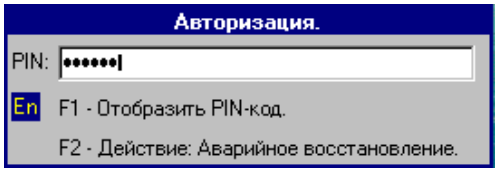


Рис. 567. Аварийное восстановление диска через загрузчик

Запустится процесс обратного преобразования, по завершении которого появится соответствующее сообщение.

Внимание! Процесс аварийного восстановления жесткого диска используется в экстренных случаях и по времени является довольно длительным. Например, на физическом ПК под управлением ОС Windows 7 системный диск объемом 40 Гб аварийно восстанавливается 1 час 25 минут.

После завершения обратного преобразования областей дисков будет произведена попытка загрузки ОС. При сбое системы защиты Dallas Lock 8.0 загрузка ОС станет невозможной, в этом случае необходимо произвести аварийное отключение системы защиты в ручном режиме или с помощью загрузочного диска (см. «Аварийное отключение Dallas Lock 8.0 с помощью загрузочного диска»).

22.2 Аварийное отключение загрузчика для ПК с UEFI-интерфейсом BIOS

Помимо стандартного BIOS модуль загрузчика DL поддерживается на ПК с материнскими платами, имеющими UEFI–интерфейс и GPT–разметку жесткого диска. Для данных ПК аварийное отключение

загрузчика Dallas Lock 8.0-C имеет свои особенности.

Если включен модуль загрузчика DL, но нет возможности осуществить вход в загрузчике, то его можно отключить. Для этого необходимо выполнить следующие шаги:

1. Необходимо загрузиться с установочного диска Windows (или любого другого с доступом к командной строке и ФС) и получить доступ к командной строке, например, с помощью нажатия Shift+F10.
2. В командной строке необходимо ввести команду «Diskpart». Откроется утилита (командный интерпретатор), позволяющая управлять объектами (дисками, разделами или томами).
3. Далее необходимо ввести команду «List volume». Данная команда позволит отобразить список всех доступных объектов (разделов), определить их номер и букву. В списке нужно определить системный раздел, в котором хранится загрузчик. Это будет скрытый неименованный раздел размером ≈100 Мбайт. Необходимо определить, какой порядковый номер имеет данный раздел.
4. Далее необходимо ввести команду «Select volume номер_раздела». На раздел с загрузчиком будет перемещен фокус.
5. Далее необходимо ввести команду «Assign letter F». Для раздела с загрузчиком будет назначена буква диска (в данном примере — F).
6. Далее с помощью команды «Exit» необходимо выйти из утилиты. Командная строка вернется автоматически.
7. В командной строке необходимо перейти на раздел с загрузчиком с помощью команды «Cd /d F:» (на раздел F в данном примере) или просто «F:».
8. В выбранном разделе необходимо перейти в папку с загрузчиком с помощью команды «Cd efi\microsoft\boot».
9. Далее необходимо ввести следующие команды:
   - «Rename bootmgfw.efi bootmgfw_dl.efi»;
   - «Rename bootmgfw_old.efi bootmgfw.efi».

   Данными командами файлы установленного загрузчика Dallas Lock 8.0 («bootmgfw.efi») и стандартного загрузчика Windows («bootmgfw_dl.efi») переименовываются и меняются местами. Просмотреть содержимое папки, чтобы убедиться в наличии файлов загрузчика, можно с помощь команды «dir:».
10. После этого необходимо перезагрузить компьютер и осуществить аварийное отключение системы защиты Dallas Lock 8.0. Если Загрузка ОС на защищенном ПК происходит корректно, то удаление Dallas Lock 8.0 производится штатным образом с помощью Мастера установок Windows (см. «Удаление системы защиты»).

Примечание. Следует иметь в виду, что если было произведено аварийное отключение загрузчика на ПК с UEFI-интерфейсом BIOS, то далее через оболочку администратора Dallas Lock 8.0 производить отключение модуля загрузчика DL не нужно, так как один раз он был уже отключен вручную. Если же отключение загрузчика через оболочку администратора было выполнено, то необходимо повторно выполнить команду переименования файлов «Rename bootmgfw_old.efi bootmgfw.efi».

11. После удаления Dallas Lock 8.0 с помощью Мастера установок перед загрузкой ОС необходимо опять получить доступ к командной строке и переименовать файл загрузчика Windows, который был автоматически переименован уже в процессе удаления Dallas Lock 8.0:
    - «Rename bootmgfw_old.efi bootmgfw.efi».
12. Если по каким-то причинам возможности загрузить ОС нет, то следует воспользоваться аварийным отключением системы защиты в ручном режиме или с помощью загрузочного диска (см. ниже).

Примечание. Приоритет загрузки в UEFI–интерфейсе должен быть установлен у параметра «Загрузка Windows Boot Manager».

22.3 Аварийное отключение Dallas Lock 8.0 с помощью загрузочного диска

После завершения восстановления преобразованных областей дисков (если такие были) необходимо загрузиться со специального диска восстановления СЗИ Dallas Lock 8.0. Для получения данного диска необходимо обратиться к разработчику.

22.3.1 Отключение загрузчика и подмена системных файлов

Необходимо вставить компакт-диск для аварийного восстановления Dallas Lock 8.0 в привод и произвести загрузку с него (предварительно установив в BIOS загрузку с CD).

Примечание. Если на диске есть преобразованные области, то при попытке загрузки диска восстановления появится сообщение о необходимости произвести предварительное восстановление зон преобразования. После вывода такого сообщения, нужно отправить компьютер в загрузку с жесткого диска (HDD) и руководствоваться предыдущим пунктом инструкции.

В появившемся меню загрузочного диска необходимо выбрать пункт «Аварийное отключение DL 8.0» (Рис. 568).

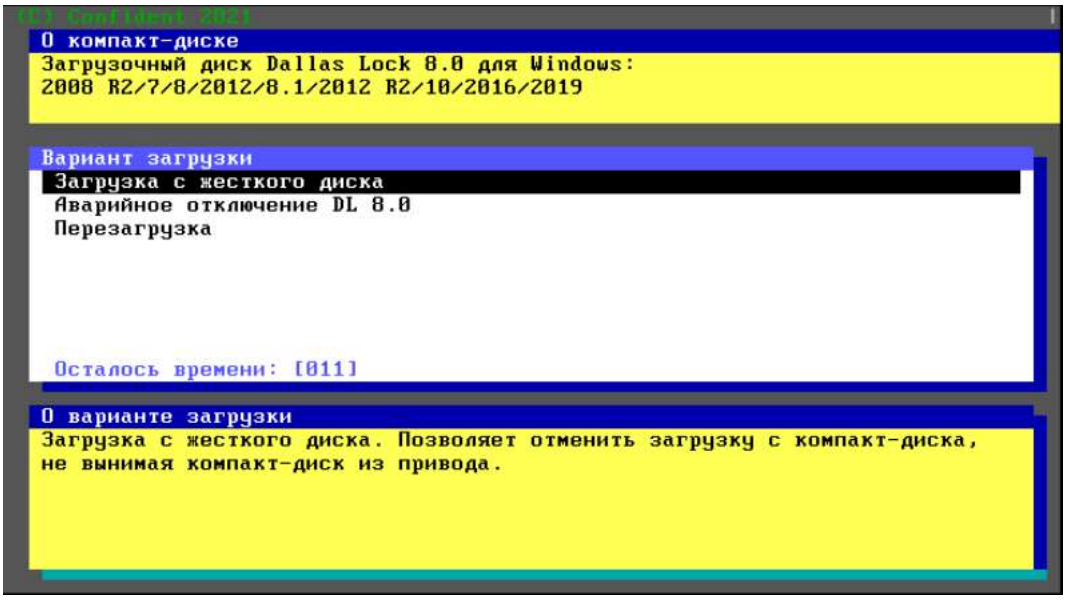


Рис. 568. Меню консоли диска восстановления

После загрузки в консоли аварийного восстановления будут предложены команды:

- **«DLOFF» —** аварийное отключение Dallas Lock в Windows;
- **«DLMBROFF» —** отключение загрузчика Dallas Lock;
- **«RESTART» —** перезагрузка;
- **«HELP» —** справка.

Если был активирован модуль загрузчика DL, то его необходимо отключить командой «**DLMBROFF»**. После этого система выведет сообщение о том, что в MBR установлен оригинальный загрузчик.

