СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

ПАВЛОВА С. А. • ШАНЬГИН Д. А.

САНКТ – ПЕТЕРБУРГ, 2023

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данное пособие предназначено для рассмотрения теоретических вопросов и приобретения практических навыков использования сертифицированного ФСТЭК России продукта – программно-аппаратного средства защиты информации от несанкционированного доступа Dallas Lock 8.0.

Документ включает в себя 6 лабораторных работ, в которых рассматривается назначение и возможности:

- средства защиты информации от несанкционированного доступа СЗИ НСД Dallas Lock 8.0;
- персонального межсетевого экрана СЗИ НСД Dallas Lock 8.0;
- системы обнаружения вторжений СЗИ НСД Dallas Lock 8.0;
- системы контроля накопителей СЗИ НСД Dallas Lock 8.0;
- модуля резервного копирования СЗИ НСД Dallas Lock 8.0;
- подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0.

Пособие может использоваться в учебных учреждениях для обучения студентов по направлению УГСНП «Информационная безопасность», в целях рассмотрения теоретических аспектов и приобретения практических навыков настройки и эксплуатации СЗИ НСД Dallas Lock 8.0.

Для выполнения заданий потребуется следующее программное обеспечение:
1. Демонстрационная или коммерческая версия СЗИ НСД Dallas Lock 8.0 редакций «С» или «К».
2. Пакет офисных программ Open Office или MS Office.
3. Утилита Recuva или аналогичное ПО для восстановления удаленных файлов.

Для выполнения некоторых лабораторных работ потребуется развернуть локальную сеть в составе трех (или двух) автоматизированных рабочих мест (далее — АРМ) и USB-Flash накопитель.

1. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ

СЗИ НСД 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.

1.1 ОБЩЕЕ ОПИСАНИЕ

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 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 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 НСД Dallas Lock 8.0 состоит из следующих основных компонентов, рисунок 1:

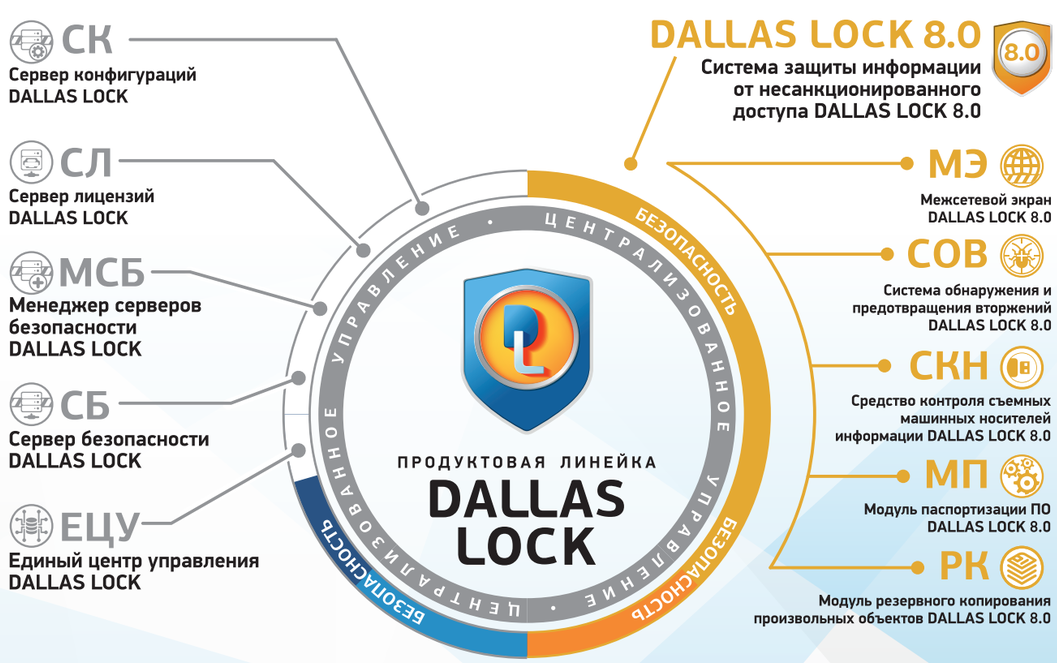

Рисунок 1. Структура и составные модули Dallas Lock

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 неактивированным. 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 НСД DALLAS LOCK 8.0

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 Lite SD, 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, ESMART Token ГОСТ, ESMART 64K;
- 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.

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 авторизо-

вать 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 ЭП при обновлении СЗИ Dallas Lock 8.0.

28. При использовании нескольких защищенных СЗИ Dallas Lock 8.0 и СЗИ 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 ком-

пьютер, 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 и контроля конфигурации сетевого оборудования) используется Единый центр управления Dallas Lock, который представляет 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 серверы 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.

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 ВОЗМОЖНОСТИ МЕЖСЕТЕВОГО ЭКРАНА DALLAS LOCK

МЭ является модулем СЗИ НСД 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.

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.
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». Для работы МЭ не требуется внесение изменений в структуру существующей сети.
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.
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 ДБ, 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.
Сбор информации о работе сети ведется на всех компьютерах системы, на которых установлен МЭ Dallas Lock.
Модуль МЭ позволяет обнаруживать атаки внутри виртуальной сети VipNet.

1.5 ВОЗМОЖНОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ DALLAS LOCK

СОВ Dallas Lock является модулем СЗИ Dallas Lock 8.0 и 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 том числе выключаясь при выключении МЭ). В случае неактивного модуля МЭ модуль СОВ работает независимо.
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, близком к реальному масштабу времени;
- для снижения трудоемкости и эффективной настройки СОВ возможно в упрощенном интерфейсе определить требуемые уровни защищенности системы без проведения индивидуальных и точных настроек;
- 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.

Модуль СОВ позволяет обнаруживать атаки внутри виртуальной сети VipNet.

1.6 ВОЗМОЖНОСТИ СИСТЕМЫ КОНТРОЛЯ НАКОПИТЕЛЕЙ DALLAS LOCK

В СЗИ Dallas Lock 8.0 в формате двух отдельных модулей реализована система контроля съемных машинных накопителей (СКН). Данные сертифицированные модули предназначены для контроля подключения съемных машинных носителей информации и контроля отчуждения (переноса) информации на такие носители.

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.
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 в рамках ДБ позволяет 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.**

1.7 ВОЗМОЖНОСТИ МОДУЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ DALLAS LOCK

Модуль резервного копирования (РК) СЗИ НСД Dallas Lock 8.0 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.

В ходе настройки механизмов РК 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.

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 задаются по следующей схеме: «*Имя клиента*_*Имя задания*_ДД.ММ.ГГГГ_ЧЧ.ММ.СС».

2. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

2.1 ЛАБОРАТОРНАЯ РАБОТА № 1. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА DALLAS LOCK 8.0

Цель работы
Ознакомление с методами защиты информации от несанкционированного доступа на примере СЗИ НСД Dallas Lock 8.0.

Исходные данные
Для ознакомления с методами защиты информации от несанкционированного доступа на примере СЗИ НСД Dallas Lock 8.0 потребуестя ПК АРМ1 с установленной СЗИ НСД и USB-Flash накопитель. Должны быть созданы в ОС учетные зиписи для пользователей: Авдейченко, Травин, Смирнов.
Для построения модели автоматизированной сети в защищенном исполнении рассматривается некое предприятие, ведущее разработку проектно-конструкторской документации по различным направлениям.
Несколько не связанных между собой групп инженеров ведут разработку самостоятельных проектов (Проект JET, Проект MicRo, Проект NaCW). Сами проекты являются конфиденциальными программами, а их документация – охраняемыми данными. Структура каталогов компьютерной системы предприятия представлена на рисунке 2.