Далее необходимо отключить саму систему защиты Dallas Lock 8.0 командой «**DLOFF»**. После этого система выведет сообщение о том, что система защиты аварийно отключена.

Затем необходимо ввести команду «**RESTART»** для перезагрузки компьютера. После перезагрузки система защиты Dallas Lock 8.0 будет отключена.

22.3.2 Очистка реестра

Далее для корректного отключения системы защиты необходимо внести изменения в реестр. Сделать это вручную можно способом, описанным в предыдущем разделе, или с помощью специальной утилиты по очистке реестра «**DlRestoreSystem»**, которая находится на диске аварийного восстановления в директории «**util».**

Необходимо войти в ОС под учетной записью администратора Windows и запустить файл «DlRestoreSystem.exe» с диска (рис. 569).

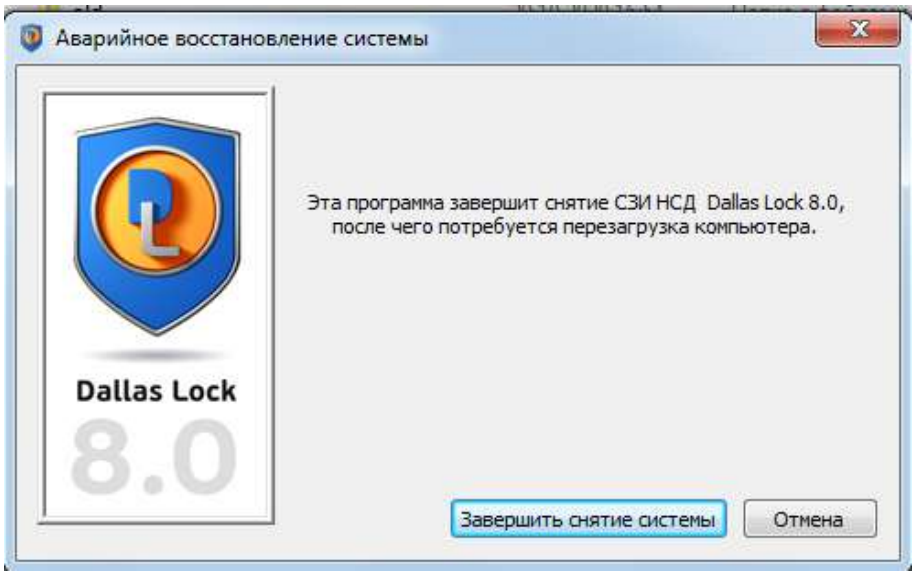


Рис. 569. Запуск утилиты по очистке реестра

После запуска данной утилиты с правами администратора и команды завершения снятия СЗИ Dallas Lock 8.0 будет предложено перезагрузиться. Также в процессе снятия системы защиты будет предложено оставить или удалить системную папку «DLLOCK80» с хранящимися в ней журналами и другими конфигурационными файлами.

После перезагрузки система защиты Dallas Lock 8.0 будет удалена с компьютера, и можно будет снова запустить ее установку.

Если по каким-либо причинам данный способ аварийного восстановления не сработал, то необходимо воспользоваться аварийным восстановлением в ручном режиме, описанном в следующем разделе.

Примечание. Перед выполнением очистки реестра необходимо отключить антивирус. В противном случае работа утилиты может быть заблокирована.

22.4 Аварийное отключение Dallas Lock 8.0 в ручном режиме

22.4.1 Порядок аварийного отключения для Windows

1. Для аварийного отключения системы защиты Dallas Lock 8.0 в ОС Windows необходимо получить доступ к ФС.

Для этого можно воспользоваться, в том числе, платформой восстановления Windows Recovery Environment (WinRE), которая является «преемником» консоли восстановления для предыдущих версий ОС.

WinRE может быть загружена с установочного диска ОС. Но можно воспользоваться встроенным инструментом восстановления, не требующим загрузки с CD. Для этого необходимо запустить меню дополнительных вариантов загрузки (перед началом загрузки ОС нажать F8 на клавиатуре) (рис. 570).

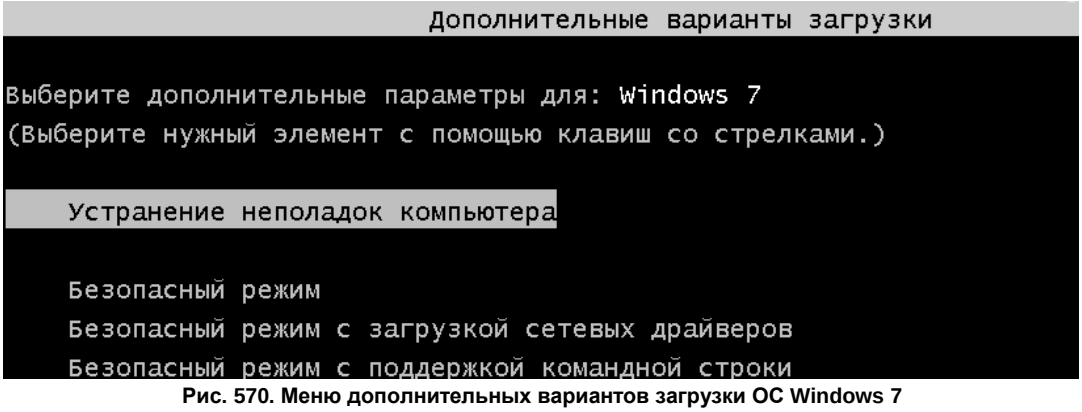


Рис. 570. Меню дополнительных вариантов загрузки ОС Windows 7

Необходимо выбрать пункт «Устранение неполадок компьютера» (Repair Your Computer). Windows загрузит необходимые файлы и запустит процесс восстановления. Система попросит выбрать язык и ввести авторизационные данные. Появится необходимое окно параметров восстановления системы. В нем следует выбрать открытие окна командной строки.

С помощью командной строки необходимо переключиться на диск (раздел жесткого диска), где установлена система защиты Dallas Lock 8.0. Следует учесть, что буква того диска, который определен консолью восстановления как диск с установленной системой защиты, может не совпадать с буквой диска назначенного ОС, на который система защиты была установлена (диск C) (рис. 571).