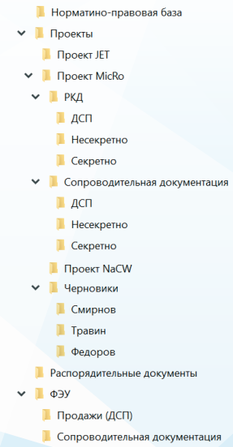

Рисунок 2. Структура каталогов

Документация предприятия представляет собой множество электронных документов, обрабатываемых в корпоративной информационно-вычислительной сети и имеющих различный уровень конфиденциальности: «Несекретно», «Для служебного пользования (ДСП)» и «Секретно».
К документации каждого из направлений имеют доступ конкретные сотрудники предприятия, которые имеют различные уровни допуска к информации.
Руководитель предприятия Авдейченко Ю. Б. имеет максимальный уровень допуска к информации и возможность работы с документацией любого проекта.
Экономист Кустова А. Н. работает над ресурсом «ФЭУ».
Администратор безопасности Гусев О. Л. имеет полный доступ к любым документам, имеет возможность управлять настройками компьютерной системы и реализует на практике политику безопасности предприятия в части информационных технологий.
В состав автоматизированной системы включена база данных нормативно-правовых документов. Администратор поддерживает в актуальном состоянии ресурс «Нормативно-правовая база». Руководитель предприятия издает приказы и указания и публикует их в каталоге «Распорядительные документы». Сотрудники предприятия могут беспрепятственно знакомиться с содержанием данных ресурсов, но вносить изменения в эти каталоги не могут.
В рамках лабораторной работы рассматриваются «Проект MicRo», ресурс «Нормативно-правовая база», каталоги «ФЭУ» и «Распорядительные документы» учетные записи сотрудников, имеющих уровни допуска к несекретной, ДСП и секретной информации согласно таблице 1.

Таблица 1. Уровни допуска сотрудников

Уровень допуска	Сотрудник
Несекретно	Смирнов Д. А.
ДСП	Травин О. Е., Кустова А. Н.
Секретно	Федоров Е. М., Авдейченко Ю. Б., Гусев О. Л.

В зависимости от своих функциональных обязанностей сотрудники могут осуществлять различные действия с документами: добавлять, редактировать, просматривать, удалять, копировать, распечатывать. Для предварительной проработки проектной документации инженеры могут создавать черновики документов. Черновики создаются в каталоге «Черновики» и предназначены для индивидуального пользования, они доступны только автору, администратору и руководителю предприятия.

Права доступа сотрудников к документации предприятия разрешенного уровня конфиденциальности отражены в матрице доступа, таблица 2. Буквой «П» обозначен тип доступа – **полный доступ**, «Ч» – **только чтение**, пробелом – **запрет доступа**.
Администратор и руководитель предприятия имеют допуск в систему в любой день недели с 7:00 до 23:00. Остальные сотрудники могут входить в систему только в рабочие дни с 8:30 до 17:30.

Таблица 2. Матрица доступа предприятия

Каталог	Смирнов	Травин	Федоров	Гусев	Кустова	Авдейченко
\Нормативно-правовая база	Ч	Ч	Ч	П	Ч	П
\Проекты\Проект MicRo\РКД\ДСП		П	П	П		П
\Проекты\Проект MicRo\РКД\Несекретно	П	П	П	П		П
\Проекты\Проект MicRo\Сопроводительная документация\ДСП		П	П	П		П
\Проекты\Проект MicRo\РКД\Секретно			П	П		П
\Проекты\Проект MicRo\Сопроводительная документация\Несекретно	П	П	П	П		П
\Проекты\Проект MicRo\Сопроводительная документация \Секретно			П	П		П
\Проекты\Проект MicRo\Черновики\Смирнов	П			П		П
\Проекты\Проект MicRo\Черновики\Травин		П		П		П
\Проекты\Проект MicRo\Черновики\Федоров			П	П		П
\Распорядительные документы	Ч	Ч	Ч	П	Ч	П
\ФЭУ				П	П	П

Порядок выполнения работы

1. Загрузить образ СЗИ НСД Dallas Lock 8.0 и зарегистрироваться в системе.

2. Создать учетные записи пользователей в СЗИ: Федоров, Кустова. Пароли выбрать произвольно.

3. Добавить пользователей из ОС в СЗИ: Авдейченко, Травин, Смирнов.

4. По очереди зарегистрироваться в системе каждым из пользователей.
Перед созданием новой учетной записи необходимо убедиться в том, что нужная учетная запись еще не создана в ОС. Если учетная запись создана в ОС, то достаточно будет ее просто зарегистрировать, выбрав из списка вызываемой кнопкой поиска (диалоговое окно «Создание учетной записи»).

Для создания нового пользователя в оболочке администратора СЗИ НСД Dallas Lock 8.0 необходимо:
- запустить оболочку администратора СЗИ НСД;
- выбрать вкладку «Учетные записи», на панели «Субъекты доступа» выбрать категорию «Учетные записи»;
- на панели «Действия» выбрать команду «Создать»;
- в открывшемся диалоговом окне в поле «Логин» указать логин (имя) учетной записи, рисунок 3.

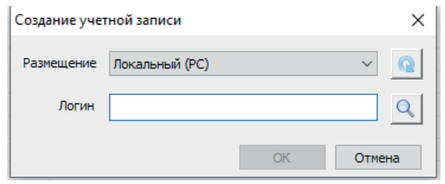

Рисунок 3. Окно создания учетной записи

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 в ОС: “ / \ [ ] : | < > + = ; , ? @ *);
- разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, т. е. заглавные и прописные буквы воспринимаются как одинаковые.

Кнопка поиска, расположенная рядом с полем «Логин», открывает список учетных записей, зарегистрированных в ОС данного ПК, и позволяет выбрать учетную запись из уже существующих.

- после ввода логина и нажатия «ОК» откроется диалоговое окно редактирования параметров учетной записи, рисунок 4.

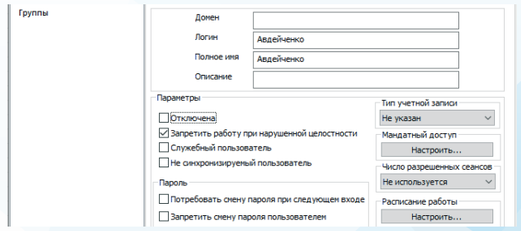

Рисунок 4. Окно редактирования параметров учетной записи

На вкладке «Общие» предлагается заполнить следующие параметры:

- «Полное имя» пользователя;
- «Описание» – любой комментарий. Длина комментария не более 256 символов;
- «Логин» и «Домен» недоступны для редактирования (название домена для локального пользователя остается пустым);
- политики «Отключена» и «Запретить работу при нарушенной целостности» задаются при необходимости.

Администратор имеет возможность отключать учетную запись любого пользователя, после чего пользователь не сможет авторизоваться в ОС до тех пор, пока администратор не деактивирует эту опцию.

Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «Запретить работу при нарушенной целостности» включена, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется. Если эта опция отключена, то при обнаружении нарушения целостности будет отображено только предупреждение;

- «Служебный пользователь». Установленный флаг для данного параметра означает, что для учетной записи не будут действовать ограничения на вход с различными уровнями или метками мандатного доступа;
- «Тип учетной записи». Для типа «Временный» обязательным условием является настройка расписания работы пользователя. По умолчанию будет установлено значение «Не указан»;
- «Уровень мандатного доступа» (**только для Dallas Lock 8.0 редакции «С»**). Уровень мандатного доступа, под которым пользователь сможет работать;
- «Число разрешенных сеансов». По умолчанию выставлено значение «Не используется». При установленном значении для каждой учетной записи будет проверяться количество одновременных интерактивных и сетевых сессий;
- «Расписание работы». Настройка периода и времени работы пользователя. Вне указанного периода пользователь не сможет зайти на защищаемый ПК. По окончании времени работы АРМ пользователя будет заблокирован при условии включения параметра безопасности «Принудительное завершение работы по расписанию» (вкладка «Параметры безопасности», категория «Права пользователей»);
- «Потребовать смену пароля при следующем входе». При установленном флаге единовременно будет выполнен запрос на смену пароля при входе;
- «Запретить смену пароля пользователем». Запрет для пользователя на смену своего пароля, в т. ч. и по истечении срока действия;

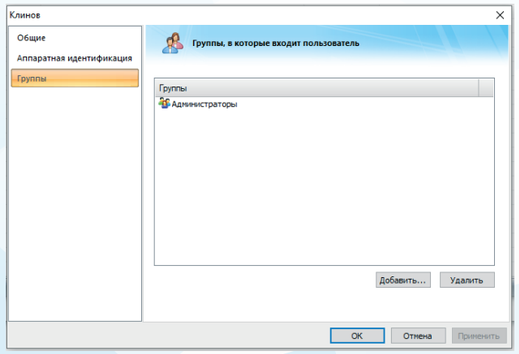

Рисунок 5. Окно редактирования списка групп учетной записи

- «Пароль без ограничения срока действия». Отменяет действие глобальной политики входа «Максимальный срок действия паролей» (вкладка «Параметры безопасности», категория «Вход»), распространяемой на всех пользователей.
- в процессе регистрации учетной записи администратор имеет возможность включать ее в определенную группу. В окне создания учетной записи необходимо перейти в раздел «Группы». В разделе отображены названия групп, в которые включен пользователь, рисунок 5. По умолчанию каждый новый пользователь входит в группу «Пользователи».

Группы предназначены для объединения пользователей, у которых права безопасности могут быть схожими.
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 СЗИ необходимо выбрать категорию «Группы» на вкладке «Учетные записи». В окне СЗИ Dallas Lock 8.0 автоматически появится ряд предварительно сконфигурированных групп в локальной ОС Windows, в которые можно включать пользователей. Вновь созданные с помощью СЗИ НСД Dallas Lock 8.0 группы автоматически создаются и на локальном ПК. Удаленные локальные группы удаляются и из ОС на локальном ПК. Категория «Группы» представлена на рисунке 6.

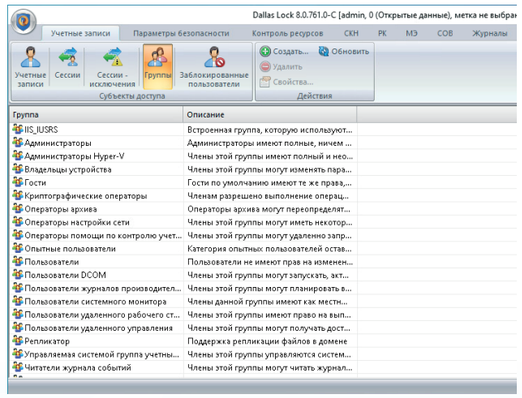

Рисунок 6. Общий вид категории «Группы»

Для создания новой группы необходимо:

- на вкладке «Учетные записи» перейти в категорию «Группы». На панели «Действия» выбрать команду «Создать...»;
- в открывшемся диалоговом окне заполнить поле «Группа» (название группы) и поле «Описание» (назначение группы или комментарий при необходимости), рисунок 7.

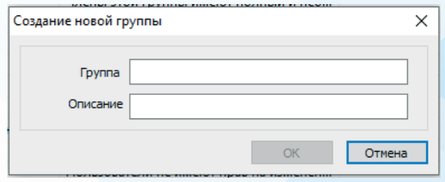

Рисунок 7. Создание новой группы

5. Разрешить полный доступ к USB-Flash дискам пользователям: Авдейченко, Гусев. Разрешить доступ «только чтение» к USB-Flash дискам пользователям: Федоров, Травин. Для всех остальных пользователей – запретить.

6. Запретить доступ к CD-ROM (при наличии дисковода) всем пользователям, кроме Авдейченко и Гусева.

7. Зарегистрироваться и проверить доступ к USB-Flash диску пользователями: Авдейченко, Федоров, Кустова.

8. Зарегистрироваться и проверить доступ к CD-ROM (при наличии дисковода) пользователями: Авдейченко, Кустова.

Чтобы установить дискреционный доступ к USB-Flash дискам, необходимо перейти на вкладку «Контроль ресурсов», на панели «Выбор по типу ресурса» выбрать категорию «Устройства». В списке параметров найти раздел «Сменные накопители» и открыть свойства «USB-Flash диски». Открыть свойства параметра, перейти в раздел «Дискреционный доступ», рисунок 8.

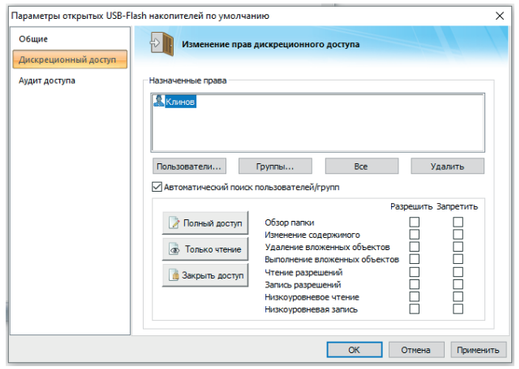

Рисунок 8. Назначение прав дискреционного доступа

Чтобы назначить определенные дискреционные права для пользователей, необходимо:
- 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;
- для каждой учетной записи, пользователя или группы в списке необходимо задать набор разрешений/запрещений, который будет определять права по доступу к данному объекту файловой системы, рисунок 9;

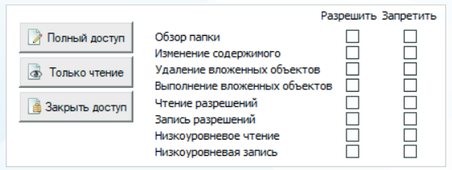

Рисунок 9. Список прав дискреционного доступа

- далее нажать «Применить» и «ОК».

9. Создать каталоги и разграничить права доступа пользователей к ним в соответствии с таблицей 2.

10. Зарегистрироваться пользователем Кустова и просмотреть содержимое каталога «С:\ФЭУ». Убедиться, что вложенные в «С:\Проекты» каталоги для этого пользователя недоступны.

11. Зарегистрироваться пользователем Федоров и просмотреть содержимое каталога «С:\Проекты\Проект MicRo\Сопроводительная документация\Секретно». Убедиться, что каталог «С:\ФЭУ» недоступен.

12. Создать в каталоге «С:\Распорядительные документы» пользователем Авдейченко короткий текстовый файл «Приказ об увольнении.txt» с приказом об увольнении Травина.

13. Убедиться, что Травин сможет прочитать приказ о своем увольнении, но не сможет изменить его.
Для того чтобы назначить дискреционный доступ для конкретного объекта ФС, необходимо выполнить следующее:
- открыть его дескриптор безопасности, используя оболочку администратора СЗИ НСД Dallas Lock 8.0 или через контекстное меню объекта (для объектов ФС):
  - открыть дескриптор с помощью контекстного меню значка объекта ФС можно, выбрав пункт меню «DL8.0: Права доступа», рисунок 10;

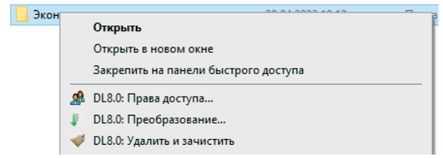

Рисунок 10. Контекстное меню

  - открыть дескриптор безопасности объекта ФС через оболочку администратора Dallas Lock 8.0. Открыть вкладку «Контроль ресурсов». На панели «Выбор по типу ресурса» выбрать категорию «ФС». На панели «Фильтр по типу контроля» выбрать «Дискреционный доступ». На панели «Действия» выбрать команду «Добавить (ФС)...». В появившемся окне проводника, как в проводнике Windows, необходимо найти нужный объект ФС и нажать кнопку «Выбрать». Для выбранного объекта откроется окно дескриптора.
- в окне дескриптора безопасности необходимо выбрать раздел «Дискреционный доступ».

В соответствии с дискреционным принципом доступа каждому ресурсу файловой системы может быть сопоставлен список пользователей и/или групп пользователей. Каждому пользователю (группе) из списка можно разрешить или запретить определенную операцию с данным ресурсом;
- чтобы назначить определенные дискреционные права для определенных пользователей, необходимо при помощи кнопок «Пользователь», «Группы», «Все», «Удалить» выбрать определенные учетные записи пользователей или групп;
- для выбранных пользователей/групп необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту, рисунок 9.