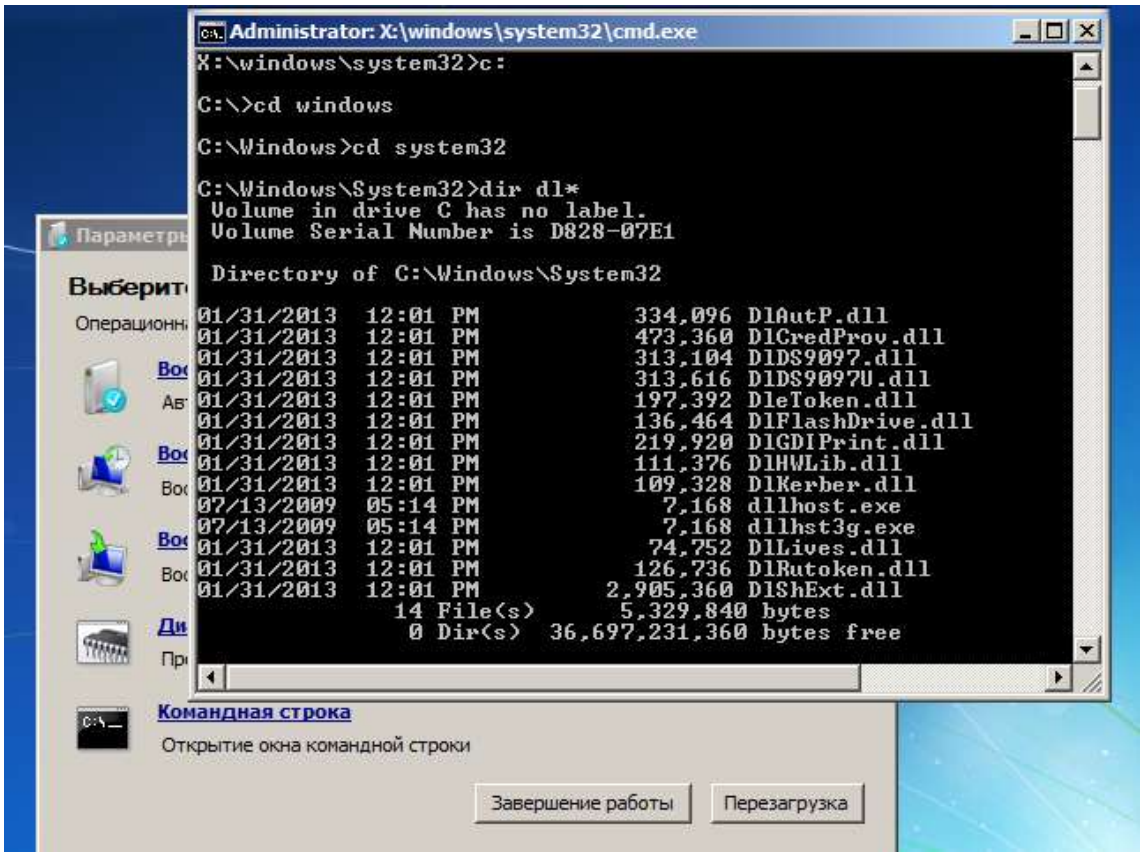


Рис. 571. Консоль восстановления системы в Windows 7 и список системных файлов

Примечание. Следует учесть, что платформа восстановления WinRE имеется не на всех загрузочных дисках. Можно воспользоваться другими аварийно-восстановительными средствами получения прямого доступа к ФС в обход установленной ОС, например, Live CD Windows.

2. **После получения доступа к ФС необходимо подменить системные файлы.**

После получения доступа к ФС необходимо зайти в папку System32 с помощью команды «cd %windir%\system32» и ввести следующие команды:

- «ren dlautp.dll dlautp_.dll»;
- «copy msv1_0.dll dlautp.dll»;
- «ren dlkerber.dll dlkerber_.dll»;
- «copy kerberos.dll dlkerber.dll»;
- «ren dllives.dll dllives_.dll»;
- «copy livessp.dll dllives.dll»[17];
- «ren dlcloud.dll dlcloud_.dll (только для Windows 10)»;
- «copy cloudAP.dll dlcloud.dll (только для Windows 10)».

Для отключения драйвера МЭ (при установленной версии с МЭ или МЭ и СОВ) необходимо выполнить команды «cd %windir%\system32\drivers», «ren dlfirewall.sys» и «dlfirewall_.sys».

3. **После подмены системных файлов необходимо очистить реестр.**

После отключения модуля интерактивного входа для корректного отключения системы защиты

[17] Отсутствие файлов «dllives.dll» и «livessp.dll» не является критичным.

необходимо внести изменения в реестр. Открыть редактор реестра можно с помощью командной строки командой «regedit» после ввода предыдущих команд. Можно открыть реестр из ОС, так как после подмены системных файлов компьютер должен успешно загрузиться (в поле ввода меню «Пуск» ввести команду «regedit»). В редакторе реестра следует проделать следующие операции:

1. Изменить значение на «0» параметра «Disabled» по пути:
   - для Windows 7/2008R2
     «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}»;
2. Удалить ветки реестра «{9123E0C2-FF5E-4b38-BAB9-E2FA800D2548}» и «{9123E0C2-FF5E-4b38-BAB9-E2FA810E2649}» по пути
   «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers».
3. Полностью удалить из реестра следующие разделы:
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlConv»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlDisk»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlFlt»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlHwCtrl»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dlfirewall»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlLwf»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlIPSService»;
   - «HKEY_CLASSES_ROOT\DaLoDisk»;
   - «HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DaLoDisk».

   Актуально только для 32-х битных ОС Windows 7 и Windows Server 2008 R2:
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLCRYPT»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLFlt».

   Для удаления разделов из ветки «Root» необходимо изменить права доступа для текущего пользователя (это удобнее сделать не для каждого ключа, а для ветки «Root»).
4. Изменить значение ключа «UpperFilters» в ветке
   «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}» вместо «DlDisk PartMgr» следует оставить «PartMgr».
5. Необходимо удалить значение «dlhwctrl» для ключей в ветке
   «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\...» в тех разделах, в которых он имеется. Для этого можно воспользоваться автопоиском по ветке реестра (функция «Найти…» в контекстном меню и кнопка F3 для перехода к следующей записи).
6. Необходимо удалить значение «DlDisk» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E965-E325-11CE-BFC1-08002BE10318}».
7. Необходимо удалить значение «DlDisk» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E980-E325-11CE-BFC1-08002BE10318}».
8. Необходимо изменить значение ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E96B-E325-11CE-BFC1-08002BE10318}» вместо «kbdclass DlFlt» следует оставить «kbdclass».

Примечание. При корректной загрузке ОС данные операции возможны и в режиме «Безопасный режим с поддержкой командной строки». В этом случае потребуется дополнительная авторизация в ОС Windows с правами администратора.

После выполнения описанных операций необходимо перезагрузить компьютер. После перезагрузки система защиты будет отключена, теперь можно снова запустить ее установку либо воспользоваться функцией «Восстановить» в окне установки и удаления программ.

Примечание. Для корректной установки Dallas Lock 8.0 после ее аварийного отключения необходимо удостовериться в отсутствии приложения «BlockIcon». Для этого нужно получить доступ в папку по пути «C:\Users\All users\Start Menu\Programs\Start Up» («C:\Documents snd Settings\All users\Start Menu\Programs\Start Up» или «C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка»). Сделать это можно, например, с помощью командной строки. В случае наличия «BlockIcon» его необходимо удалить.

23 РЕЗЕРВНОЕ ВОССТАНОВЛЕНИЕ ДИСКА

НСД может привести не только к потере ценных данных, но и к выводу из строя ОС в процессе доступа к данным в обход СЗИ. Данный вид потери данных относится к человеческому фактору, но ОС может выйти из строя в результате воздействия вредоносных программ, стихийных или техногенных бедствий, или производственного брака. Чтобы иметь возможность быстро восстановить ОС можно создать образа диска.

Создание образа диска (image) — это процесс создания резервной копии раздела или всего жесткого диска, то есть резервное копирование Windows, настроек, драйверов, программ, данных пользователя.

Простой рабочей станции компании даже в течение часа может привести к крупным финансовым потерям. Восстановление системы из сохраненного образа диска занимает значительно меньше времени, чем установка заново ОС, программ, создание пользователей и выполнение настроек.

На сегодняшний день существует множество программ, позволяющих создавать образы дисков. В данном разделе будет рассмотрено восстановление с помощью программы Acronis. Acronis — это современная линейка сертифицированных корпоративных средств резервного копирования и восстановления.

Большинство программ по работе с жестким диском являются корпоративными, поэтому компания должна самостоятельно и своевременно их приобрести.

Рекомендуется сохранять образ диска до установки Dallas Lock 8.0. Не обязательно делать образ всего жесткого диска, достаточно сделать образ только системного диска с установленной ОС.

Если же необходимо сделать образ диска с установленной Dallas Lock 8.0, то необходимо сохранять образ всего жесткого диска, так как при установке Dallas Lock 8.0 прописывается информация о Dallas Lock в загрузочную область жесткого диска (master boot record — MBR).

23.1 Создание загрузочного диска Acronis

Существует несколько версий Acronis для резервного копирования и аварийного восстановления рабочих станций, физических серверов, виртуальных машин, баз данных и т. д. Во всех версиях алгоритм создания образа примерно одинаковый.

Существуют автономные версии программы и расширенные версии с централизованным управлением. Версии с централизованным управлением предназначены для создания резервных копий для нескольких машин. Они включают в себя сервер управления, обеспечивающий централизованное управление, и узлы хранения резервных копий данных. В отличие от автономных версий расширенные версии обеспечивают удаленное подключение к ПК. В обоих случаях для каждой машины, для которой должна создаваться резервная копия, требуется отдельная лицензия.

Далее будет рассмотрено создание образа диска защищенной Dallas Lock 8.0 автономной рабочей станции при помощи Acronis Backup & Recovery 11 Workstation. В разных версиях Acronis последовательность действий сохранения и восстановления образа диска может несколько отличаться.

Примечание. Для корректного сохранения и восстановления образа диска с помощью программы Acronis необходимо выполнение следующих условий:

1. На диске не должно быть преобразованных областей жесткого диска (см. «Прозрачное преобразование дисков»).
2. Если включен модуль загрузчика DL, то в процессе резервного восстановления диска дополнительно необходимо отметить сохранение и восстановление MBR (или раздела с загрузчиком для материнских плат с интерфейсом UEFI).
3. Если восстановление образа диска происходит не на том ПК, с которого был снят образ, необходимо учесть, что разметка разделов диска должна быть одинаковой с тем ПК, с которого был снят образ.