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.

14. Для пользователя Кустова создать группу «Фин_управление» и организовать ЗПС. Разрешить запуск следующих программ:
- Калькулятор;
- Блокнот;
- WordPad.

15. Зарегистрироваться пользователем Кустова и проверить запуск программ:
- Калькулятор;
- WordPad;
- Outlook;
- Microsoft Edge.

Для настройки ЗПС с использованием режима обучения в системе защиты Dallas Lock 8.0 существует дополнительный механизм «Права для файлов». Пусть пользователь, для которого нужно организовать ЗПС, уже создан и инициализирован (к примеру, он называется zps[1]). Далее для настройки ЗПС необходимо выполнить следующие шаги по настройке:
- создать специальную группу, например, ZPS-gr[2], и включить пользователя zps в группу ZPS-gr;
- осуществить вход в ОС под учетной записью пользователя zps до включения режима обучения;
- войти под учетной записью администратора безопасности. Для группы ZPS-gr в глобальных настройках запретить выполнение вложенных объектов (вкладка «Контроль ресурсов», выбор по типу ресурса «Глобальные», «Параметры ФС по умолчанию»), рисунок 11;

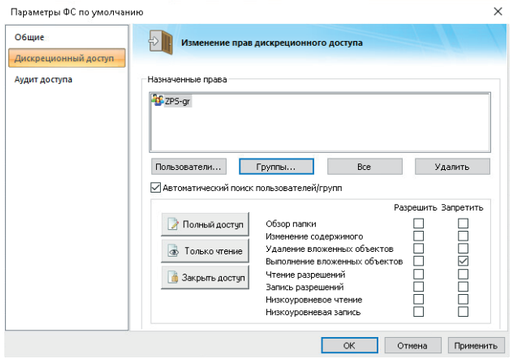

Рисунок 11. Глобальный запрет запуска программ для настройки ЗПС

- включить режим обучения СЗИ НСД (пункт меню кнопки основного меню «Настройка режимов работы», «Включить режим обучения»);
- нажать «Да» в окне подтверждения, рисунок 12;

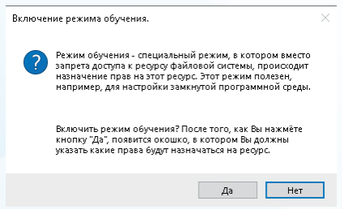

Рисунок 12. Подтверждение включения режима обучения

- в появившемся окне редактирования дескриптора безопасности назначить дискреционные права для груп ZPS-gr «Только чтение» и нажать «ОК», рисунок 13;

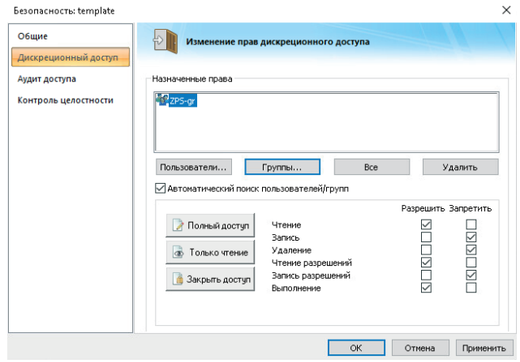

Рисунок 13. Фильтр журнала доступа к ресурсам

- нажать «ОК» в появившемся информационном окне, рисунок 14;

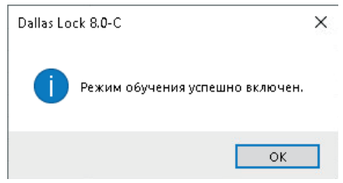

Рисунок 14. Информационное окно о включении режима обучения

- перезагрузить ПК АРМ1;
- осуществить вход в ОС под учетной записью пользователя zps. Запустить все приложения, с которыми пользователь имеет право работать (но не запускать ничего лишнего);
- осуществить смену пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора СЗИ НСД, пункт меню кнопки основного меню «Настройка режимов работы», «Выключить режим обучения»);
- далее нажать «ОК» в информационном окне, рисунок 15.

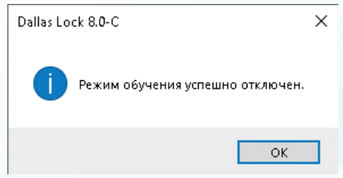

Рисунок 15. Информационное окно об отключении режима обучения

Таким образом замкнутая программная среда организована. Теперь необходимо зайти пользователем, входящим в группу ZPS-gr. Этот пользователь сможет работать только с необходимыми программами.

1. Для самостоятельного выполнения настройка ЗПС выполняется для учетной записи «Кустова».
2. Для самостоятельного выполнения настройка ЗПС выполняется для группы «Фин_управление».

16. Создать группу пользователей «Инженеры» и включить Травина, Федорова и Смирнова. Для группы организовать ЗПС. Разрешить запуск следующих программ:
- MS Excel или OpenOffice Calc;
- MS Word или OpenOffice Writer;
- Paint.

17. Зарегистрироваться одним из пользователей группы «Инженеры» и проверить запуск программ:
- MS Word или OpenOffice Writer;
- MS PowerPoint или OpenOffice Impress;
- Microsoft Edge;
- Paint.

18. Зарегистрироваться администратором, создать в каталоге «C:\Нормативно-правовая база» короткий текстовый файл «БД.txt». Настроить контроль целостности этого файла с использованием алгоритма ГОСТ Р 34.11-94.

19. Перезагрузить компьютер, зарегистрироваться администратором и изменить содержимое файла «БД.txt». Снова перезагрузить компьютер и попытаться зарегистрироваться пользователем Федоров. Возможно ли это? Перезагрузить компьютер, после чего зарегистрироваться администратором и отключить контроль целостности файла «БД.txt».

Для настройки контроля целостности необходимо в оболочке администратора на вкладке «Параметры безопасности» выделить категорию «Контроль целостности». В окне автоматически откроются параметры контроля целостности, рисунок 16.

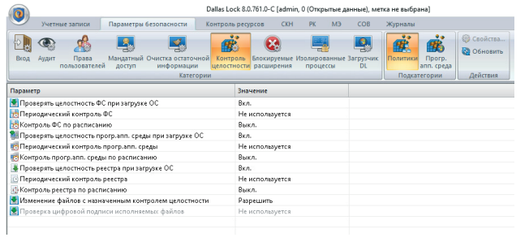

Рисунок 16. Категория «Контроль целостности»

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, рисунок 17.

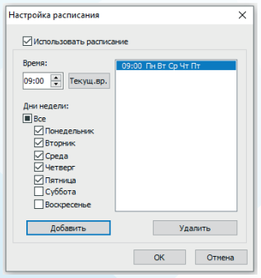

Рисунок 17. Настройка расписания контроля целостности

В окне настройки расписания необходимо включить контроль (поставить флажок в поле «Контроль по расписанию включен») и установить расписание. Каждое событие 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.

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 НСД или вызвав контекстное меню файла щелчком по его значку. Объекты файловой системы, на которые назначен контроль целостности любым из способов, автоматически появляются в списке объектов в окне категории «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.