Установка программы Acronis подробно описана в соответствующей документации, с которой можно ознакомиться на официальном сайте продукта[18]. После установки на локальный компьютер программа полностью готова к работе и не требует дополнительных настроек.

В меню «Пуск» появляется пункт меню «Acronis», который содержит значки компонентов Acronis Backup & Recovery 11 (рис. 572):

- Консоль управления — инструмент для локальной работы с программой восстановления.
- Мастер создания загрузочного носителя для аварийного восстановления.

[18] https://www.acronis.ru/support/documentation/

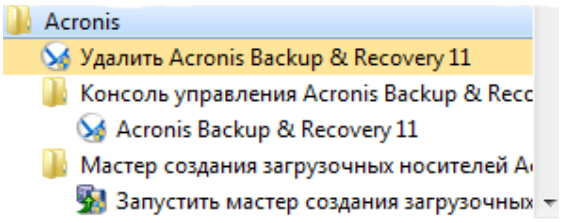


Рис. 572. Меню компонентов программы Acronis

Чтобы запустить программу, необходимо выбрать Acronis Backup & Recovery 11.

При первом запуске программа известит о необходимости создания загрузочного диска. Это действие можно отложить и запустить мастер создания загрузочных носителей позже. Созданный этой программой загрузочный носитель позволит в дальнейшем восстановить ОС компьютера, которую не удастся запустить, или работать с сохранением и восстановлением файлов на компьютере без установленной программы Acronis (рис. 573).

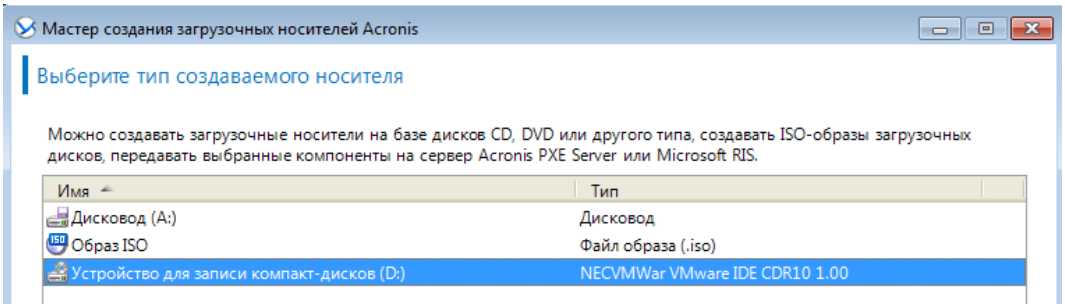


Рис. 573. Создание загрузочного носителя для восстановления

После выбора необходимых параметров и нажатия кнопки «Продолжить» загрузочный диск для восстановления будет записан (рис. 574).

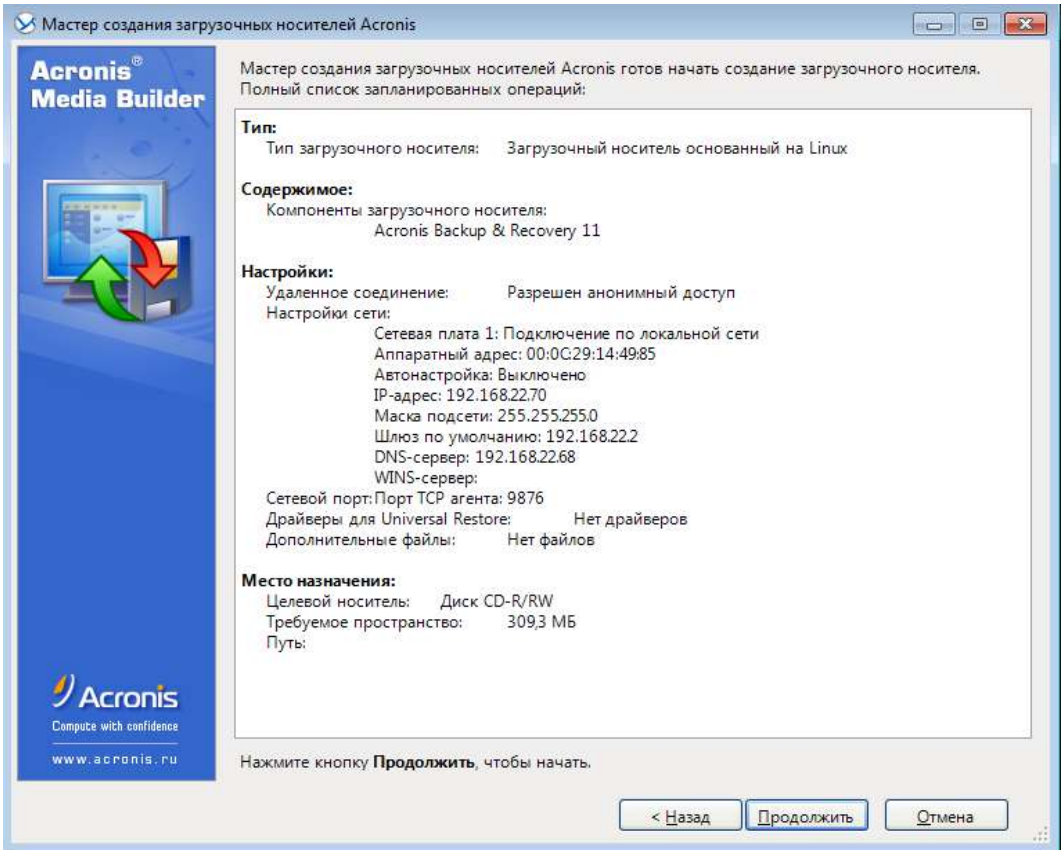


Рис. 574. Настройки мастера создания загрузочного носителя

Примечание. При запуске Acronis Backup & Recovery 11/11.5 на Windows 8/8.1 может возникать ошибка «Error 1075 The dependency service does not exist or has be marked for deletion». Для корректного продолжения работы программы необходимо удалить запись «protected storage» из ключа реестра Windows HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MMS\DependOnService и перезагрузить компьютер.

23.2 Сохранение образа диска с помощью Acronis

Чтобы сохранить сам образ диска, необходимо воспользоваться Консолью управления.

Данную консоль можно запустить, воспользовавшись пунктом меню, а можно — запустив компьютер с предварительно записанного загрузочного компакт-диска, настроив BIOS компьютера на загрузку с диска (рис. 575).

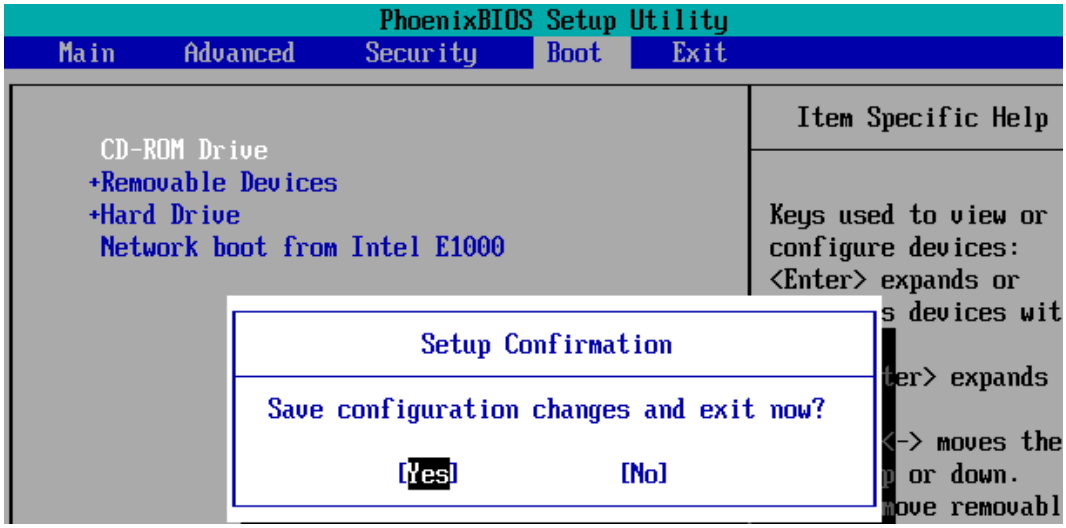


Рис. 575. Настройка BIOS компьютера для загрузки с диска

Следует учесть следующее. При запуске Консоли управления с защищенного СЗИ Dallas Lock 8.0 компьютера не с загрузочного диска, а через меню программ, необходимо зарегистрировать в системе защиты учетную запись для запуска служб Acronis.

После установки программы в ОС автоматически создаются учетные записи данных для служб Acronis. Для корректной работы программы учетную запись Acronis необходимо зарегистрировать еще и в СЗИ обычным созданием учетной записи и включить для нее свойство «Служебный пользователь». В противном случае ОС выдаст сообщение: «Служба Managed Machine Service Acronis недоступна», и программа не сможет работать.

Зарегистрировать службу Acronis можно, выбрав ее из списка локальных учетных записей, воспользовавшись кнопкой поиска (рис. 576).

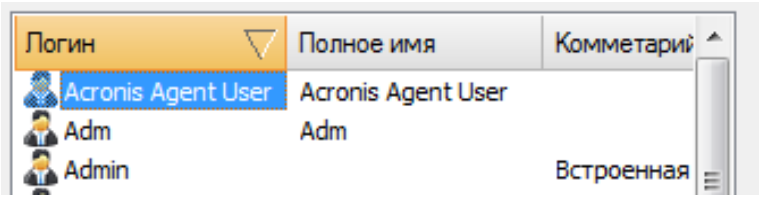


Рис. 576. Регистрация учетной записи службы Acronis в СЗИ

После регистрации учетной записи для службы необходимо перезагрузить компьютер. После этого на вкладке «Сессии» в списке появится сессия службы Acronis (рис. 577).

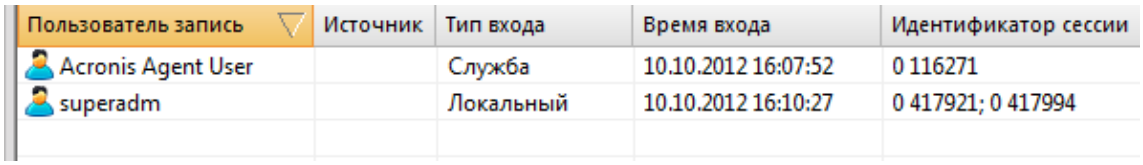


Рис. 577. Сессия учетной записи службы Acronis

После этого консоль управления Acronis запустится корректно (рис. 578).

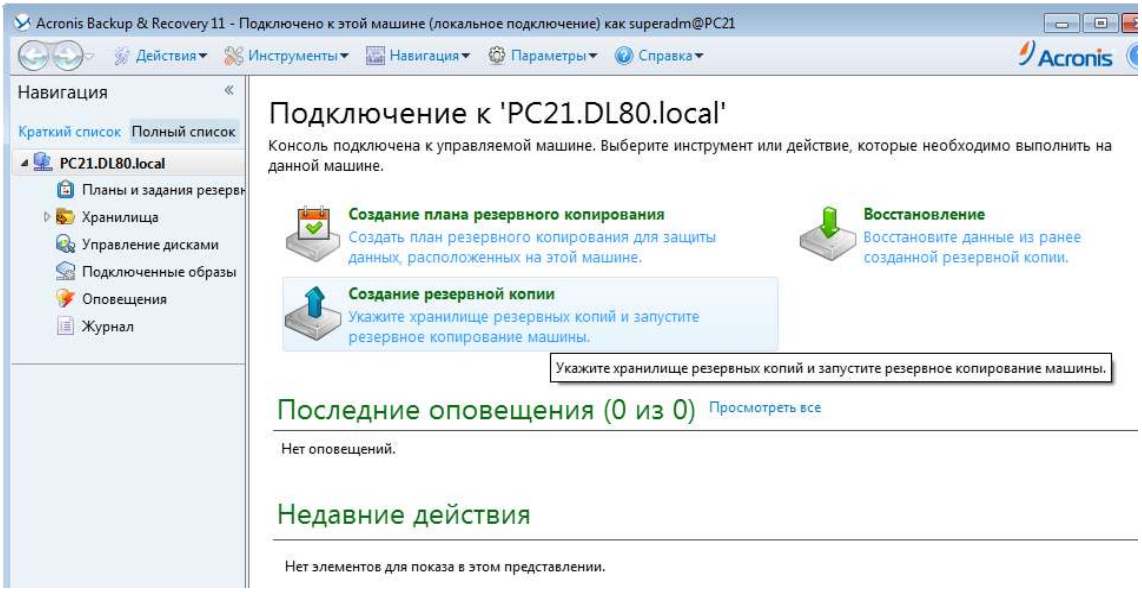


Рис. 578. Окно консоли управления Acronis

Окно программы состоит из дерева пунктов меню, основной области и верней строки меню. Дерево меню содержит следующие основные элементы:

- **Имя машины**, к которой в настоящий момент подключена консоль.
- Элемент для управления **планами и заданиями резервного копирования** на ПК: запуск, изменение, остановку и удаление планов и заданий резервного копирования, просмотра хода их выполнения.
- **Хранилища** — для управления индивидуальными хранилищами и архивами для создаваемых резервных копий и выполнения операций с ними.
- **Оповещения** — для просмотра предупреждающих сообщений.
- **Управление дисками** — для выполнения операций на жестких дисках машины.
- **Журнал** — для просмотра сведений об операциях, выполненных программой на управляемой машине.
- **Подключенные образы** — для управления подключенными образами.

Для того, чтобы создать и сохранить резервную копию диска, необходимо выбрать в основном окне программы соответствующий пункт «Создание резервной копии». Появится окно выбора параметров для создания резервной копии (рис. 579).

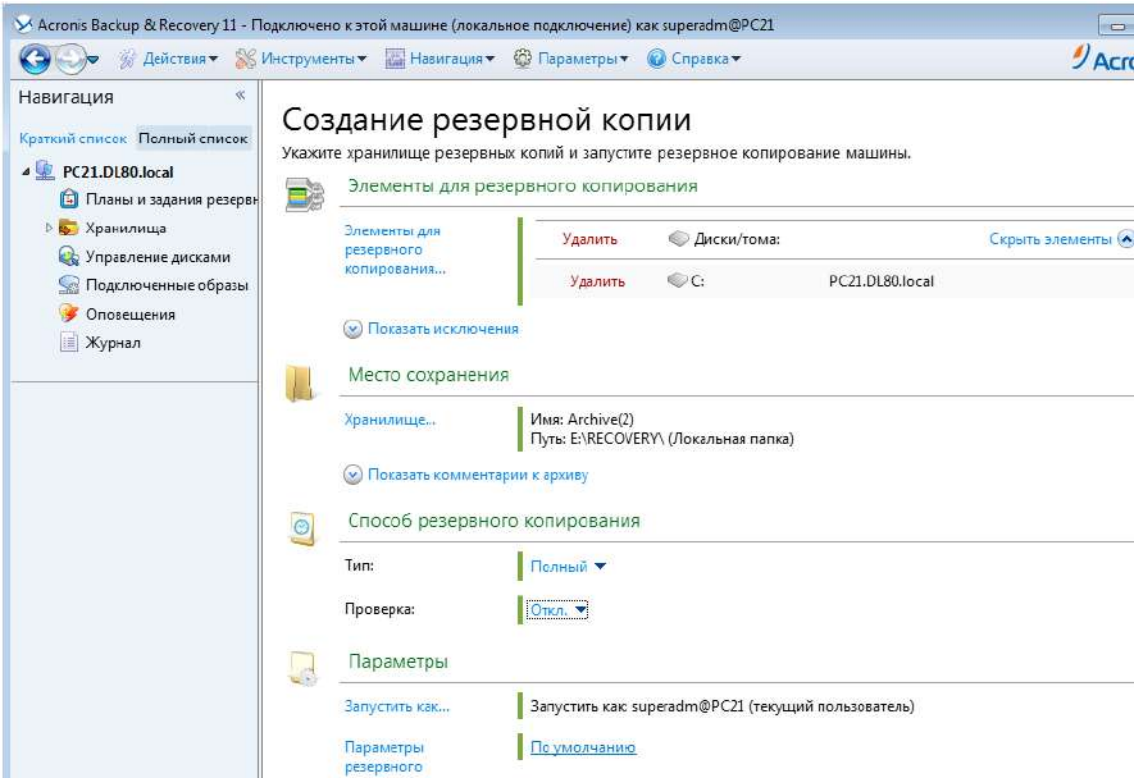


Рис. 579. Настройки создания резервной копии образа диска

В этом окне необходимо обязательно выбрать элемент для резервного копирования: весь жесткие диск или раздел и место для сохранения резервной копии (рис. 580, рис. 581).