Для того чтобы установить целостность для конкретного объекта ФС, необходимо выполнить следующее:
- открыть дескриптор безопасности объекта, используя оболочку администратора Dallas Lock 8.0. Вкладка «Контроль ресурсов», тип ресурса «ФС», фильтр по типу контроля «Контроль целостности», команда «Добавить (ФС)» на панели «Действия» или через контекстное меню объекта (пункт «Права доступа» для объекта ФС), рисунок 18;

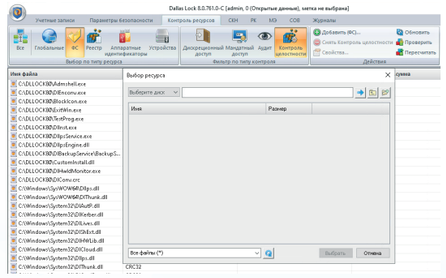

Рисунок 18. Назначение контроля целостности на объект ФС

- в отобразившемся окне дескриптора безопасности объекта необходимо открыть закладку «Контроль целостности», рисунок 19;

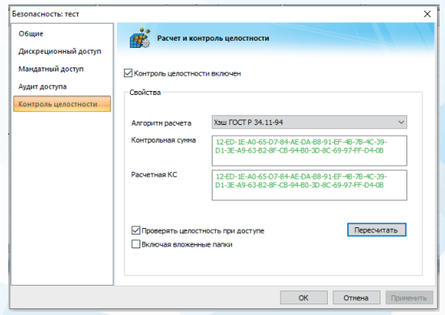

Рисунок 19. Контроль целостности ресурса ФС

- необходимо отметить флажком поле «Контроль целостности включен», выбрать алгоритм расчета контрольной суммы (CRC32, Хэш ГОСТ Р 34.11-94, Хэш MD5) и нажать «Пересчитать»;
- 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 у учетной записи включен параметр «Блокировать при нарушении 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;
  - 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.
- нажать «Применить» и «ОК».

Если некоторый объект файловой системы 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, рисунок 20.

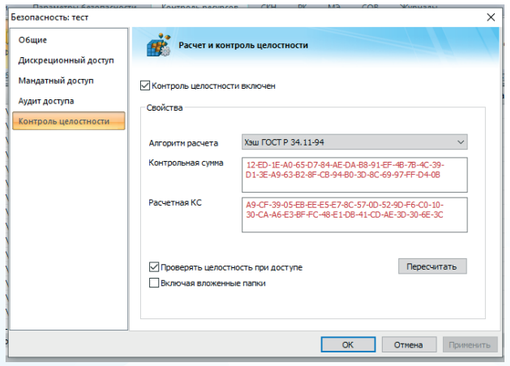

Рисунок 20. Нарушение контроля целостности

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.

При проверке целостности по команде администратора (действие «Проверить» в оболочке администратора) в списке объектов категории «Контроль целостности» значок объекта, у которого нарушена целостность, будет выделен символом ⊗.

Значения контрольных сумм для контролируемых объектов в оболочке администратора появляются после команд проверки и пересчета контрольных сумм.

Содержание отчета
Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения: описание и назначение СЗИ НСД Dallas Lock 8.0, разграничение доступа к объектам файловой системы, замкнутая программная среда, подсистема обеспечения целостности, журналирование событий информационной безопасности.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности по следующим параметрам:
- идентификация и аутентификация пользователей (путем создания учетных записей и назначения им паролей);
- разграничение доступа, реализация дискреционной модели, а также принцип замкнутой программной среды;
- контроль целостности, включая подсистемы контроля целостности для защиты конфиденциальных данных от несанкционированной модификации;
- регистрация событий, политика аудита для выявления наиболее опасных действий нарушителя.

4. Ответы на контрольные вопросы.

Контрольные вопросы
1. Какие возможности по разграничению доступа реализует СЗИ НСД Dallas Lock 8.0?
2. Охарактеризуйте подсистему централизованного управления.
3. Какие категории событий отражаются в журнале регистрации событий СЗИ НСД Dallas Lock 8.0?
4. Что такое дескриптор объекта?
5. Что такое дескриптор по пути?
6. Опишите способы настройки ЗПС.
7. Укажите категории средств обеспечения информационной безопасности, которые, помимо СЗИ НСД Dallas Lock 8.0, должны функционировать в комплексе средств защиты информации.

2.2 ЛАБОРАТОРНАЯ РАБОТА № 2.

НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ПЕРСОНАЛЬНОГО МЕЖСЕТЕВОГО ЭКРАНА СЗИ НСД DALLAS LOCK 8.0

Цель работы
Ознакомление с функциональными возможностями и особенностями конфигурирования межсетевых экранов и фильтров на примере модуля МЭ СЗИ НСД Dallas Lock 8.0.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования МЭ СЗИ НСД Dallas Lock 8.0 потребуются 2 ПК, взаимодействующих в одной подсети: АРМ1, имеющий доступ к интернету, с установленной СЗИ НСД (с межсетевым экраном) и АРМ2.
Необходимо выполнить настройку правил МЭ на запрет запуска страницы http://www.yandex.ru на ПК АРМ1 и на запрет любых направлений передачи по протоколу Ethernet для ПК АРМ2.
Выполнить настройку правил фильтрации на примере параметра «Анализ SSL трафика».

Порядок выполнения работ
1. Включить ПК АРМ1 и ПК АРМ2.

2. Проверить через командную строку для ПК АРМ1 и ПК АРМ2 значение IP-адресов. На ПК АРМ2 через командную строку выполнить команду «ping» в отношении ПК АРМ1. Убедиться, что все пакеты прошли и присутствует запись «0% потерь».

3. Запустить оболочку администратора СЗИ НСД Dallas Lock 8.0 на ПК АРМ1.

4. Выполнить настройку правила МЭ на запрет запуска страницы http://www.yandex.ru:
- для настройки правила необходимо на вкладке «МЭ» перейти в категорию «Правила МЭ» и ознакомиться с набором предустановленных правил, рисунок 21;

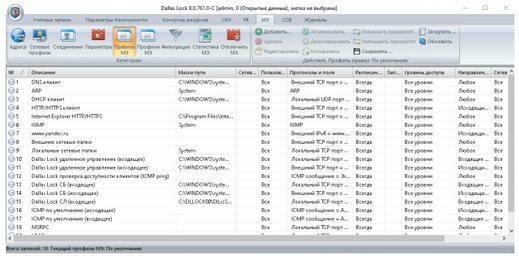

Рисунок 21. Набор предустановленных правил межсетевого экрана

- открыть свойства правила №7 «www.yandex.ru». Выбрать тип действия «Запретить» и активировать правило, рисунок 22;
- выполнить проверку. Открыть любой интернет-браузер и перейти на страницу http://www.yandex.ru. Страница http://www.yandex.ru должна быть недоступна.

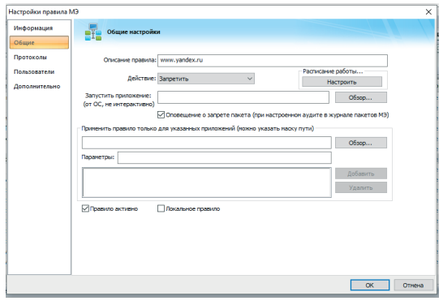

Рисунок 22. Редактирование правила

5. Открыть оболочку администратора СЗИ НСД Dallas Lock 8.0.

6. Создать запрещающие правило на любое направление передачи по протоколу Ethernet для ПК АРМ2:
- добавить новое правило;
- задать произвольное описание правила;
- выбрать тип действия «Запретить» и активировать правило;
- в разделе «Протоколы» из выпадающего списка «Список протоколов» выбрать «Ethernet», нажать кнопку «Добавить»;
- отметить пункт «Внешний MAC» и ввести в поле «MAC в формате...» значение физического адреса ПК АРМ2, полученное при выполнении шага 2, рисунок 23;

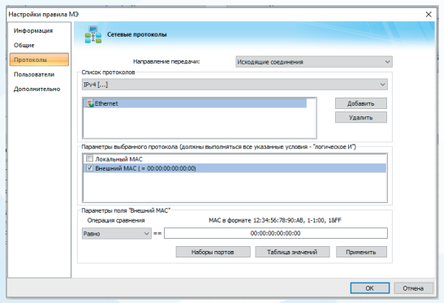

Рисунок 23. Настройка раздела «Протоколы»

- перейти в раздел «Пользователи», нажать кнопку «Все»;
- нажать кнопку «ОК» для применения и создания правила;
- перейти в категорию «Параметры». Отключить параметр «Доверенные правила МЭ»;
- выполнить проверку. На ПК АРМ2 через командную строку выполнить команду «ping» в отношении ПК АРМ1. В командной строке должна появиться запись «100% потерь».

7. В оболочке администратора СЗИ НСД Dallas Lock 8.0 на вкладке «МЭ» перейти в категорию «Фильтрация» и включить параметр «Анализ SSL трафика».

8. На панели «Параметры фильтрации» выбрать категорию «Фильтры». Ознакомиться со списком предустановленных фильтров.

9. Открыть свойства параметра «JScript» и выполнить блокировку данного фильтра, рисунок 24.

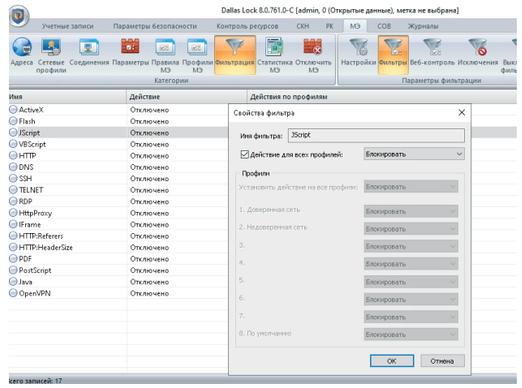

Рисунок 24. Блокировка фильтра

10. Выполнить проверку. Используя любой интернет-браузер, перейти на страницу, содержащую JavaScript, например www.rbc.ru. Если настройка была выполнена правильно, то страница не откроется.

Содержание отчета

Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения — межсетевой экран СЗИ НСД Dallas Lock 8.0.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности:
- настройка правила МЭ на запрет запуска страницы http://www.yandex.ru на ПК АРМ1;
- настройка правила на запрет любых направлений передачи по протоколу Ethernet для ПК АРМ2;
- настройка правил фильтрации на примере параметра «Анализ SSL трафика».

4. Ответы на контрольные вопросы.

Контрольные вопросы

1. Назначение межсетевого экрана СЗИ НСД Dallas Lock 8.0.
2. Посредством чего осуществляется работа МЭ?
3. Что такое правила межсетевого экрана?
4. Как выполняется создание правила МЭ в оболочке администратора СЗИ НСД Dallas Lock 8.0?
5. Какое действие применяется к пакетам, не попавшим ни под одно правило МЭ?
6. Какая функциональная возможность МЭ позволяет выполнять контроль сетевого трафика по его содержимому?

2.3 ЛАБОРАТОРНАЯ РАБОТА № 3.

НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ СЗИ НСД DALLAS LOCK 8.0

Цель работы
Ознакомление с функциональными возможностями и особенностями конфигурирования системы обнаружения вторжений на примере модуля СОВ СЗИ НСД Dallas Lock 8.0.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования СОВ СЗИ НСД Dallas Lock 8.0 потребуются 2 ПК, взаимодействующих в одной подсети: АРМ1 с установленной СЗИ НСД (с модулем СОВ) и АРМ2. Создана учетная запись СЗИ Смирнов.
Необходимо выполнить настройку запрещающего правила контроля приложений для приложения «Блокнот».
Выполнить проверку функциональной возможности «Безопасная среда».

Порядок выполнения работ

1. Включить ПК АРМ1.

2. Запустить оболочку администратора СЗИ НСД Dallas Lock 8.0.

3. Перейти на вкладку «СОВ», выбрать категорию «Параметры СОВ».

4. Выполнить настройку запрещающего правила контроля приложений для программы «Блокнот»:
- на панели «Параметры СОВ» выбрать команду «Контроль приложений». На панели «Действия» нажать кнопку «Добавить...»;
- в открывшемся окне, рисунок 25, указать название правила;

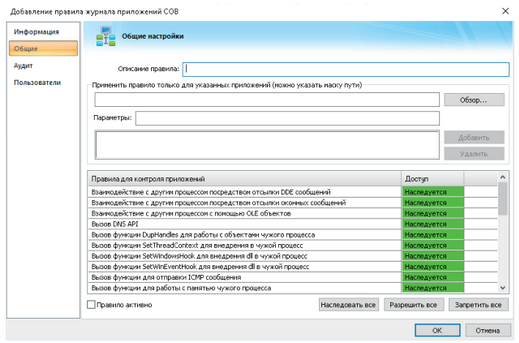

Рисунок 25. Добавление правила контроля приложений

- в поле «Применить правило только для указанных приложений» ввести путь к расположению notepad.exe и нажать кнопку «Добавить»;
- в разделе «Правила для контроля приложений» для правила «Изменение файла HOSTS» выставить значение «Запрещено» (выбрать из выпадающего списка в поле «Доступ»);
- активировать правило (выставить флаг «Правило активно»), сохранить изменения.

5. Выполнить проверку:
- авторизоваться в ОС под учетной записью Смирнов;
- открыть через приложение «Блокнот» файл C:\Windows\System32\drivers\etc\hosts;
- внести любые изменения и сохранить правки.

6. Включить ПК АРМ2, авторизоваться с правами администратора.

7. На ПК АРМ1 в оболочке администратора СЗИ НСД Dallas Lock 8.0 открыть вкладку «СОВ», выбрать категорию «Безопасная среда СОВ», на панели «Безопасная среда СОВ» выбрать «Контроль приложений», на панели «Действия» нажать кнопку «Добавить».

8. Заполнить поле «Описание правила», для правила «Вызов функции для отправки ICMP сообщения» установить значение доступа «Запрещено», сохранить изменения, рисунок 26.

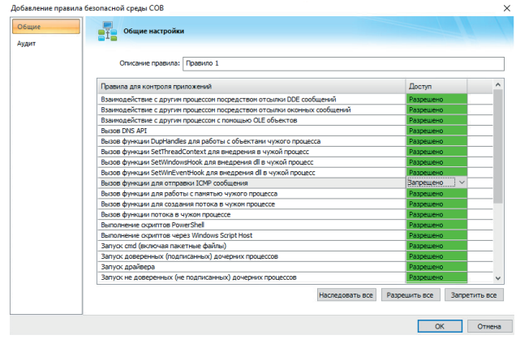

Рисунок 26. Добавление правила безопасной среды СОВ

9. На панели «Безопасная среда СОВ» выбрать «Настройки»:
- для параметра «Эвристический анализ для блокировки работы опасных процессов» установить значение «Режим с настройками по умолчанию»;
- для параметра «Отчет по завершении работы процесса в БС» установить значение «Вкл.», рисунок 27.

Рисунок 27. Настройки «Безопасной среды» СОВ

10. Выполнить проверку:
- открыть в проводнике папку «C:\Windows\System32», открыть контекстное меню файла «cmd.exe», выбрать команду в контекстном меню «DL8.0: Запустить в Безопасной среде...»;
- в поле «Правило» выбрать правило, созданное ранее, нажать «ОК»;
- выполнить команду: «ping <IP-адрес_ПК_АРМ2>»;
- закрыть окно командной строки;
- открыть отчет безопасной среды (по умолчанию каталог на рабочем столе пользователя «Отчеты БС Dallas Lock»);
- в отчете безопасной среды в таблице «Вызов функции для отправки ICMP сообщения» в строке «Информация:» должно быть значение «IP-адрес_ПК_АРМ2, 1 вызов».

Содержание отчета
Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения — система обнаружения вторжений СЗИ НСД Dallas Lock 8.0.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности:
- настройки запрещающего правила контроля приложений для приложения «Блокнот»;
- настройки механизма «Безопасная среда».

4. Ответы на контрольные вопросы.

Контрольные вопросы
1. Назначение системы обнаружения вторжений СЗИ НСД Dallas Lock 8.0.
2. Какие типы событий отслеживает СОВ в рамках обнаружения аномалий в поведении приложений и ОС?
3. При выполнении контроля приложений, если приложение не было найдено в пользовательских правилах, где в дальнейшем СОВ проверяет доступ для данного приложения?
4. За что отвечают глобальные параметры настройки эвристики «Уровень блокировки» и «Уровень журналирования», применимые к сигнатурам трафика и правилам контроля приложений?
5. Перечислите дополнительные настройки эвристики.
6. Что такое «Безопасная среда СОВ»?

2.4 ЛАБОРАТОРНАЯ РАБОТА № 4.

НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ КОНТРОЛЯ НАКОПИТЕЛЕЙ СЗИ НСД DALLAS LOCK 8.0

Цель работы
Ознакомление с функциональными возможностями и особенностями конфигурирования системы контроля накопителей (СКН) СЗИ НСД Dallas Lock 8.0.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования модуля СКН СЗИ НСД Dallas Lock 8.0 потребуются 3 ПК: АРМ1 и АРМ2 с установленной СЗИ НСД (с модулем СКН) и АРМ3 без СЗИ НСД Dallas Lock 8.0, сменный накопитель. В СЗИ НСД должна быть зарегистрирована учетная запись пользователя User.
Выполнить проверку функциональной возможности преобразования сменных накопителей.
Выполнить проверку функциональной возможности разграничения доступа пользователей к сменным накопителям информации.

Порядок выполнения работ
1. Включить ПК АРМ1.

2. Открыть оболочку администратора СЗИ НСД Dallas Lock 8.0.

3. Выполнить преобразование сменного накопителя:
- перейти на вкладку «СКН», выбрать категорию «Преобразование сменных накопителей», рисунок 28;

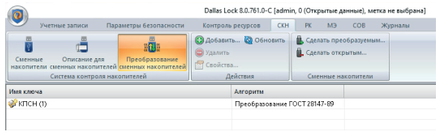

Рисунок 28. Преобразование сменных накопителей

- на панели «Действия» нажать кнопку «Добавить»;
- в окне создания ключа преобразования сменных накопителей (рисунок 29) задать алгоритм ГОСТ 28147-89) и пароль для преобразования, имя ключа «КПСН (1)», нажать «ОК»;

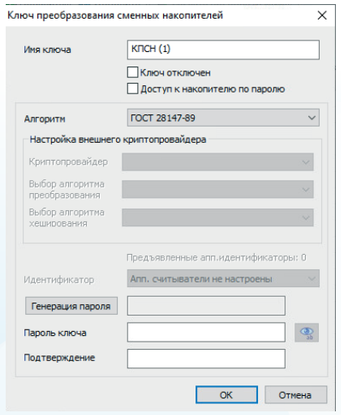

Рисунок 29. Создание ключа

- подключить сменный накопитель к USB-порту ПК АРМ1;
- в оболочке администратора СЗИ НСД Dallas Lock 8.0 на вкладке «СКН» в категории «Преобразование сменных накопителей» на панели «Сменные накопители» выбрать команду «Сделать преобразуемым...»;
- выбрать подключенный накопитель в списке «Сменный накопитель» и КПСН (1) в списке «Ключ преобразования». Нажать кнопку «Выполнить» и дождаться окончания процесса преобразования, рисунок 30.

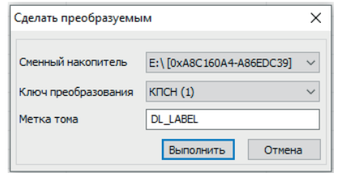

Рисунок 30. Выбор ключа преобразования

4. Выполнить проверку:
- сохранить на сменный накопитель любой файл;
- отключить сменный накопитель от ПК АРМ1 и подключить сменный накопитель к USB-порту ПК АРМ2;
- убедиться, что невозможно получить доступ к данным на накопителе, так как на ПК АРМ2 отсутствует ключ КПСН (1). Появится сообщение о том, что работа с данным накопителем возможна только после его форматирования в ОС;
- отключить сменный накопитель от ПК АРМ2 и подключить сменный накопитель к USB-порту ПК АРМ3;
- убедиться, что невозможно получить доступ к данным на накопителе, так как на ПК АРМ3 не установлена СЗИ НСД. Появится сообщение о том, что работа с данным накопителем возможна только после его форматирования в ОС.

5. Выполнить обратное преобразование сменного накопителя:
- открыть консоль администратора СЗИ НСД;
- на вкладке «СКН» в категории «Преобразование сменных накопителей» на панели «Сменные накопители» выбрать команду «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.

6. Выполнить преобразование сменного накопителя:
- выполняется по аналогии с п.3 данной лабораторной работы;
- при вводе параметров ключа преобразования установить в верхней части окна галочку «Доступ к накопителю по паролю».

7. Выполнить проверку:
- отключить и подключить накопитель;
- в появившемся диалоговом окне «Доступ к накопителям» ввести заданный ранее пароль;
- создать и удалить на накопителе текстовый файл;
- отключить и подключить накопитель;
- в появившемся диалоговом окне «Доступ к накопителям» ввести неверный пароль;
- убедиться, что доступ к накопителю не предоставлен.

8. В оболочке администратора СЗИ НСД Dallas Lock 8.0 перейти на вкладку «Параметры безопасности».

9. В категории «Вход» в общем списке параметров открыть свойства параметра «Блокировать подключение незарегистрированных накопителей USB Flash», установить значение «Да».

10. Выполнить проверку:
- завершить сеанс учетной записи администратора;
- авторизоваться в ОС под учетной записью User;
- подключить к ПК незарегистрированный USB-Flash накопитель;
- проверить возможность доступа к подключенному USB-Flash накопителю.

Содержание отчета
Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности:
- преобразования сменных накопителей;
- настройки прав получения доступа к съемному машинному носителю информации.

4. Ответы на контрольные вопросы.

Контрольные вопросы
1. Назначение системы контроля носителей СЗИ НСД Dallas Lock 8.0.
2. Для каких типов сменных накопителей доступно преобразование?
3. Какие алгоритмы преобразования можно выбрать при создании ключа преобразования?
4. Допускается ли использование действующего аппаратного идентификатора в качестве ключа преобразования USB-Flash накопителя?
5. На каких компьютерах можно использовать преобразованный сменный накопитель?
6. Как выполняется обратное преобразование сменного накопителя?
7. После обратного преобразования сменного накопителя, будут ли распространяться какие-либо ограничения на данное устройство при использовании на компьютерах?
8. Регистрируется ли в реестре информация о подключении накопителя при включенном параметре «Блокировать подключение незарегистрированных накопителей USB Flash»?

2.5 ЛАБОРАТОРНАЯ РАБОТА № 5.

НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ МОДУЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ СЗИ НСД DALLAS LOCK 8.0

Цель работы
Ознакомление с функциональными возможностями и особенностями конфигурирования модуля резервного копирования (РК) СЗИ НСД Dallas Lock 8.0.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования модуля РК СЗИ НСД Dallas Lock 8.0 потребуется ПК АРМ1 с установленной СЗИ НСД (с модулем РК). Должна быть создана учетная запись «Кузнецов», имеющая доступ к сетевому ресурсу.
Выполнить проверку функциональной возможности автоматизированного создания резервных копий произвольных объектов файловой системы.
Выполнить проверку функциональной возможности сохранения файла резервной копии.

Порядок выполнения работ

1. Включить ПК АРМ1.

2. Открыть оболочку администратора СЗИ НСД Dallas Lock 8.0.

3. Создать задание на выполнение резервного копирования объектов ФС:
- открыть вкладку «РК»;
- на панели «Действия» выбрать команду «Создать»;
- в открывшемся диалоговом окне «Мастер создания задания» установить флаг «Активировать расписание запуска», рисунок 31;

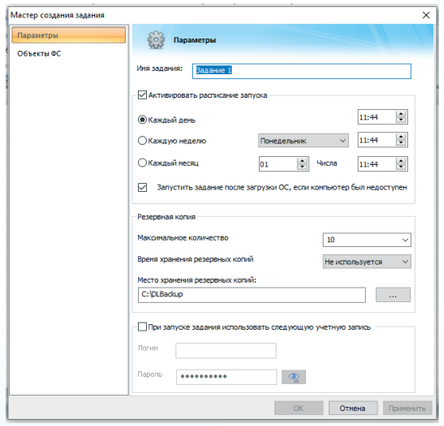

Рисунок 31. Мастер создания задания

- установить периодичность создания резервных копий;
- указать максимальное количество резервных копий;
- в разделе «Объекты ФС» Мастера создания задания выбрать объекты ФС, для которых будет выполняться копирование. Сохранить изменения.