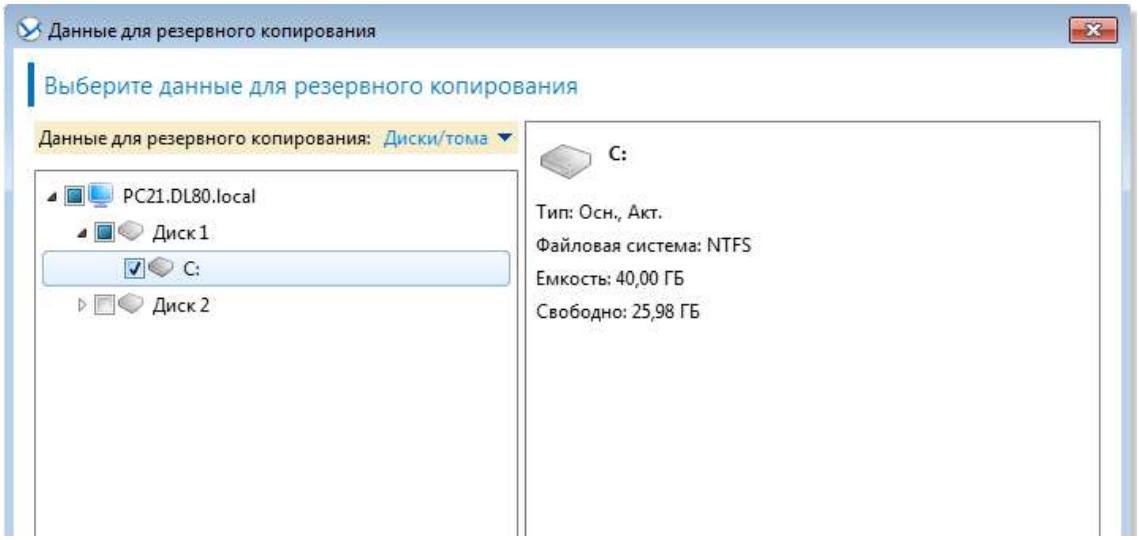


Рис. 580. Выбор диска для создания его образа

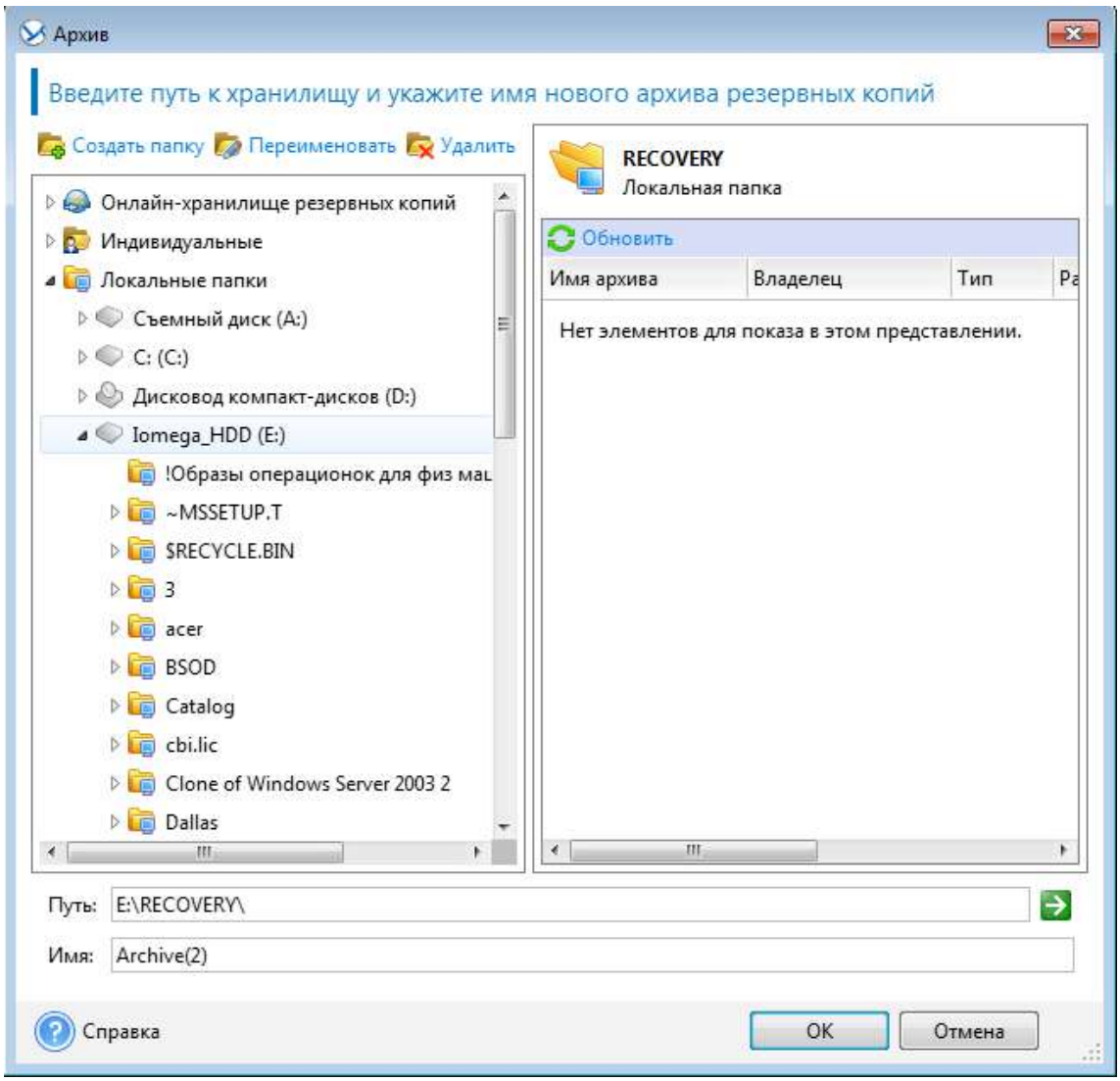


Рис. 581. Выбор хранилища для резервной копии образа диска

Параметры способов резервного копирования стоит оставить без изменения. После нажатия кнопки «OK» запустится процесс резервного копирования образа диска в выбранное хранилище (рис. 582).

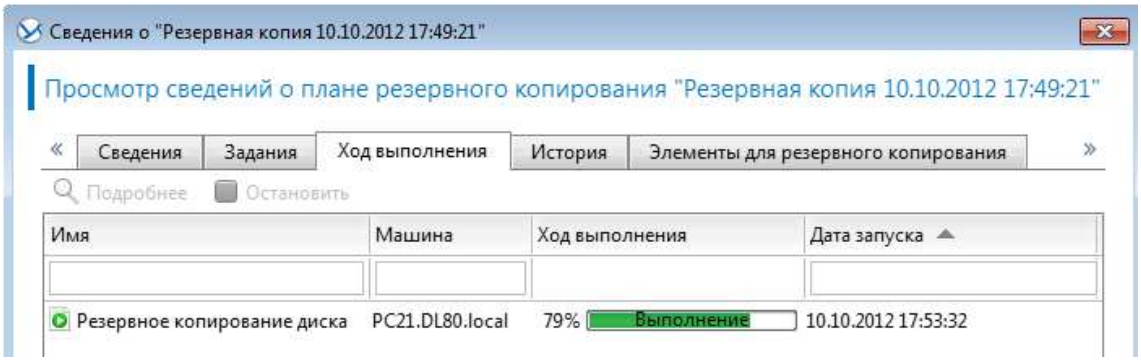


Рис. 582. Процесс создания резервной копии

После завершения создания образа появится соответствующее сообщение об успешном окончании операции.

23.3 Восстановление образа диска с помощью Acronis

При выходе из строя ОС компьютера, когда отсутствуют возможность ее загрузки, можно воспользоваться восстановлением образа диска с данными с помощью сохраненной его копии программой Acronis. Для этого необходим загрузочный диск с консолью управления программы Acronis Backup & Recovery 11, с которого нужно запустить ПК, предварительно настроив для этого BIOS (рис. 583).

Рис. 583. Окно приветствия при загрузке с диска Acronis

После выбора в окне приветствия загрузку программы Acronis появится окно описанной выше Консоли управления Acronis, в которой необходимо выбрать пункт «Восстановление» (Рис. 584).

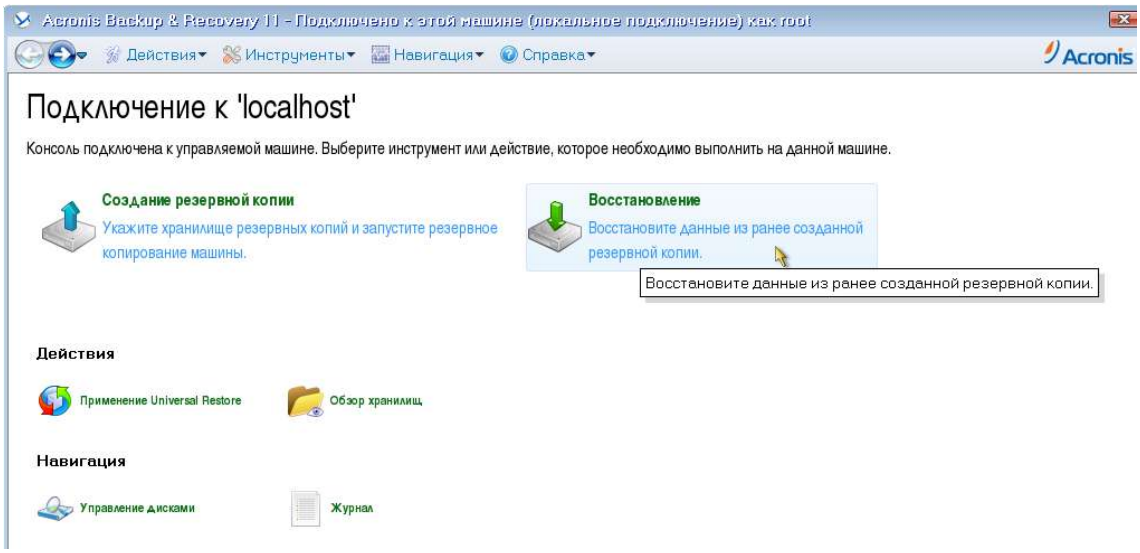


Рис. 584. Выбор пункта восстановления в консоли управления Acronis

В параметрах восстановления необходимо указать хранилище сохраненного образа, предварительно подключив его, если это съемный носитель (рис. 585, Рис. 586).

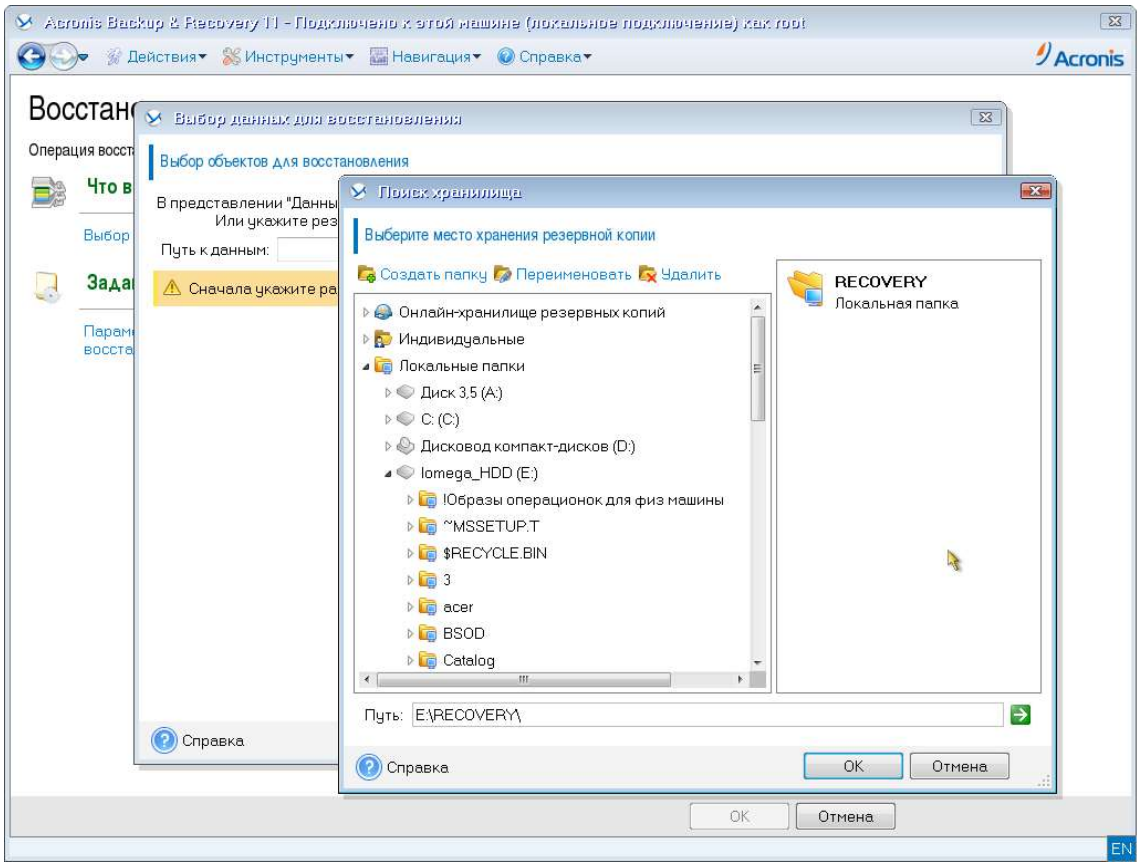


Рис. 585. Выбор хранилища созданной резервной копии для восстановления

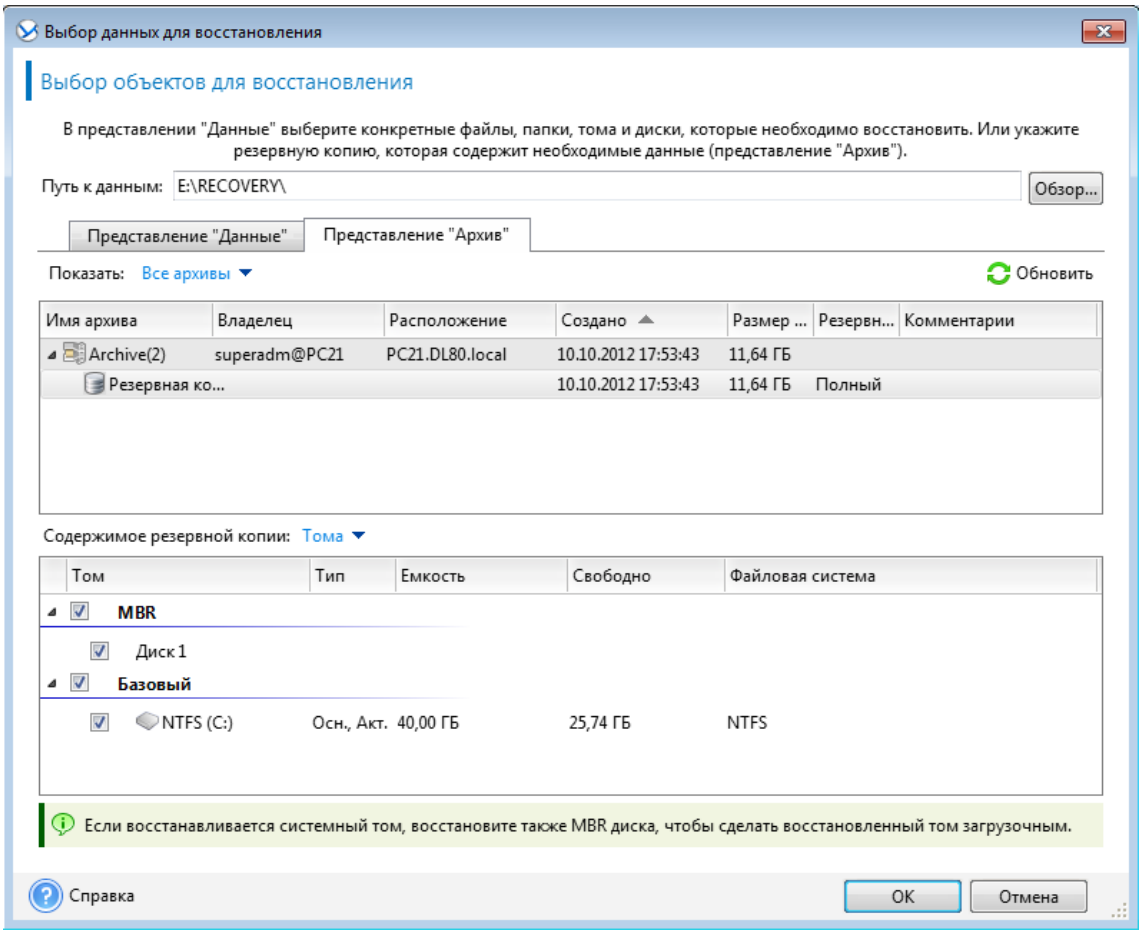


Рис. 586. Параметры восстановления резервной копии

Также необходимо указать место назначения, в которое будут восстановлены выбранные данные. Автоматически выбранные объекты восстановления будут восстановлены на физические диски ПК, так как Acronis Backup & Recovery 11 автоматически сопоставляет образы дисков или томов с целевыми дисками, но при определенных настройках программы это можно сделать вручную.

После установки параметров и нажатия «OK» начнется процесс восстановления. По завершении которого потребуется перезагрузка компьютера и вход в восстановленную ОС (рис. 587).

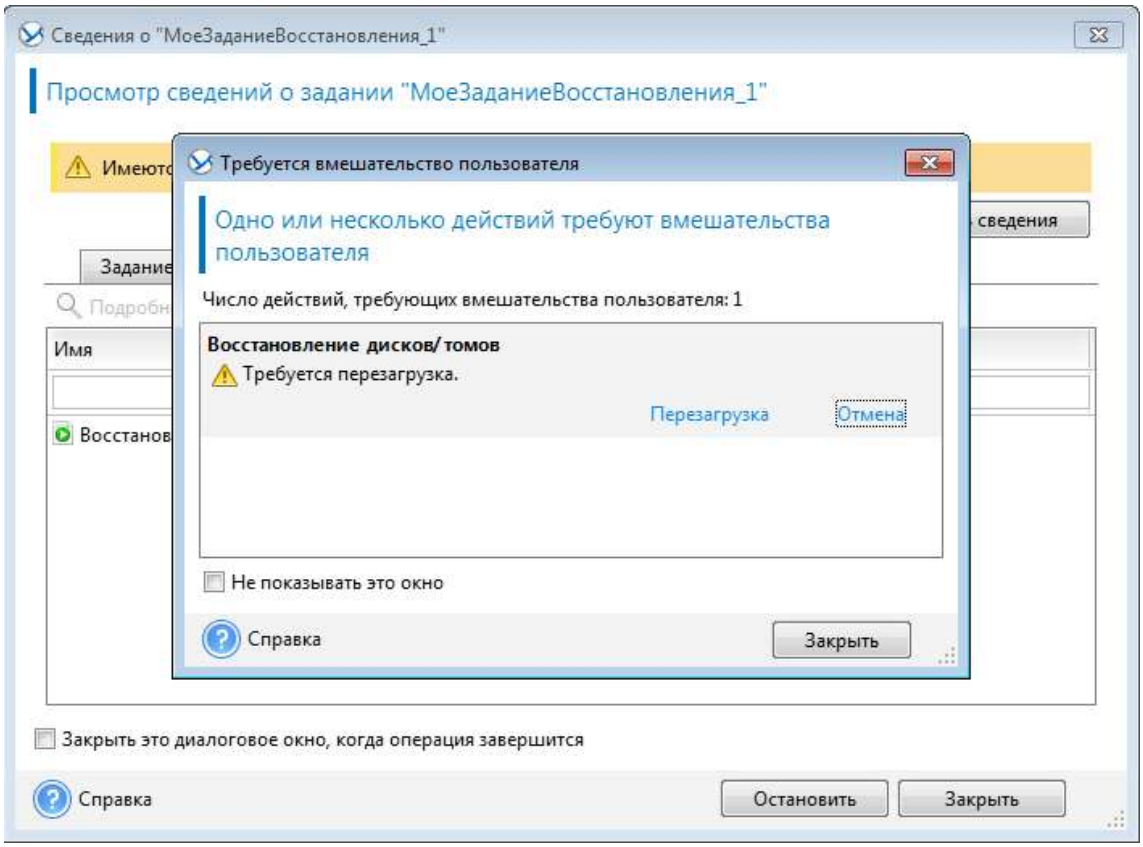


Рис. 587. Завершение процесса восстановления

Таким образом, данные жесткого диска ПК будут восстановлены. Следует учесть, что восстановление данных будет произведено с той версией системы Dallas Lock 8.0 и теми настройками, которые были установлены при создании образа.

Термины и сокращения

Некоторые термины, содержащиеся в тексте руководства, уникальны для системы защиты Dallas Lock 8.0, другие используются для удобства, третьи выбраны из соображений краткости.

Термины *«компьютер», «ПК», «рабочая станция»* считаются эквивалентными, и используются в тексте руководства.

Домен безопасности — организация единой политики безопасности совокупностью СБ и клиентских рабочих станций, работающих под управлением СБ.

Загрузчик — модуль загрузчика DL, отрабатывает между Включением ПК и до начала загрузки ОС.

Замкнутая программная среда — режим работы защищенного ПК, при котором для конкретных пользователей определяется список доступных для работы программ.

Клиент — компьютер, защищенный Dallas Lock 8.0, входящий в состав ДБ.

Мышь — ручной манипулятор, преобразующий механические движения в движение курсора на экране.

Параметры безопасности, или политики безопасности — совокупность правил по обеспечению безопасности информации, выраженные настраиваемыми категориями системы защиты.

Суперадминистратор ЗАРМ Dallas Lock — пользователь, под учетной записью которого выполнена установка системы защиты.

Суперадминистратор СБ Dallas Lock — пользователь, под учетной записью которого выполнена установка системы защиты на СБ.

Администратор ЗАРМ Dallas Lock — пользователь, наделенный всеми полномочиями на администрирование системы защиты на ЗАРМ.

Администратор СБ Dallas Lock — пользователь, наделенный всеми полномочиями на администрирование СБ системы защиты.

Аудитор ЗАРМ Dallas Lock — пользователь, наделенный правами на просмотр параметров аудита и журналов системы защиты.

Аудитор СБ Dallas Lock — пользователь, наделенный правами на просмотр параметров аудита и журналов на СБ системы защиты.

Администратор ОС ЗАРМ — пользователь, наделенный полномочиями на администрирование ОС на защищаемом компьютере.

Администратор ОС СБ — пользователь, наделенный полномочиями на администрирование ОС на СБ.

Сокращение	Полная формулировка
АЛП	Автоматические локальные правила
АС	Автоматизированная система
БС	Безопасная среда
ЗАРМ	Защищенное автоматизированное рабочее место
ЗПС	Замкнутая программная среда
ДБ	Домен безопасности
ИПС	Изолированная программная среда
КСБ	Консоль сервера безопасности
ЛВС	Локальная вычислительная сеть
ЛБ	Лес безопасности
МСБ	Менеджер серверов безопасности
ОС	Операционная система
ОУ	Оперативное управление
ПК	Персональный компьютер
ПО	Программное обеспечение
СБ	Сервер безопасности
СЗИ	Система защиты информации от несанкционированного доступа
СК	Сервер конфигураций

СЛ	Сервер лицензий
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ТС	Техническое средство
СОВ	Система обнаружения вторжений
БРП	База решающих правил
ФС	Файловая система
ЭП	Электронная подпись
ЭЦП	Электронно-цифровая подпись
AD	Active Directory
DL	Dallas Lock 8.0
MBR (Master Boot Record)	Системная область жесткого диска. Содержит программы начальной загрузки ОС и информацию о размещении логических дисков. Используется на этапе загрузки компьютера
BIOS	Набор микропрограмм, образующих системное ПО, которые обеспечивают начальную загрузку компьютера и последующий запуск ОС
SP (Service Pack)	Пакет обновлений для ОС
VNC	Virtual Network Computing
WFP (Windows Filtering Platform)	Функциональная возможность для драйверов ОС семейства Windows, упрощающая анализ сетевого трафика.
KES	Kaspersky Endpoint Security
KSC	Kaspersky Security Center