4. Выполнить проверку:
- в соответствии с установленным расписанием должна быть создана резервная копия объекта ФС;
- из списка заданий выбрать и открыть созданное задание, перейти в раздел «Резервные копии», выбрать последнюю созданную копию;
- выполнить восстановление объекта ФС.

5. В оболочке администратора СЗИ НСД перейти на вкладку «РК», на панели «Действия» выбрать команду «Создать».

6. В окне Мастера создания задания убрать флаг «Активировать расписание запуска» и выбрать сетевую директорию для хранения резервных копий.

7. Установить флаг «При запуске задания использовать следующую учетную запись» и ввести учетные данные пользователя «Кузнецов».

8. Перейти на вкладку «Объекты ФС» и выбрать объект ФС, для которого будет создаваться резервная копия. Сохранить изменения.

9. Выполнить задание на резервное копирование.

10. Задание считается успешно выполненным, если после п.9 в указанном сетевом каталоге успешно была создана резервная копия указанного объекта ФС.

Содержание отчета
Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения — назначение и общие принципы работы модуля резервного копирования.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности:
- автоматизированного создания резервных копий произвольных объектов файловой системы;
- сохранения файла резервной копии.

4. Ответы на контрольные вопросы.

Контрольные вопросы
1. Назначение модуля резервного копирования СЗИ НСД Dallas Lock 8.0.
2. Сколько одновременно может выполняться заданий?
3. Если клиентский компьютер включен в Домен безопасности, будут ли доступны для него функции создания, копирования, удаления и деактивации заданий?
4. За что отвечает параметр «Активировать расписание запуска» в Мастере создания задания?
5. Можно ли выполнить восстановление данных из резервной копии во время выполнения задания?

2.6 ЛАБОРАТОРНАЯ РАБОТА № 6.

НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ПОДСИСТЕМЫ ОЧИСТКИ ОСТАТОЧНОЙ ИНФОРМАЦИИ СЗИ НСД DALLAS LOCK 8.0

Цель работы
Ознакомление с функциональными возможностями и особенностями подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0. Получение навыков настройки средств гарантированной очистки удаленной информации.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0 потребуются: ПК АРМ1 с установленной СЗИ НСД, USB-Flash накопитель, утилита Recuva.
Для достижения целей лабораторной работы необходимо рассмотреть рабочее место в отделе кадров некоторой организации. Файлы с конфиденциальной информацией находятся на жестком диске компьютера. Файлы и содержание файлов на жестком диске представлены в таблице 3.

Таблица 3. Структура каталогов отдела кадров

№	Полный путь к файлу	Содержание файла
1	Данные сотрудников\Авдейченко.txt	Персональные данные сотрудника: Авдейченко
2	Данные сотрудников\Смирнов.txt	Персональные данные сотрудника: Смирнов
3	Данные сотрудников\Травин.txt	Персональные данные сотрудника: Травин

Порядок выполнения работ

1. Включить ПК АРМ1.
2. Зарегистрироваться администратором и скопировать на USB-Flash накопитель папку «Данные сотрудников» со всеми файлами.
3. Безвозвратно удалить данные файлы (Shift+Delete) с жесткого диска и USB-Flash накопителя.
4. Выключить ПК АРМ1.

При эмуляции действий потенциального злоумышленника предполагается, что он имеет доступ к учетной записи администратора и съемному накопителю с удаленной информацией. Для восстановления данных можно использовать различные свободно распространяемые программы. В данном случае предлагается использовать утилиту Recuva.

5. Включить ПК АРМ1 и зарегистрироваться администратором.
6. С помощью утилиты Recuva выполнить поиск остаточной информации на жестком диске ПК АРМ1 и USB-Flash накопителе, рисунок 32.

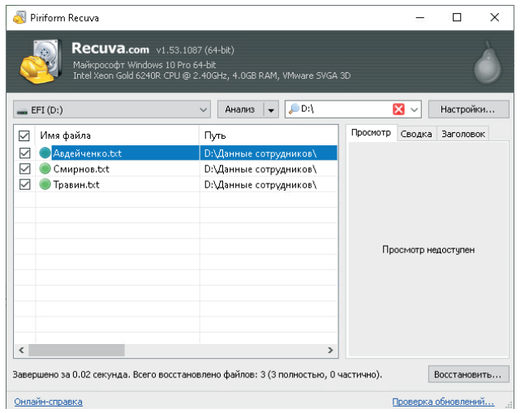

Рисунок 32. Поиск остаточной информации с помощью утилиты Recuva

7. С помощью утилиты Recuva выполнить восстановление файлов. Просмотреть их содержимое. Файлы должны сохранить всю информацию на момент их удаления.
8. Восстановить каталоги из таблицы 3 на жестком диске и на USB-Flash накопителе.
9. Открыть оболочку администратора СЗИ НСД Dallas Lock 8.0.
10. Настроить механизм очистки остаточной информации. Для этого перейти на вкладку «Параметры безопасности» и открыть категорию «Очистка остаточной информации».

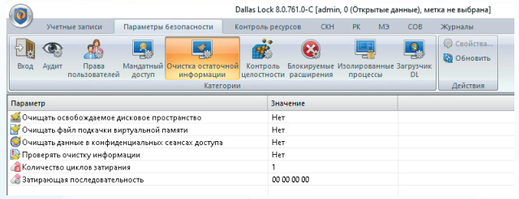

Рисунок 33. Настройка подсистемы очистки остаточной информации

11. Для параметров «Очищать освобождаемое дисковое пространство», «Очищать файл подкачки виртуальной памяти» установить значение «Да».
12. Безвозвратно удалить упомянутые файлы (Shift+Delete), содержащиеся в папке «Данные сотрудников» на жестком диске и USB-Flash накопителе.
13. Перезагрузить ПК АРМ1.
14. Зарегистрироваться администратором. С помощью утилиты Recuva выполнить поиск остаточной информации на жестком диске ПК АРМ1 и USB-Flash накопителе.
15. С помощью утилиты Recuva выполнить восстановление файлов. Просмотреть их содержимое. В файлах не должно быть информации, которую они содержали до удаления.

Содержание отчета

Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения — назначение и возможности подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности.
4. Ответы на контрольные вопросы.

Контрольные вопросы

1. Назначение подсистемы очистки остаточной информации СЗИ НСД Dallas Lock 8.0.
2. Укажите максимальное количество циклов затирания остаточной информации в СЗИ НСД Dallas Lock 8.0.
3. Как выполнить зачистку дискового пространства по команде пользователя?

3. ЛИТЕРАТУРА

1. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации: РД: утв. Гостехкомиссией России – М.: Изд-во стандартов, 1992. – 29 с.
2. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации: РД: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992. – 21 с.
3. Духан Е. И., Синадский Н. И., Хорьков Д. А. Применение программно-аппаратных средств защиты компьютерной информации: учебное пособие / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков; науч. ред. д-р техн. наук, проф. Н. А. Гайдамакин. – Екатеринбург: УГТУ-УПИ, 2008. – 182 с.
4. Зегжда Д. П. Как построить защищенную информационную систему. Технология создания безопасных систем / Д. П. Зегжда, А. М. Ивашко; под науч. ред. П. Д. Зегжды, В. В. Платонова. – СПб.: Мир и Семья-95, Интерлайн, 1998. – 312 с.
5. Описание применения СЗИ НСД Dallas Lock 8.0-К [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-dallas-lock-8-0/szi-ot-nsd-dallas-lock-8-0-k/#tabs-2.
6. Руководство оператора СЗИ НСД Dallas Lock 8.0 [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-dallas-lock-8-0/szi-ot-nsd-dallas-lock-8-0-k/#tabs-2.
7. Руководство по эксплуатации СЗИ НСД Dallas Lock 8.0 [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-dallas-lock-8-0/szi-ot-nsd-dallas-lock-8-0-k/#tabs-2.

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

https://www.**confident**.ru/
https://www.**dallaslock**.ru/
e-mail:
distribution@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда: