УТВЕРЖДЕН
RU.48957919.26.20.40.142.001 92-ЛУ
(взамен RU.48957919.501410-01 92-ЛУ)

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock 8.0

(версия 14.7.7.959)

Руководство по эксплуатации

RU.48957919.26.20.40.142.001 92
(взамен RU.48957919.501410-01 92)

Листов 342

АННОТАЦИЯ

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

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

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **8**

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ **8**

ТЕРМИНЫ И СОКРАЩЕНИЯ **9**

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ **11**

1.1 Общее описание 11
1.2 Структура и составные модули 11
1.3 Возможности 12
1.4 Политика лицензирования 17

2 УСТАНОВКА И УДАЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ **18**

2.1 Подготовка компьютера к установке 18
2.1.1 Требования к аппаратному и программному обеспечению 18
2.1.2 Ограничения 18
2.1.3 Предварительная подготовка 19
2.1.4 Особенности установки 20
2.2 Установка системы защиты 21
2.3 Удаление системы защиты 25
2.4 Обновление системы защиты 26
2.5 О программе 26
2.6 Вход на защищенный компьютер 27
2.6.1 Вход с использованием смарт-карт с сертификатом УЦ Windows 28
2.6.2 Вход с аппаратным идентификатором 29
2.6.3 Ограничение количества терминальных сессий 32

3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ **34**

3.1 Администрирование Dallas Lock 34
3.2 Панель действий 37
3.3 Контекстное меню объектов 38
3.4 Сортировка списка параметров 38
3.5 Значок блокировки на панели задач 39
3.6 Полномочия пользователей на администрирование системы защиты 39
3.6.1 Порядок предоставления полномочий 40
3.6.2 Полномочия на просмотр параметров безопасности 41
3.6.3 Полномочия на управление параметрами безопасности 42
3.6.4 Полномочия на управление дискреционным доступом 42
3.6.5 Полномочия на управление мандатным доступом 42
3.6.6 Полномочия на управление контролем целостности 42
3.6.7 Полномочия на деактивацию системы защиты 43

4 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ **44**

4.1 Управление учетными записями 44
4.1.1 Полномочия на управление учетными записями 44
4.1.2 Создание и удаление локальных пользователей 45
4.1.3 Регистрация доменных пользователей 50
4.1.4 Регистрация доменных учетных записей по маске 51
4.1.5 Создание и удаление групп пользователей 52
4.1.6 Число разрешенных сеансов 54
4.1.7 Смена пароля пользователя 55
4.1.8 Сессии-исключения 56
4.2 Заблокированные пользователи 57
4.3 Аппаратная идентификация пользователя 57
4.3.1 Назначение аппаратной идентификации 57
4.3.2 Настройка считывателей аппаратной идентификации 59
4.3.3 Принудительная двухфакторная аутентификация 65
4.3.4 Снятие аппаратной идентификации 65
4.3.5 Действия с идентификатором 65
4.3.6 Поддержка биометрии 67
4.3.7 Запись авторизационных данных в идентификатор 68

4.3.8 Определение принадлежности идентификатора ... 70
4.4 Аутентификация с PayControl ... 70
4.4.1 Подключение сервера PayControl ... 70
4.4.2 Настройка идентификатора PayControl для пользователя ... 71
4.5 Параметры входа ... 74
4.5.1 Разрешение и запрет интерактивного и удаленного входов в ОС ... 74
4.5.2 Настройка политик авторизации ... 75
4.5.3 Настройка политик паролей ... 78
4.5.4 Настройка политик доступа ... 80
4.5.5 Настройка политик сети ... 83
4.6 Изолированные процессы ... 84
4.7 Загрузчик DL ... 85
4.7.1 Включение модуля «Загрузчик DL» ... 86
4.7.2 Создание PIN-кода пользователя ... 87
4.7.3 Вход на компьютер при активном загрузчике ... 89
4.7.4 Дополнительные условия работы модуля «Загрузчик DL» ... 90

5 РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ФС ... 91

5.1 Дескрипторы объектов ... 91
5.2 Дискреционный доступ ... 92
5.2.1 Права доступа ... 92
5.2.2 Механизм определения прав доступа пользователя к ресурсам ФС ... 94
5.2.3 Дискреционный доступ для глобальных параметров ... 96
5.2.4 Дискреционный доступ для локальных объектов ФС и веток реестра ... 98
5.2.5 Дискреционный доступ к аппаратным идентификаторам ... 101
5.2.6 Низкоуровневый доступ к диску и съемным накопителям ... 102
5.2.7 Дескрипторы по пути ... 103
5.3 Мандатный доступ ... 104
5.3.1 Настройки параметров мандатного доступа ... 105
5.3.2 Переименование уровней доступа и мандатных меток ... 105
5.3.3 Уровни и метки доступа пользователей ... 106
5.3.4 Назначение мандатного доступа на объекты ... 106
5.3.5 Механизм разграничения мандатного доступа ... 108
5.3.6 Механизм разделяемых папок ... 108
5.3.7 Текущий уровень и метка доступа пользователя ... 109
5.3.8 Служебный пользователь ... 111
5.3.9 Пример настройки мандатного доступа по сети ... 112
5.3.10 Настройка мандатного доступа для корректной работы пользователя с ПО ... 112
5.4 Дополнительные режимы доступа ... 115
5.4.1 Режим обучения ... 115
5.4.2 Неактивный режим ... 116
5.4.3 Замкнутая программная среда ... 118
5.5 Графическая оболочка Dallas Lock ... 122
5.5.1 Включение и выключение оболочки ... 122
5.5.2 Настройка оболочки ... 124

6 ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА ... 125

6.1 Средства аудита ... 125
6.1.1 Политики аудита ... 125
6.1.2 Полномочия на просмотр и управление параметрами безопасности ... 129
6.2 Аудит доступа ... 130
6.2.1 Аудит глобальных параметров ... 131
6.2.2 Аудит локальных объектов ФС и веток реестра ... 132
6.3 Журналы ... 133
6.3.1 Фильтры журналов ... 139
6.3.2 Группировка записей журнала ... 140
6.4 Теневое копирование ... 140

7 ПОДСИСТЕМА ПЕЧАТИ ... 142

7.1 Разграничение доступа к печати ... 142
7.1.1 Мандатное разграничение доступа к печати ... 143
7.1.2 Разграничение доступа к принтерам ... 143
7.2 Аудит печати ... 143

7.2.1 Журнал печати 144
7.2.2 Теневые копии распечатываемых документов 144
7.2.3 Добавление штампа на распечатываемые документы 145

8 ОЧИСТКА ОСТАТОЧНОЙ ИНФОРМАЦИИ 149

8.1 Регистрация действий по очистке остаточной информации 149
8.2 Параметры очистки остаточной информации 149
8.2.1 Проверка очистки информации 150
8.2.2 Очистка освобождаемого дискового пространства 150
8.2.3 Очистка файла подкачки виртуальной памяти 150
8.2.4 Очистка данных в конфиденциальных сеансах доступа 150
8.2.5 Количество циклов затирания, затирающая последовательность 150
8.3 Удаление файлов и зачистка остаточной информации по команде 150
8.4 Запрет смены пользователя без перезагрузки 152
8.5 Зачистка диска 152

9 ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ 154

9.1 Настройка политик контроля целостности 154
9.2 Контроль целостности объектов ФС и веток реестра 156
9.2.1 Установка целостности 156
9.2.2 Проверка целостности 158
9.2.3 Восстановление файла или ветки реестра в случае нарушения целостности 159
9.3 Контроль целостности программно-аппаратной среды 159

10 КОНТРОЛЬ УСТРОЙСТВ 162

10.1 Полномочия на управление контролем устройств 163
10.2 Разграничение доступа к устройствам 163
10.2.1 Дискреционный доступ к устройствам 164
10.2.2 Мандатный доступ к устройствам 165
10.3 Аудит доступа к устройствам 166

11 УДАЛЕННЫЙ ДОСТУП И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ 167

11.1 Удаленный доступ к незащищенному компьютеру с защищенного 167
11.2 Удаленный доступ к защищенному компьютеру с незащищенного 167
11.3 Удаленный доступ к защищенному компьютеру с защищенного 167
11.4 Ключи защиты сетевого взаимодействия 168
11.5 Сетевое администрирование 169

12 ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ 171

12.1 Прозрачное преобразование дисков 171
12.2 Преобразование данных в файл-контейнер 172
12.2.1 Преобразование объектов ФС 172
12.2.2 Обратное преобразование объектов ФС 174
12.3 Преобразованные файл-диски 174
12.3.1 Создание преобразованного файл-диска 174
12.3.2 Работа на преобразованном файл-диске 176
12.3.3 Доступ к преобразованным файл-дискам 176

13 СИСТЕМА КОНТРОЛЯ НАКОПИТЕЛЕЙ 177

13.1 Права доступа к съемным накопителям 177
13.2 Описание для съемных накопителей 179
13.3 Преобразование съемных накопителей 179
13.3.1 Создание ключей преобразования 180
13.3.2 Процесс преобразования накопителя 181
13.3.3 Доступ к преобразованным накопителям 181
13.3.4 Обратное преобразование 184

14 РЕЗЕРВНОЕ КОПИРОВАНИЕ 185

14.1 Назначение и общие принципы работы 185
14.2 Эксплуатация 185

15 МЕЖСЕТЕВОЙ ЭКРАН 190

15.1 Назначение и общие принципы работы 190
15.1.1 Возможности межсетевого экрана 190
15.2 Эксплуатация 190
15.2.1 Адреса 191
15.2.2 Сегменты сети 191
15.2.3 Соединения 192
15.2.4 Параметры 193
15.2.5 Правила МЭ 199
15.2.6 Профили МЭ 212
15.2.7 Фильтрация 215
15.2.8 Статистика МЭ 226
15.2.9 Отключение МЭ 227
15.3 Журналы МЭ 227
15.3.1 Служебный журнал 228
15.3.2 Журнал пакетов МЭ 228
15.3.3 Журнал соединений 229
15.3.4 Журнал трафика фильтрации МЭ 230

16 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ 232

16.1 Назначение и общие принципы работы 232
16.1.1 Возможности системы обнаружения вторжений 232
16.2 Основное 232
16.2.1 Статистика СОВ 232
16.2.2 Обновления 233
16.2.3 Порты 234
16.3 Настройки сигнатур 234
16.3.1 Сигнатуры журналов 234
16.3.2 Сигнатуры трафика 237
16.3.3 Настройки переменных 240
16.3.4 Исключения 242
16.4 Блокировки 242
16.4.1 Заблокированные адреса 242
16.4.2 Доверенные адреса 244
16.5 Параметры СОВ 245
16.5.1 Контроль приложений 245
16.5.2 Контроль реестра 250
16.5.3 Настройки эвристики 251
16.5.4 Глобальные параметры 253
16.5.5 Отключить СОВ 258
16.6 Безопасная среда СОВ (песочница) 259
16.6.1 Настройки 259
16.6.2 Настройки эвристики безопасной среды 261
16.6.3 Контроль приложений 265
16.6.4 Файловая система и реестр 267
16.6.5 Режим безопасной среды 267
16.7 Журналы СОВ 271

17 СРЕДСТВО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ 274

17.1 Параметры СОР 274
17.2 Индикаторы компрометации (IoC) 278
17.3 Индикаторы атаки (IoA) 286
17.4 Правила автоматического реагирования 287
17.5 Отчеты 290
17.6 Обновления 291
17.7 Блокировки 292
17.8 Журнал СОР 292

18 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ 295

18.1 Отчеты 295
18.1.1 Создание отчета о правах и конфигурации 295
18.1.2 Создание отчета об уязвимостях ПО в соответствии с БДУ ФСТЭК России 296
18.1.3 Создание отчета по журналам СЗИ 297
18.1.4 Создание паспорта программного обеспечения 298

18.1.5 Создание паспорта аппаратной части ПК 299
18.2 Автоматическое тестирование функций СЗИ 300
18.3 Сохранение резервной копии файлов СЗИ 301
18.4 Возврат к настройкам по умолчанию 303
18.5 Шаблоны информационных систем 304

19 СОХРАНЕНИЕ КОНФИГУРАЦИИ 305

19.1 Сохранение файла конфигурации Dallas Lock 305
19.2 Автоматическое сохранение конфигурации 306
19.3 Применение файла конфигурации Dallas Lock 307

20 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK 308

21 ВОССТАНОВЛЕНИЕ КОМПЬЮТЕРА ПРИ СБОЕ СИСТЕМЫ ЗАЩИТЫ 310

21.1 Обратное преобразование жесткого диска в аварийном режиме 310
21.2 Аварийное отключение загрузчика для ПК с UEFI-интерфейсом BIOS 310
21.3 Аварийное отключение Dallas Lock 8.0 с помощью загрузочного диска 311
21.3.1 Отключение загрузчика и подмена системных файлов 311
21.3.2 Очистка реестра 312
21.4 Аварийное отключение Dallas Lock 8.0 в ручном режиме 313
21.4.1 Порядок аварийного отключения для Windows 313

22 РЕЗЕРВНОЕ ВОССТАНОВЛЕНИЕ ДИСКА 316

22.1 Создание загрузочного диска Acronis 316
22.2 Сохранение образа диска с помощью Acronis 318
22.3 Восстановление образа диска с помощью Acronis 321

ПРИЛОЖЕНИЕ А 324

А.1 Шаблоны автоматизированных систем 324
А.2 Шаблоны государственных информационных систем 329
А.3 Шаблоны информационных систем персональных данных 335

ВВЕДЕНИЕ

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

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

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

Руководство состоит из 23 глав и имеет следующую структуру:

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

Сайт компании-разработчика **Dallas Lock 8.0 ООО «Конфидент»** доступен по ссылке: www.confident.ru.

Информация о продуктах линейки **Dallas Lock** представлена на странице сайта http://www.dallaslock.ru/. На данном сайте можно получить информацию о системе защиты **Dallas Lock 8.0**, предыдущих версиях, а также заказать комплекс услуг по проектированию, внедрению и сопровождению продукта. Также при необходимости можно обратиться в службу технической поддержки **Dallas Lock 8.0** по электронному адресу: helpdesk@confident.ru.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

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

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

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



ТЕРМИНЫ И СОКРАЩЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для системы защиты **Dallas Lock 8.0**, другие используются для удобства, третьи выбраны из соображений краткости.

Термины *«компьютер», «ПК», «рабочая станция»* считаются эквивалентными, и используются в тексте руководства.

Загрузчик — **модуль загрузчика DL**, отрабатывает между Включением ПК и до начала загрузки ОС.

Замкнутая программная среда — режим работы защищенного ПК, при котором для конкретных пользователей определяется список доступных для работы программ.

Клиент — компьютер, защищенный **Dallas Lock 8.0**, входящий в состав ДБ.

Мышь — ручной манипулятор, преобразующий механические движения в движение курсора на экране.

Параметры безопасности, или политики безопасности — совокупность правил по обеспечению безопасности информации, выраженные настраиваемыми категориями системы защиты.

Суперадминистратор ЗАРМ Dallas Lock — пользователь, под учетной записью которого выполнена установка системы защиты.

Администратор ЗАРМ Dallas Lock — пользователь, наделенный всеми полномочиями на администрирование системы защиты на ЗАРМ.

Аудитор ЗАРМ Dallas Lock — пользователь, наделенный правами на просмотр параметров аудита и журналов системы защиты.

Администратор ОС ЗАРМ — пользователь, наделенный полномочиями на администрирование ОС на защищаемом компьютере.

Сокращение	Полная формулировка
АИБ	Администратор информационной безопасности
АЛП	Автоматические локальные правила
АС	Автоматизированная система
БДУ	Банк данных угроз безопасности информации
БС	Безопасная среда
ЗАРМ	Защищенное автоматизированное рабочее место
ЗПС	Замкнутая программная среда
ДБ	Домен безопасности
ИПС	Изолированная программная среда
ЛВС	Локальная вычислительная сеть
ОС	Операционная система
ОУ	Оперативное управление
ПК	Персональный компьютер
ПО	Программное обеспечение
СЗИ	Система защиты информации от несанкционированного доступа
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ТС	Техническое средство
СОВ	Система обнаружения вторжений
СОР	Система обнаружения и реагирования
БРП	База решающих правил
ФС	Файловая система
ЭП	Электронная подпись
ЭЦП	Электронно-цифровая подпись
AD	Active Directory
DL	Dallas Lock 8.0

Сокращение	Полная формулировка
IoA	Индикатор атаки
IoA-объект	JSON-объект, который содержит описание индикатора атаки
IoA-файл	Файл, в котором определены один или несколько IoA-объектов
IoC	Индикатор компрометации
IoC-объект	JSON-объект, который содержит описание индикатора компрометации
IoC-файл	Файл, в котором определены один или несколько IoC-объектов
MBR (Master Boot Record)	Системная область жесткого диска. Содержит программы начальной загрузки ОС и информацию о размещении логических дисков. Используется на этапе загрузки компьютера
BIOS	Набор микропрограмм, образующих системное ПО, которые обеспечивают начальную загрузку компьютера и последующий запуск ОС
SP (Service Pack)	Пакет обновлений для ОС
VNC	Virtual Network Computing
WFP (Windows Filtering Platform)	Функциональная возможность для драйверов ОС семейства Windows, упрощающая анализ сетевого трафика.

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ

1.1 Общее описание

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

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

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

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

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

1.2 Структура и составные модули

СЗИ состоит из следующих основных компонентов:

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

   Драйвер защиты автоматически запускается на защищенном автоматизированном рабочем месте (далее — АРМ) 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.
3. **Подсистема управления доступом**. Включает в себя:
   - Подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов.
   - Подсистему доступа к ФС, реестру и устройствам, в составе которой:
     - подсистема дискреционного доступа;
     - подсистема мандатного доступа (только для Dallas Lock 8.0 редакции «С»).
   - Модуль **Загрузчик DL** (только для Dallas Lock 8.0 редакции «С»). Является опционным

модулем, включается по команде администратора и может быть не активированным. Активный модуль отрабатывает до начала загрузки ОС.

4. **Подсистема регистрации и учета**. Включает в себя:
   - Подсистему аудита. Обеспечивает ведение аудита и хранение информации 13 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 съемных 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 резервного копирования.** Модуль **Резервное копирование** позволяет восстанавливать безвозвратно модифицированные или удаленные файлы, или каталоги (с поддержкой вложенных файлов).

1.3 Возможности

СЗИ предоставляет следующие возможности:

1. В соответствии со своим назначением **СЗИ** 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, объектам ФС, веткам реестра и 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 съемных накопителей (таких как компакт-диск, USB-Flash накопитель и прочие) **СЗИ** обеспечивает следующие функции:
   - разграничение доступа как к типам накопителей, так и к конкретным экземплярам;
   - преобразование съемных накопителей с использованием ключа (в качестве ключа преобразования используется алгоритм преобразования, пароль и (или) аппаратный идентификатор);
   - создание теневых копий файлов, отправляемых на съемные или сетевые накопители.
3. В **СЗИ** реализована возможность включения функции блокировки компьютера при подключении незарегистрированных машинных носителей информации.
4. **СЗИ** 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 Touch, Рутокен ЭЦП PKI, Рутокен S, Рутокен ЭЦП 2.0 3000, Рутокен ЭЦП 2.0 Flash, Рутокен Lite 1000, Рутокен Lite 1010, Рутокен ЭЦП 3.0 3100, Рутокен ЭЦП 3.0 3200, Рутокен ЭЦП 3.0 3220, Рутокен ЭЦП Bluetooth, Рутокен Web, Рутокен PINPad, Рутокен 2151;
- USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash;
- USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64K;
- NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X);
- Guardant ID 2.0.

Дополнительно имеется возможность определения принадлежности аппаратного идентификатора.



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

5. 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.
6. Есть возможность включения функции блокировки компьютера пользователя при отключении назначенного аппаратного идентификатора.
7. 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.
8. 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.
9. Включение модуля **Загрузчик DL** (только для Dallas Lock 8.0 редакции «С») позволяет авторизовать пользователя при входе на ПК до загрузки ОС. Загрузка ОС с жесткого диска осуществляется только после ввода особого PIN-кода и его проверки в **СЗИ**.
10. 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»).
11. 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).
12. **Dallas Lock 8.0** позволяет настраивать **Замкнутую программную среду** (далее — ЗПС) — режим, в котором пользователь может запускать только программы, определенные администратором.
13. 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 **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**.

14. 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**.

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

16. 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.

17. 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.

18. В **СЗИ** 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.

19. **СЗИ** 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.

20. В **СЗИ** 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.

21. В **СЗИ** реализовано ведение 13 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.
- **Системный журнал**. 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.
- **Журнал средства обнаружения и реагирования**. В журнал заносятся события, связанные с индикаторами компрометации и правилами автоматического реагирования **СОР**.

Для облегчения работы с журналами есть возможность фильтрации, архивации, группировки по заданному набору полей, экспорта записей журналов в различные форматы и формирования отчета по всем журналам **СЗИ**. 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.

22. 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.
23. 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.
24. Преобразование информации средствами **СЗИ** осуществляется встроенными алгоритмами преобразования.
25. 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.
26. Реализована возможность включения функции блокировки, преобразованного файл-диска при отключении назначенного аппаратного идентификатора.
27. При использовании нескольких защищенных **СЗИ** 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.
28. Реализован механизм проверки электронной подписи (далее — ЭП) при обновлении **СЗИ**.
29. Для решения задач организации централизованного управления решениями продуктовой линейки **ООО Конфидент** (**СЗИ Dallas Lock 8.0**, **СЗИ Dallas Lock Linux**, **СЗИ ВИ Dallas Lock**, **СДЗ Dallas Lock**, **СДЗ УБ Dallas Lock**, шлюз безопасности **WAF Dallas Lock**) и контроля конфигурации сетевого оборудования используется **Единый центр управления Dallas Lock** (далее **ЕЦУ**) 20 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK.

30. **Dallas Lock 8.0** содержит подсистему самодиагностики основных функций безопасности **СЗИ** (тестирование).
31. 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.).
32. 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»).
33. Предусматривается ведение резервных копий программных средств защиты информации, их периодическое обновление и контроль работоспособности, а также возможность возврата к настройкам по умолчанию.
34. При необходимости переноса настроек **Dallas Lock 8.0** (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.
35. **СЗИ** обеспечивает контроль съемных машинных носителей информации.
36. **СЗИ** обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.
    - Для снижения трудоемкости **настройки МЭ** возможно использовать **Режим обучения МЭ**, в котором при обращении к веб-ресурсу, доступ к которому разрешен, разрешающие права назначаются автоматически либо интерактивно.
    - Посредством фильтрации возможно контролировать сетевой трафик по его содержимому (анализируется присутствие известных протоколов, медиа-контента и мобильный код) во всем фильтруемом трафике.
    - Динамическая активация определенных **правил МЭ** в зависимости от условий функционирования системы, таких как нарушение целостности, отсутствие антивируса KES, отсутствие обновлений ОС, сигнатур **системы обнаружения вторжений** (далее — **СОВ**) или сигнатур антивируса, обеспечивается механизмом **профилей МЭ**.
    - Механизм «сегментов сетей» **МЭ** позволяет применять **правила МЭ** и фильтрации не безусловно, а в зависимости от параметров сети, через которую получен сетевой пакет. Есть возможность применять **правила МЭ** или фильтрации не безусловно, а только для определенных сетей, определяющихся сегментом сети.
    - Профиль **МЭ** «Изоляция узла» позволяет логически изолировать автоматизированное рабочее место от сети передачи данных и поддерживать соединение только с **ЕЦУ**.
37. **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.
38. **СЗИ** обеспечивает защиту АС от вирусов-шифровальщиков и минимизацию ущерба от них, включая предотвращение повреждения файлов **СЗИ**, отслеживание вредоносных активностей и подозрительных файловых операций, а также принятие решений о реагировании и регистрацию событий, связанных с активностью вирусов-шифровальщиков.
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** реализован механизм запускаемого вручную и автоматического обнаружения индикаторов компрометации на ЗАРМ, а также сканирования новых файлов в системе с возможностью гибкой настройки автоматического реагирования **СОР** на их обнаружение**.**
42. В **СЗИ** предустановлены шаблоны безопасности, соответствующие стандартам по защите автоматизированных систем, информационных систем персональных данных и государственных информационных систем.
43. В **СЗИ** реализовано проведение анализа ПО, установленного на ЗАРМ, в соответствии с Банком данных угроз безопасности информации ФСТЭК России и последующее формирование отчета об уязвимостях ПО.

1.4 Политика лицензирования

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

1. Защита от НСД (**СЗИ НСД**).
2. Средство контроля подключения носителей информации (**СКН**).
3. Средство контроля отчуждения информации с носителей информации (**СКН**).
4. Межсетевой экран (**МЭ**).
5. Система обнаружения вторжений (**СОВ**).
6. Средство обнаружения и реагирования (**СОР**).
7. Резервное копирование (**РК**).
8. Возможность аутентификации через PayControl (**PayControl**).

2 УСТАНОВКА И УДАЛЕНИЕ СИСТЕМЫ ЗАЩИТЫ

2.1 Подготовка компьютера к установке

2.1.1 Требования к аппаратному и программному обеспечению

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

СЗИ может работать на любом техническом средстве, работающем под управлением следующих ОС:

- Windows 7 (SP1)[1] (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter) (см. Формуляр RU.48957919.26.20.40.142.001 30 п. 3.3.4);
- Windows Server 2008 R2 (SP1)[1] (Foundation, Standard, Web, Enterprise, Datacenter) (см. Формуляр RU.48957919.26.20.40.142.001 30 п. 3.3.4);
- Windows 8 (Core, Pro, Enterprise);
- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows 8.1 (Core, Pro, Enterprise);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Standard, Datacenter, Essentials);
- Windows 11 (Enterprise, Pro, Home);
- Windows Server 2022 (Essentials, Standard, Datacenter);
- Windows Server 2025 (Standard, Datacenter).

Dallas Lock 8.0 поддерживает 32- и 64-битные версии ОС Windows[2].

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

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

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

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

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

2.1.2 Ограничения

СЗИ имеет следующие ограничения:

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

Для корректной работы сетевых сигнатур **СОВ** необходимо указать номера или диапазон используемых портов, раздел 16.3.2 Сигнатуры трафика.

[1] С установленными обновлениями KB3033929 и KB3080149 (или пакетами обновлений, в состав которых они входят).

[2] Архитектура IA64 (Itanium) не поддерживается.

При запуске установки **Dallas Lock 8.0** на ОС Windows, установленную на съемный накопитель по технологии Windows To Go, может возникнуть ошибка подсистемы установки Windows Installer: 2755. В этом случае нужно распаковать установочный msi-файл **Dallas Lock 8.0** в выбранный каталог командой «C:\> msiexec /a DallasLock8.0C.msi[3] /qb targetdir=c:\имя_каталога». После чего в каталоге, указанном в параметре targetdir, должны появиться: файл dlinst.exe и каталоги Files_x64, Files_x86. Затем нужно запустить программу установки из командной строки: «C:\имя_каталога\dlinst.exe /msi».

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

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

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

При обновлении ОС Windows (до Windows 8, Windows 8.1, Windows 10, Windows 11) изделие необходимо удалить, раздел 2.3 Удаление системы защиты» , выполнить обновление, после чего установить изделие, используя при необходимости функцию сохранения конфигурации, глава 19 СОХРАНЕНИЕ КОНФИГУРАЦИИ.

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

При работе с **Dallas Lock 8.0** на ОС Windows 7 возможны проблемы совместимости с продуктом DeviceLock DLP 8.0.

Для корректной совместной работы виртуальных машин Microsoft Hyper-V и **Dallas Lock 8.0** требуется настроить параметр безопасности **Исключения для приложений,** добавив исключение для контроля приложения C:\Windows\System32\vmwp.exe. При добавлении исключения для контроля приложения в блоке *Компонент* необходимо выбрать тип исключения *Все*, подраздел 4.5.2 Настройка политик авторизации.

2.1.3 Предварительная подготовка

Перед установкой **СЗИ** необходимо выполнить следующие действия:

1. Если на компьютере уже установлена **СЗИ**, ее необходимо удалить.
2. Необходимо убедиться, что на диске C имеется необходимое свободное пространство для установки системы защиты.
3. Проверить состояние жестких дисков компьютера, например, при помощи приложения chkdsk.exe или служебной программы проверки диска из состава ОС Windows и устранить выявленные дефекты.
4. Рекомендуется произвести дефрагментацию диска.
5. Проверить компьютер на отсутствие вирусов.
6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы.
7. Закрыть все запущенные приложения, так как установка системы потребует принудительной перезагрузки.
8. Если установка производится на ОС Windows 7, Windows Server 2008 R2, то необходимо предварительно установить обновления для системы безопасности ОС: KB3033929 и KB3080149.

[3] Dallas Lock8.0K.msi

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

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

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

2.1.4 Особенности установки

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

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

Если установка производится под учетной записью доменного пользователя:

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

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

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

Если же компьютер является клиентом контроллера домена и при установке использовалась конфигурация по умолчанию[4], то зайти на ЗАРМ можно под любым доменным пользователем, так как в **СЗИ** автоматически создается и регистрируется учетная запись «**»[5].

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

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

[4] Подробнее 19.1 Сохранение конфигурации.

[5] Подробнее 4.1.4 Регистрация доменных учетных записей по маске.

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

2.2 Установка системы защиты

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

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

   После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге установки предоставляется возможность отмены установки с возвратом сделанных изменений. Для этого служит кнопка **Отмена**. Выполнение следующего шага установки выполняется с помощью кнопки **Далее**.
2. При установке системы защиты на компьютере с установленной ОС 7 и выше после запуска приложения на экране будет выведено окно для подтверждения операции (рис. 1).

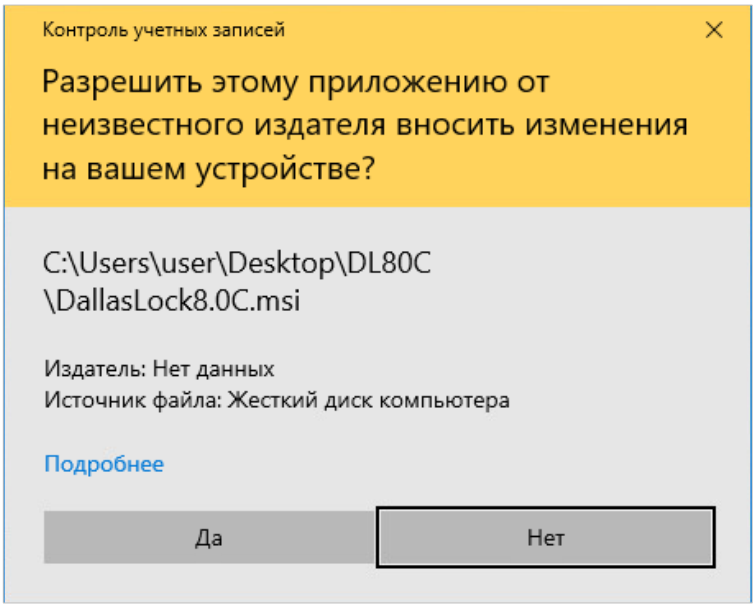


Рис. 1. Разрешение на установку программы в ОС

После подтверждения запустится программа установки **СЗИ** (рис. 2).

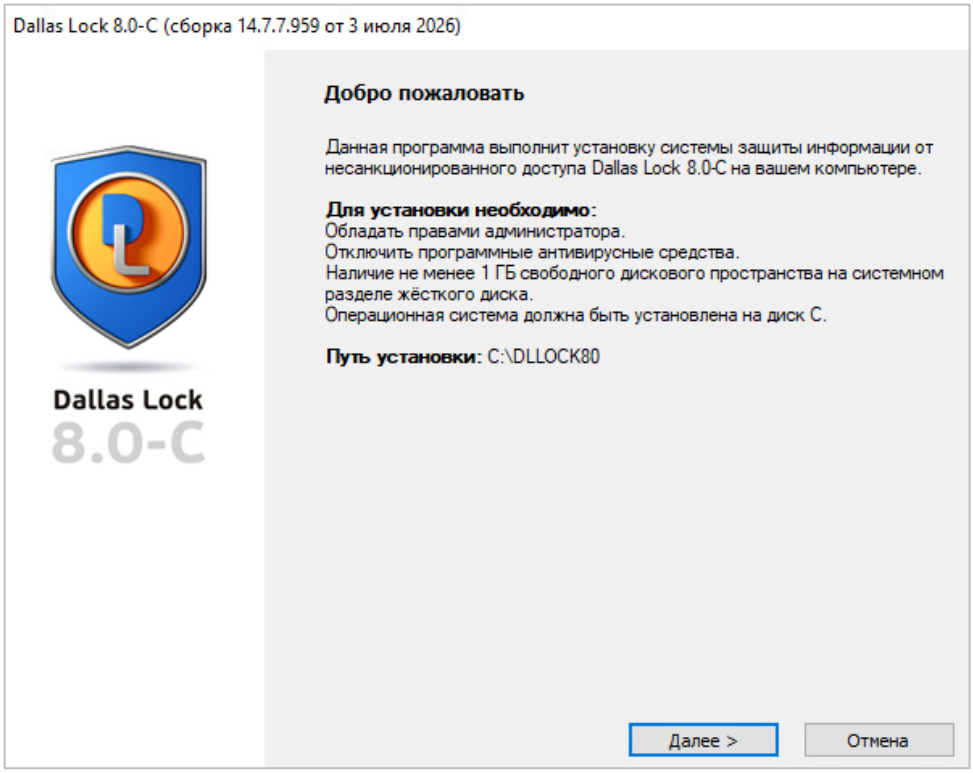


Рис. 2. Окно начала установки системы защиты

Для продолжения установки нажать кнопку **Далее**.

3. Для защиты от нелегального использования продукта необходимо ввести номер лицензии, указанный на коробке компакт-диска с дистрибутивом **Dallas Lock 8.0** или в письме, отправленном на электронную почту, и код активации технической поддержки, указанный в письме, отправленном на электронную почту (рис. 3). Номер лицензии может активировать один или несколько модулей **Dallas Lock 8.0** (**МЭ**, **СОВ**, **СОР**, **СКН-П**, **СКН-Н**, **РК**, **PayControl**), либо оставить их неактивными (в зависимости от приобретенного изделия).

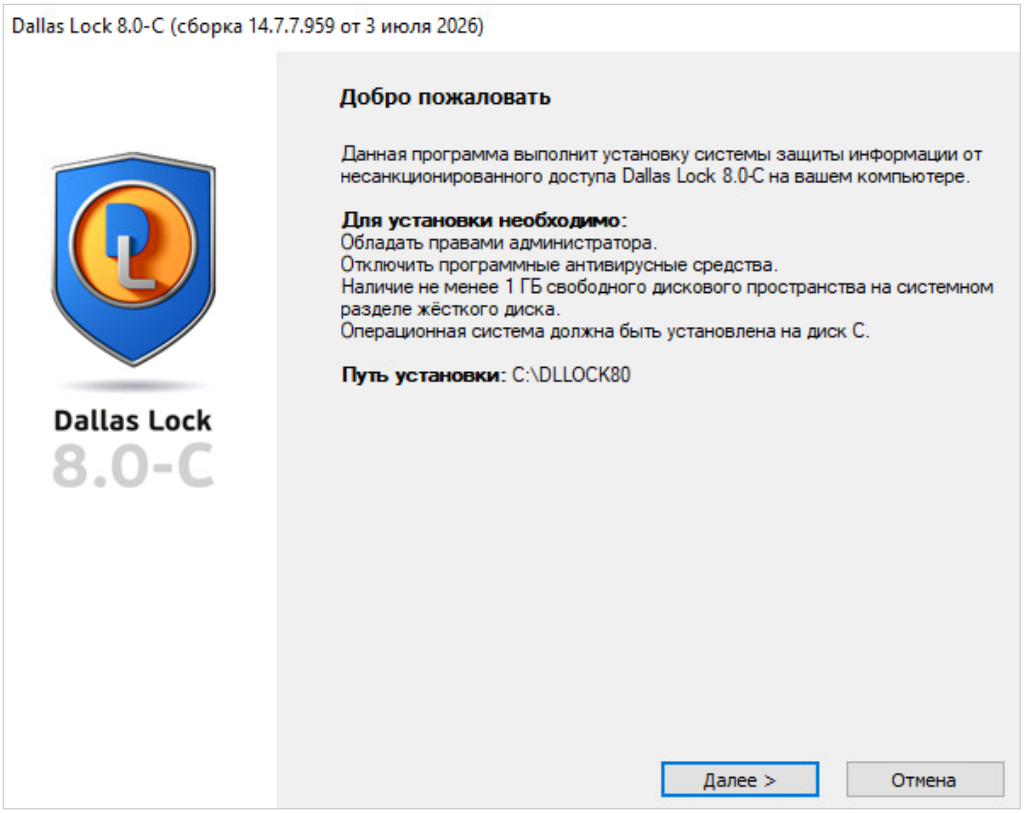


Рис. 3. Ввод параметров установки

Для продолжения установки нажать кнопку **Далее**.

4. В том случае, когда необходимо ввести компьютер в **ДБ** в процессе установки системы, необходимо поставить флаг *Ввести компьютер в домен безопасности* и заполнить поля подключения. Если этого не сделать на этапе установки, то компьютер не будет введен в **ДБ**, но это можно будет сделать и после установки **СЗИ**.

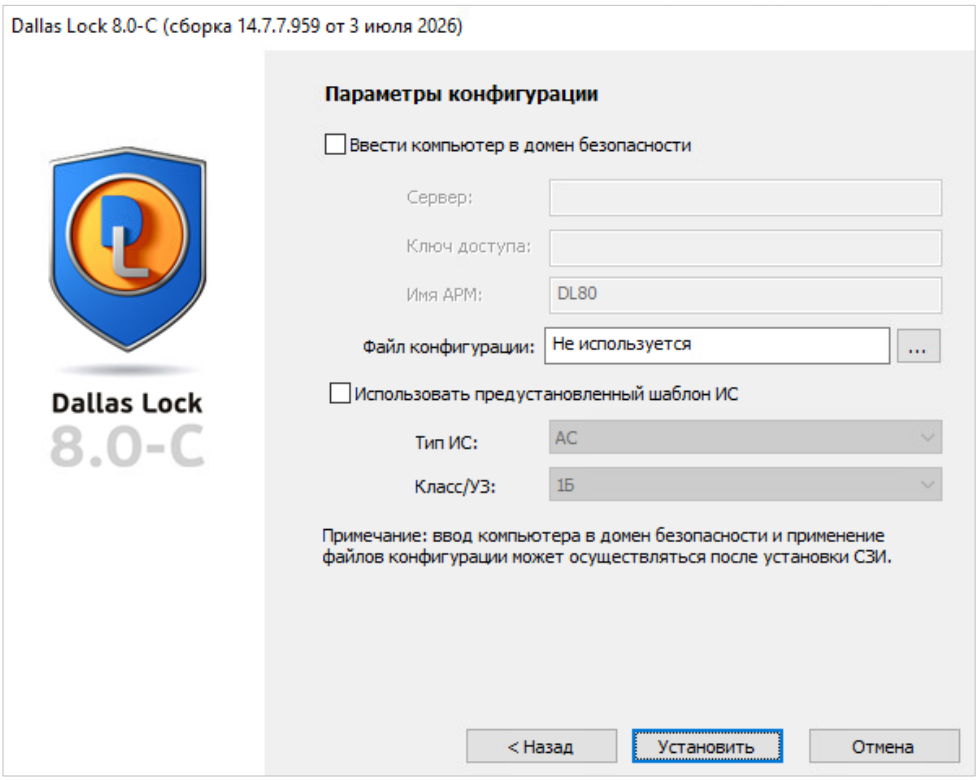
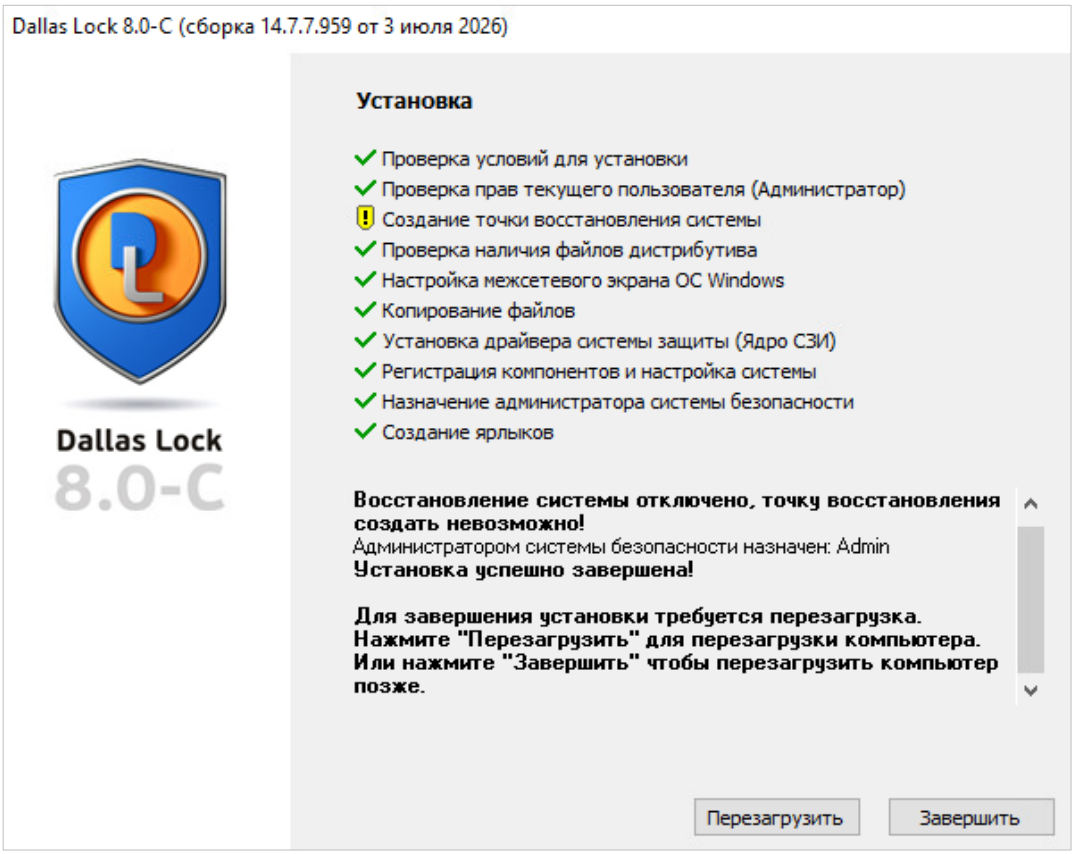


Рис. 4. Введение в ДБ на этапе установки

5. Опционально указать файл конфигурации (рис. 4) или поставить флаг *Использовать предустановленный шаблон ИС*. В выпадающих списках необходимо указать необходимый тип информационной системы и класс (уровень) защищенности в соответствии со следующими документами:
   - Руководящий документ (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (АС).
   - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей. государственную тайну, содержащейся в государственных информационных системах» (ГИС).
   - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ИСПДн).

   Для этого необходимо в выпадающем меню «Конфигурация» выбрать **Указать файл…,** нажать кнопку поиска рядом с полем ввода и в появившемся окне проводник выбрать заранее сохраненный файл, глава 19 Сохранение конфигурации. Для продолжения установки нажать кнопку **Установить**.
6. Далее возможно наблюдать за процессом установки. Если процесс прошел без ошибок, то для завершения установки требуется перезагрузка ПК. Через 1 минуту после нажатия кнопки **Перезагрузить** произойдет автоматическая перезагрузка ПК (рис. 5).



S

Рис. 5. Завершение установки программы

В процессе установки **Dallas Lock 8.0** автоматически создается точка восстановления системы.

При возникновении ошибок в создании точки восстановления системы (рис. 6), необходимо включить *Создание точки восстановления системы.*

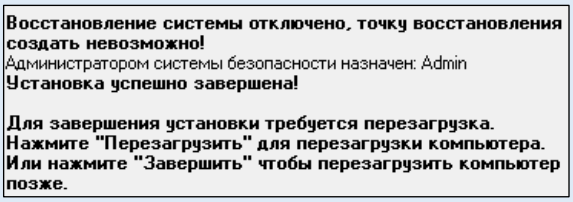


Рис. 6. Установка без точки восстановления системы

Для включения параметра *Создание точки восстановления системы* в Windows 10 необходимо открыть раздел **Система**. Если для системного диска указано значение *Отключено* в разделе **Защита системы**, потребуется нажать **Настроить**. Следует выбрать опцию *Включить защиту системы* и затем нажать **Применить** и **ОК**.

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

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

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

После установки системы защиты и перезагрузки компьютера в меню **Пуск** и на рабочем столе появится ярлык оболочки администратора **Dallas Lock 8.0.**



Рис. 7. Ярлык оболочки администратора Dallas Lock 8.0

2.3 Удаление системы защиты

Право удаления **СЗИ** может быть установлено для отдельных пользователей или групп пользователей администратором системы защиты. Необходимый параметр **Деактивация системы защиты** находится в категории **Параметры безопасности** → **Права пользователей**, раздел 3.6 Полномочия пользователей на администрирование системы защиты, при этом необходимо являться администратором ОС.

Перед удалением системы защиты с ПК рекомендуется сохранить файл конфигурации **Dallas Lock 8.0**, глава 19 Сохранение конфигурации.

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

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

В ОС Windows 10 необходимо вызвать пункт **Параметры**, выбрать пункт **Приложения**. В появившемся окне выделить **Dallas Lock 8.0C** (**Dallas Lock 8.0К**), выбрать действие **Удалить** и подтвердить удаление (рис. 8).

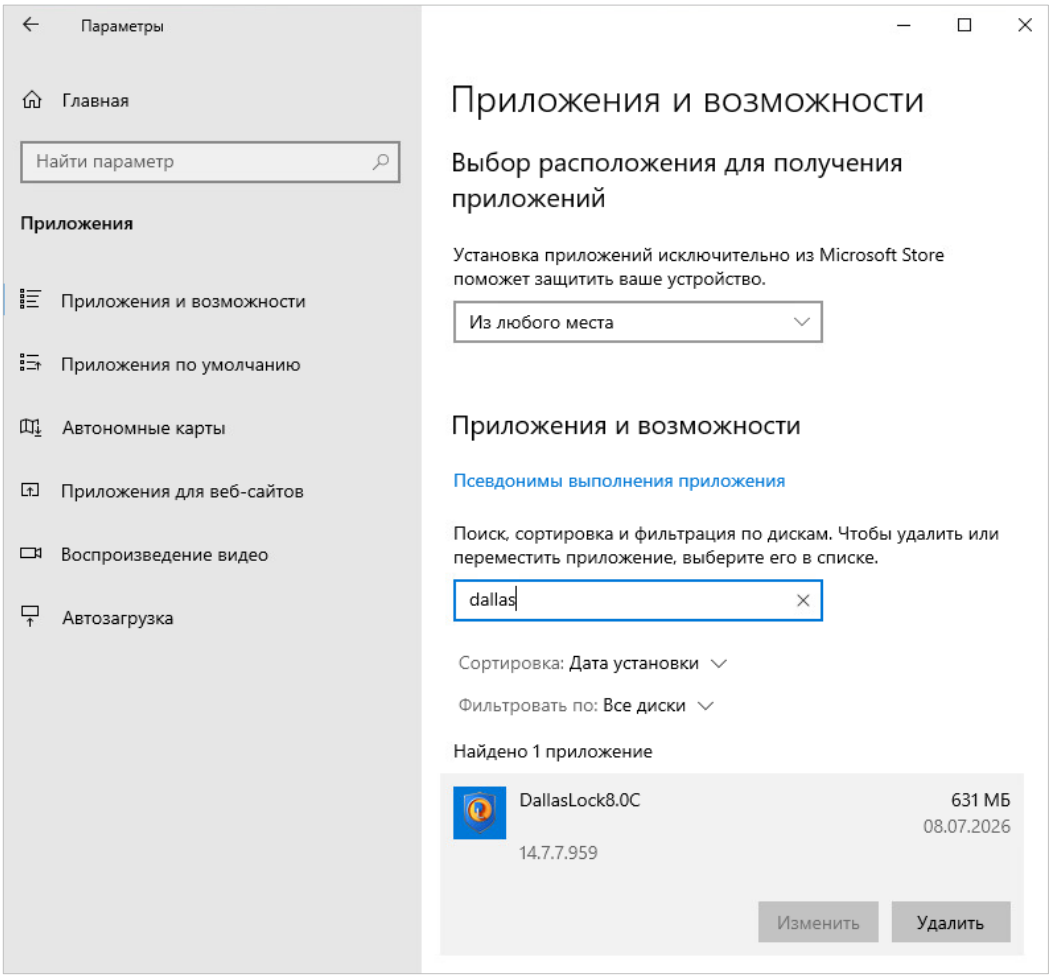


Рис. 8. Удаление Dallas Lock 8.0

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

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

1. При локальном удалении\обновлении **СЗИ** выводится сообщение об ошибке с информацией о том, что необходимо удалить преобразованные зоны (рис. 9).

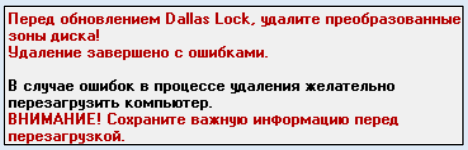


Рис. 9. Удаление Dallas Lock 8.0 с преобразованной зоной

2.4 Обновление системы защиты

Для защищенных **Dallas Lock 8.0** АРМ возможно обновление до последней сборки **Dallas Lock 8.0**, прошедшей испытания на соответствие требованиям по защите информации.

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

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

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

Обновление **Dallas Lock** на АРМ можно произвести под учетной записью, для которой выполняются следующие условия:

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

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

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

Для проверки наличия обновления необходимо выполнить следующие действия:

1. Открыть дополнительные функции кнопки главного меню[6] оболочки администратора и нажать кнопку **О программе**.
2. Нажать кнопку **Проверить обновление**.
3. Будет произведена проверка наличия обновления. В открывшемся окне будет отображено сообщение о результатах проверки.

Для получения и применения обновления необходимо выполнить действия, изложенные в п. 3.5 Формуляра RU.48957919.26.20.40.142.001 30.

2.5 О программе

Со следующими сведениями о **СЗИ** можно ознакомиться в информационном окне **О программе**, вызвав его из списка дополнительных функций кнопки главного меню[6]:

- полное наименование и редакция **СЗИ**;
- номер и дата сборки;
- номер лицензии;
- код технической поддержки;

[6] Внешний вид кнопки главного меню —  .

- дата завершения технической поддержки;
- количество терминальных сессий, подраздел 2.6.3 Ограничение количества терминальных сессий;
- активные компоненты (модули, на которые приобретена лицензия);
- адрес сайта компании разработчика;
- адрес сайта продуктовой линейки;
- адрес технической поддержки;
- номер телефона.

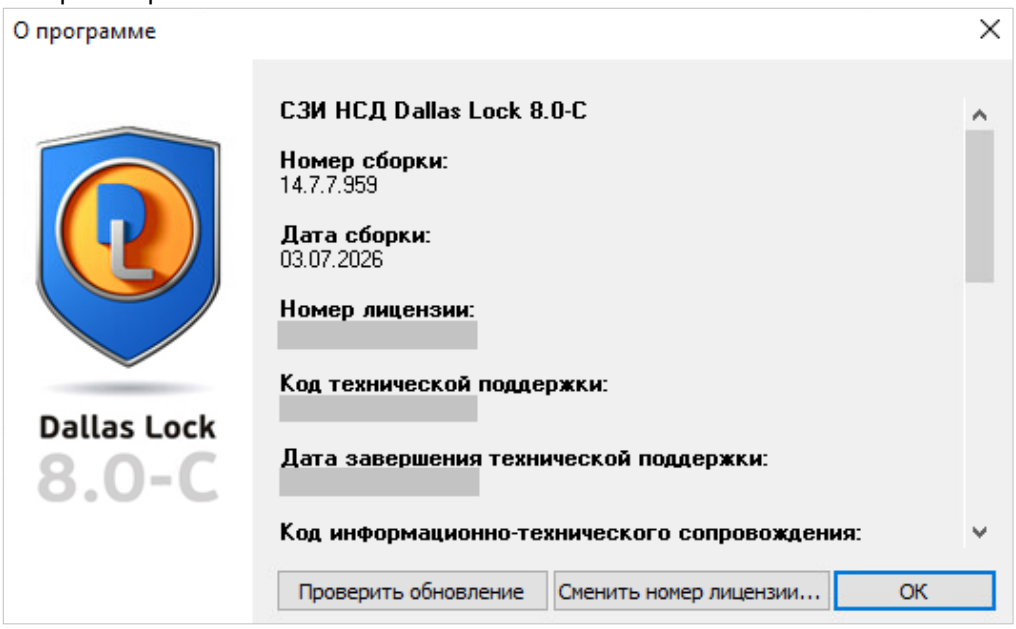


Рис. 10. Окно «О программе»

Процесс обновления **СЗИ** с помощью кнопки **Проверить обновление** описан в разделе 2.4 Обновление системы защиты.

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

Следует обратить внимание, что в случае ввода номера лицензии для изделия без модуля, который ранее был активирован, на экране появится предупреждение и соответствующий модуль будет деактивирован.

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

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

2.6 Вход на защищенный компьютер

При загрузке компьютера, защищенного **СЗИ**, в зависимости от ОС, появляется экран приветствия (приглашение на вход в систему) (рис. 11).

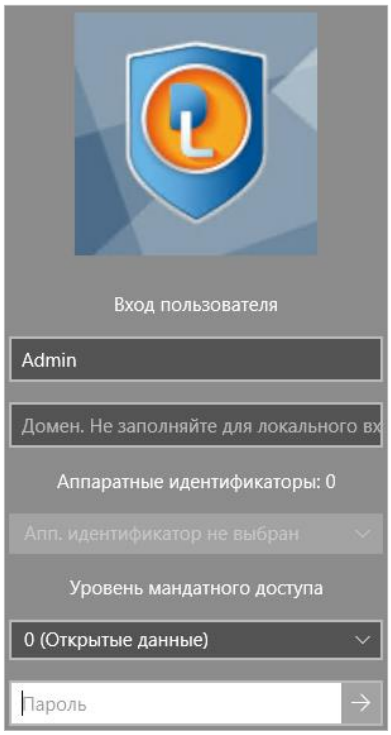


Рис. 11. Экран приветствия в ОС Windows 10

Для входа на защищенный **СЗИ** компьютер каждому пользователю предлагается выполнить следующую последовательность шагов:

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе. В зависимости от настроек системы защиты в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.
3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить (см. ниже).
4. Выбрать уровень доступа и (или) мандатную метку (если включен параметр **Выбор мандатной метки при входе в ОС**), назначенный пользователю администратором безопасности (только для Dallas Lock 8.0 редакции «С»).
5. Ввести пароль. При вводе пароля поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка).
6. При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
7. Нажать кнопку **Enter**.

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

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

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

2.6.1 Вход с использованием смарт-карт с сертификатом УЦ Windows

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

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

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

Для перехода к выбору входа по смарт-карте в ОС Windows 7 необходимо на экране приветствия нажать кнопку **Сменить пользователя**, после чего появится возможность выбрать тип входа. В ОС Windows 10 выбор типа входа отобразится внизу экрана слева (рис. 12).

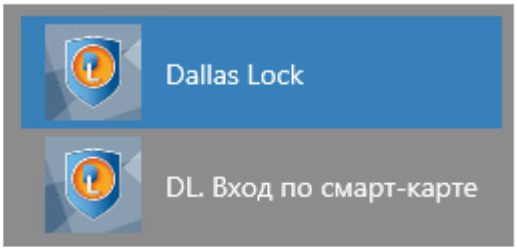


Рис. 12. Выбор типа входа в ОС Windows 10

При выборе входа по смарт-карте необходимо вставить смарт-карту в считывающее устройство, ввести PIN-код и нажать кнопку **Enter** (рис. 13).

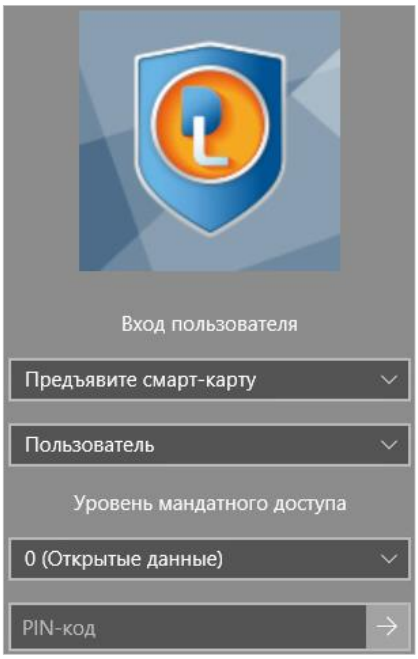


Рис. 13. Экран входа по смарт-карте в ОС Windows 10

2.6.2 Вход с аппаратным идентификатором

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

1. В зависимости от типа устройства предъявить идентификатор можно, вставив его в USB-порт или прикоснувшись к считывателю.
2. Необходимо выбрать наименование идентификатора из списка, который появится в выпадающем меню в поле *Аппаратные идентификаторы* (рис. 14).

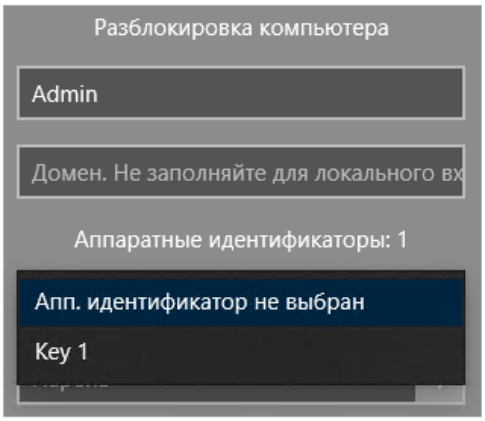


Рис. 14. Выбор аппаратного идентификатора при входе в ОС Windows

При подключении единственного идентификатора он будет выбран автоматически.

3. Далее в зависимости от настроек, произведенных администратором безопасности применительно к учетной записи пользователя, возможны следующие способы авторизации:

- выбор аппаратного идентификатора и заполнение всех авторизационных полей формы[7] (рис. 15);

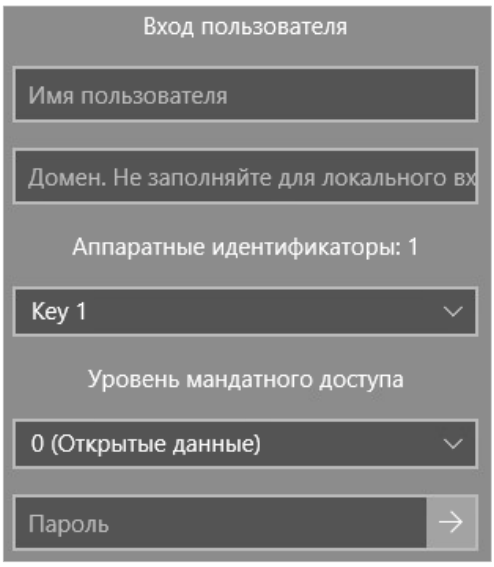
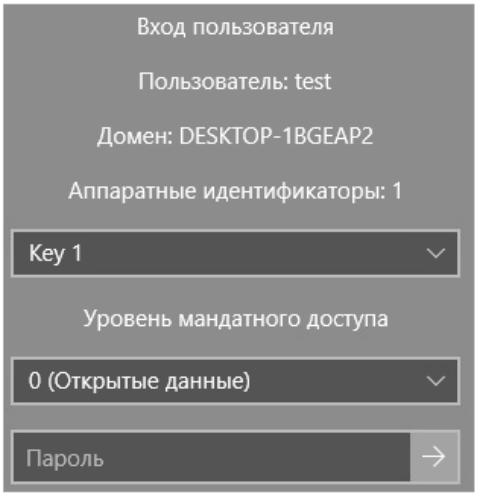


Рис. 15. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только пароля (логин автоматически считывается с идентификатора) (рис. 16);



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

Рис. 16. Поля авторизации после предъявления идентификатора

- выбор только аппаратного идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 17);

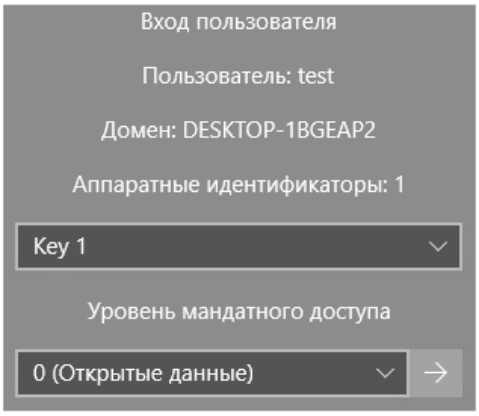


Рис. 17. Поля авторизации после предъявления идентификатора

- выбор аппаратного идентификатора и ввод только PIN-кода идентификатора (логин и пароль автоматически считываются с идентификатора) (рис. 18).

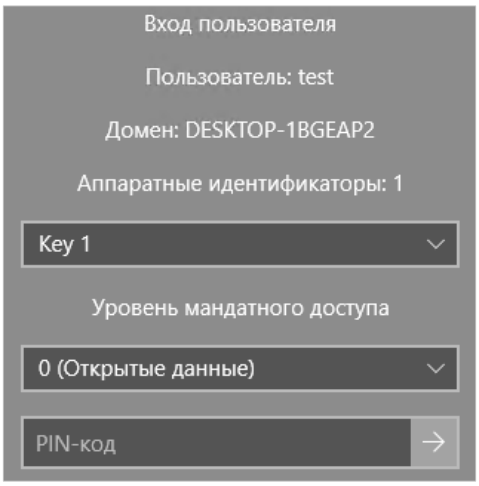


Рис. 18. Поля авторизации после предъявления идентификатора

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

- ввод PIN-кода и биометрических данных (рис. 19);

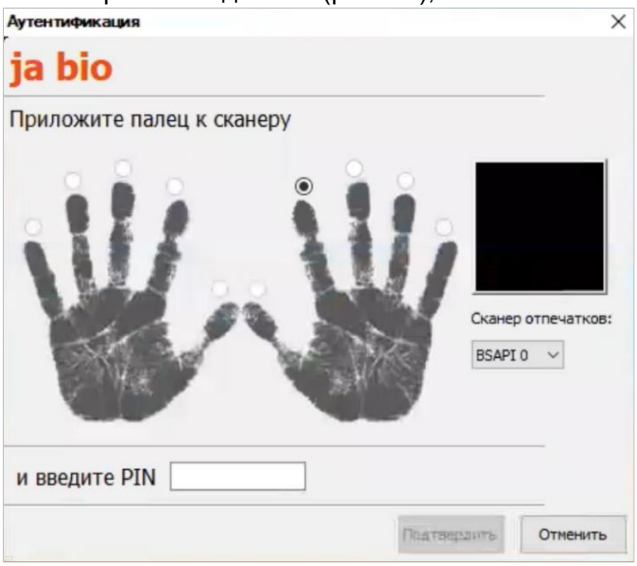


Рис. 19. Ввод авторизационных данных (PIN-код и биометрия)

- ввод PIN-кода или биометрических данных (рис. 20);

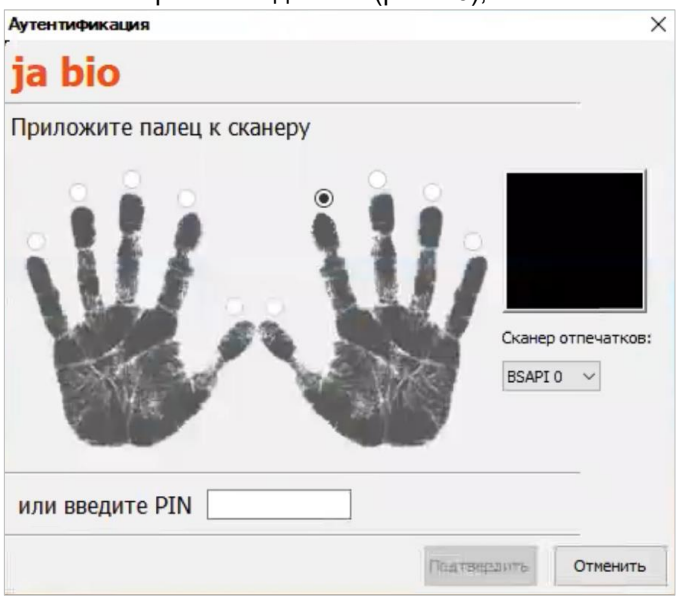


Рис. 20. Ввод авторизационных данных (PIN-код или биометрия)

- ввод только биометрических данных (рис. 21).



Рис. 21. Ввод авторизационных данных (биометрия)

2.6.3 Ограничение количества терминальных сессий

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

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

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

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

Допустимое количество терминальных сессий можно посмотреть в информационном окне «О программе», вызвав его из списка дополнительных функций кнопки главного меню[6], а также в любом сформированном отчете.

При использовании нескольких терминальных серверов рекомендуется использовать механизмы распределения терминальных сессий между ними, используя **ЕЦУ**.

При использовании **ЕЦУ** количество терминальных подключений и серверов определяется лицензией, записанной в файле. Ограничение на количество терминальных серверов указывает, сколько клиентов **Dallas Lock 8.0** может быть зарегистрировано в **ЕЦУ** в качестве терминальных серверов (подробнее об использовании **ЕЦУ** см. в документе «Инструкция по использованию ЕЦУ» RU.48957919.26.20.40.142.001 И6). Ограничение на количество терминальных сессий применяется только к клиентам **Dallas Lock 8.0**, зарегистрированным как терминальные серверы. Если клиент не зарегистрирован, количество терминальных сессий контролируется с помощью подключенного к клиенту аппаратного ключа или ограничивается двумя терминальными сессиями по умолчанию.

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

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

3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ

СЗИ состоит из программного модуля:

Название	Ярлык программы
Dallas Lock 8.0	

Для локальной настройки политик безопасности используется оболочка администратора **СЗИ** или контекстное меню объекта Windows Explorer. Для удаленной настройки используется оболочка сетевого администратора, раздел 11.5 Сетевое администрирование.

3.1 Администрирование Dallas Lock

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

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

Главное окно программы содержит следующие рабочие области (рис. 22).

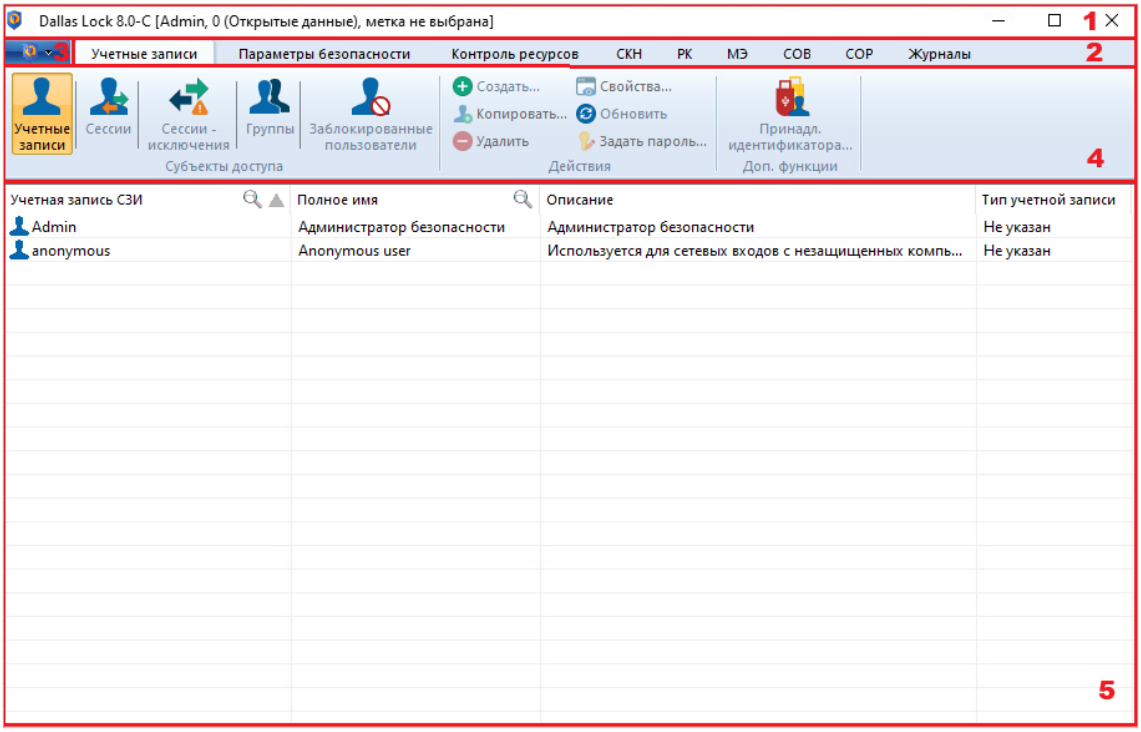


Рис. 22. Окно оболочки администратора системы защиты

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

Доступны следующие вкладки.

Учетные записи
Вкладка позволяет управлять учетными записями пользователей, создавать локальные группы и включать в них пользователей, просматривать список сессий (сеансов) учетных записей на

данном ПК, завершать активные сессии, контролировать список сессий-исключений, а также управлять списком заблокированных пользователей и определять принадлежность аппаратных идентификаторов.

Параметры безопасности

Вкладка позволяет осуществить настройку системы защиты в соответствии с требованиями. Вкладка содержит следующие категории:

- **Политики авторизации** — позволяют регулировать все настройки по входу на ЗАРМ и загрузке ОС. Эти настройки распространяются на всех зарегистрированных в системе защиты пользователей.
- **Политики аудита** — позволяют включать/отключать контроль за определенными действиями пользователей. Этот параметр регулирует ведение журналов.
- **Политики паролей** — устанавливают требования к созданию и использованию паролей, такие как их длина, сложность и срок действия.
- **Политики доступа** — позволяют настраивать параметры блокировки для ЗАРМ, устройств и расширений файлов.
- **Сеть** — настройки централизованного управления посредством **ЕЦУ Dallas Lock** и другие сетевые настройки.
- **Права пользователей** — (политики прав пользователей) позволяют присваивать права конкретному пользователю или группе пользователей.
- **Мандатный доступ** — позволяют переименовывать имеющиеся уровни доступа, а также создавать и переименовывать мандатные метки (только для Dallas Lock 8.0 редакции «С»).
- **Очистка остаточной информации** — настройка параметров очистки.
- **Политики контроля целостности** — позволяют управлять проверкой установленной целостности объектов ФС, программно-аппаратной среды и веток реестра.
- **Изолированные процессы** — позволяют управлять списком процессов, работа с которыми должна быть изолирована, исключить возможность копирования информации через буфер обмена.
- **Загрузчик DL** — позволяет настраивать модуль загрузчика DL и управлять прозрачным преобразованием жестких дисков (только для Dallas Lock 8.0 редакции «С»).

Контроль ресурсов

Вкладка позволяет контролировать объекты ФС и устройства, для которых установлены механизмы разграничения доступа, аудита и целостности. Данная вкладка позволяет управлять следующими типами ресурсов:

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

Также на данной вкладке для каждого типа ресурсов возможно выбрать определенный фильтр по типу контроля объектов:

- **Дискреционный доступ** — позволяет просмотреть список объектов ФС, на которые назначены права дискреционного доступа. В свойствах каждого объекта можно просмотреть, для каких пользователей или групп какие права назначены. Фильтр доступен для всех типов ресурсов.
- **Мандатный доступ** — позволяет просмотреть список объектов ФС, на которые назначен мандатный доступ (только для Dallas Lock 8.0 редакции «С»). Фильтр доступен для типов ресурсов *ФС* и *Устройства*.
- **Аудит** — позволяет просмотреть список объектов ФС, на которые назначен аудит. В свойствах объектов из списка можно просмотреть, на какие конкретно события назначен аудит. Фильтр доступен для всех типов ресурсов, кроме аппаратных идентификаторов.
- **Контроль целостности** — позволяет просмотреть список объектов ФС, на которые

установлен контроль целостности. Отображается также алгоритм расчета. При нажатии кнопки **Проверить** отображается эталонная контрольная сумма, хранимая в базе данных **СЗИ**. При нажатии **Пересчитать** — расчетная. Фильтр доступен для типов ресурсов *ФС* и *Реестр*.

СКН

Вкладка (только в Dallas Lock 8.0 с модулем СКН) позволяет управлять и преобразовывать съемные накопители. Эта вкладка содержит следующие категории:

- **Съемные накопители** — позволяет управлять дескрипторами на съемных накопителях (права доступа, аудит и контроль целостности для съемных накопителей выделены в отдельную категорию).
- **Описание для съемных накопителей** — описание задается для удобства администрирования.
- **Преобразование съемных накопителей** — позволяет управлять ключами преобразования и преобразовывать съемные накопители.

РК

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

МЭ

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

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

СОВ

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

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

СОР

Вкладка (только в Dallas Lock 8.0 с модулем СОР) позволяет настраивать собственные

индикаторы компрометации, добавлять правила реагирования, отображает информацию и настройку **COP**. Эта вкладка содержит следующие категории:

- **Параметры COP** — позволяет регулировать обновления, добавлять области сканирования, настраивать расписание сканирования, а также отключать правила реагирования.
- **IoC** — позволяет управлять индикаторами компрометации. По умолчанию содержит готовые шаблоны наиболее типовых индикаторов компрометации, присутствует возможность включать определенные индикаторы компрометации или добавлять собственные.
- **IoA** — позволяет управлять индикаторами атаки. По умолчанию содержит готовые шаблоны наиболее типовых индикаторов атаки, присутствует возможность активировать и деактивировать инидикаторы.
- **Правила реагирования** — позволяет управлять правилами автоматического реагирования.
- **Отчеты** — позволяет отслеживать события связанные с индикаторами компрометации.
- **Обновления** — позволяет посмотреть версию обновления базы индикаторов компрометации.
- **Блокировки** — позволяет управлять заблокированными процессами.

Журналы

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

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

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

3.2 Панель действий

Панель инструментов (действий) в **Dallas Lock 8.0** для всех категорий содержит набор типовых действий по добавлению, удалению, редактированию, обновлению параметров и другие (рис. 23).

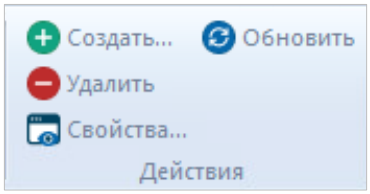


Рис. 23. Панель инструментов

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

3.3 Контекстное меню объектов

СЗИ предоставляет возможность управлять безопасностью любого объекта ФС. После установки системы защиты у каждого объекта ФС в контекстном меню появляются дополнительные пункты: **DL8.0: Права доступа**, **DL8.0: Преобразование**, **DL8.0: Удалить и зачистить, DL8.0: Запустить в безопасной среде** (рис. 24), подробный механизм каждого из которых описан в соответствующих разделах данного руководства.

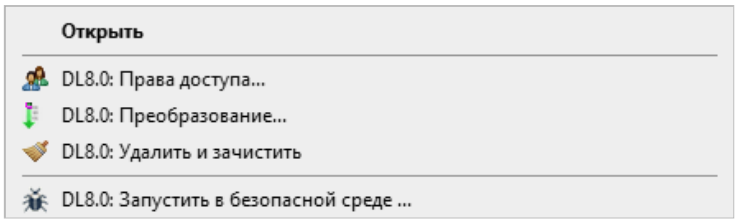


Рис. 24. Контекстное меню объекта ФС

Для таких объектов как преобразованные файл-диски, в контекстном меню дополнительно будет присутствовать пункт **DL8.0: Подключить преобразованный файл-диск**, раздел 12.3 Преобразованные файл-диски.

3.4 Сортировка списка параметров

Каждая рабочая область любой категории параметров содержит списки параметров или объектов текущей категории. Для удобства работы эти списки можно отсортировать, для чего необходимо кликнуть поле, содержащее название столбца и значок сортировки (треугольник) (рис. 25).

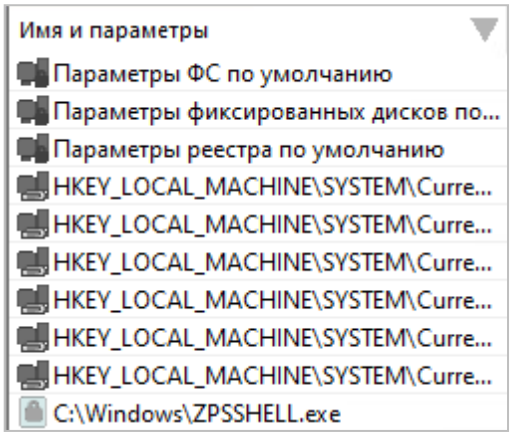


Рис. 25. Сортировка списка параметров

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

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

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

Для некоторых параметров на рабочей области реализована функция поиска по столбцам (рис. 26).

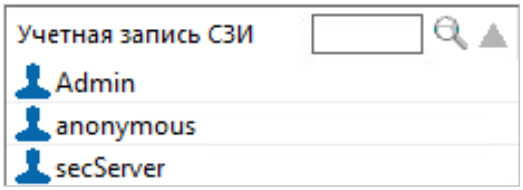


Рис. 26. Поиск значения в столбце

3.5 Значок блокировки на панели задач

После установки **СЗИ** на панели задач ОС у всех пользователей АРМ присутствует значок блокировки компьютера **BlockIcon**.

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

Также у этого значка есть контекстное меню, из которого можно запустить оболочку администратора, просмотреть свойства текущего пользователя и выполнить действия с преобразованными файл-дисками (рис. 27).

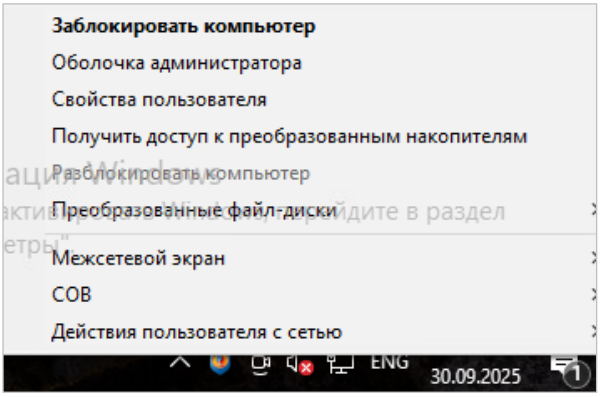


Рис. 27. Контекстное меню значка блокировки

Выбор свойств пользователя из контекстного меню откроет окно с информацией о текущем пользователе компьютера (рис. 28).

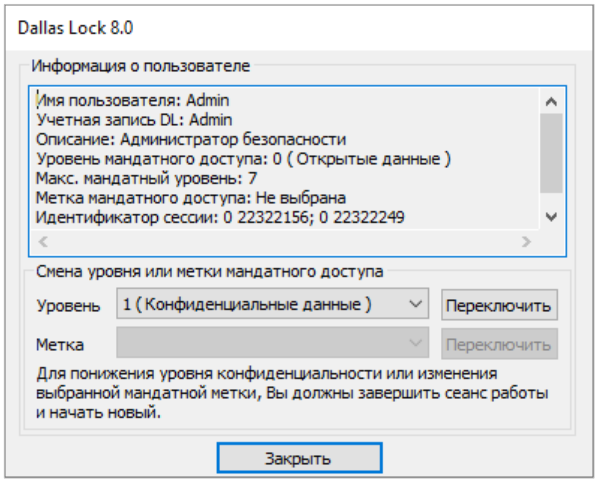


Рис. 28. Окно свойств пользователя, вызванное с помощью значка блокировки

В **Dallas Lock 8.0** редакции «С» с помощью данного окна текущему пользователю можно повысить уровень мандатного доступа, подраздел 5.3.7 Текущий уровень и метка доступа пользователя.

3.6 Полномочия пользователей на администрирование системы защиты

В **СЗИ** полномочия на эксплуатацию и администрирование системы защиты определяются статусом пользователя.

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

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

Отдельно выделяется учетная запись пользователя, выполнившего установку системы

Dallas Lock 8.0. Этот пользователь условно называется *суперадминистратором*, имеет неограниченные административные права и возможности в настройке системы.

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

Полномочия *администратора* по управлению работой системы защиты могут быть следующими:

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

3.6.1 Порядок предоставления полномочий

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

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

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

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



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

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

Для предоставления пользователю какого-либо полномочия на администрирование необходимо в оболочке администратора на вкладке основного меню *Параметры безопасности* открыть категорию **Права пользователей**. Главное окно программы будет иметь следующий вид (рис. 29):

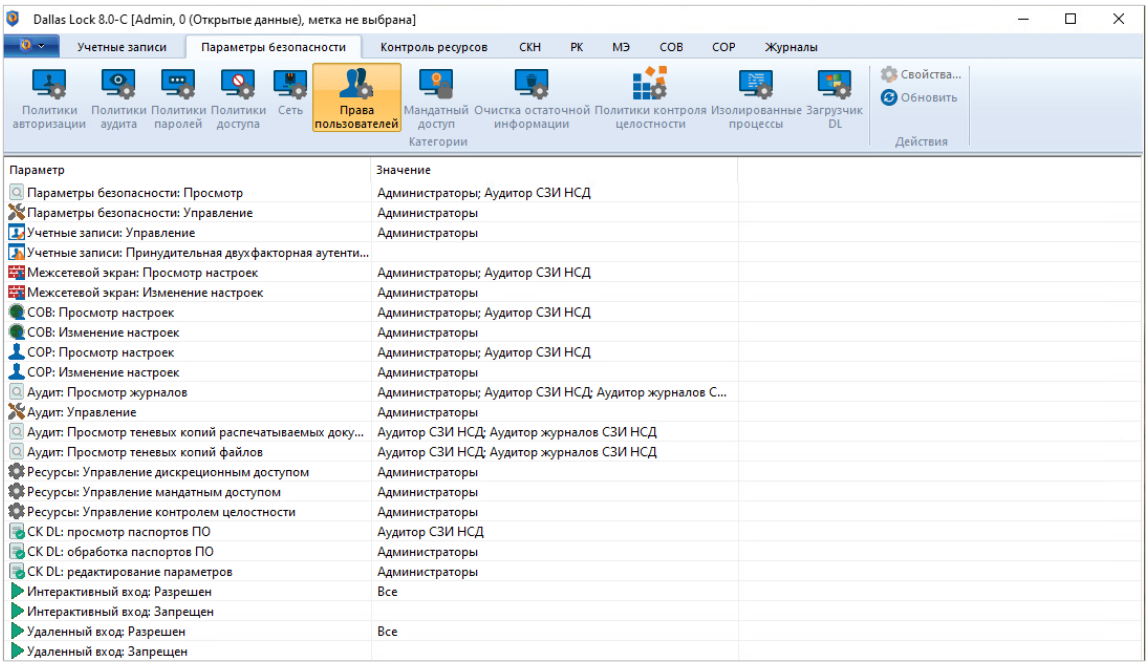


Рис. 29. Окно редактирования прав пользователей на администрирование

В основном окне данной категории перечислены все полномочия, которые могут быть предоставлены пользователям. Чтобы предоставить пользователю необходимое право, нужно дважды щелкнуть на строке с полномочием, либо выделить строку и нажать кнопку **Свойства** на панели **Действия**. Откроется окно добавления учетных записей пользователей и групп (рис. 30).

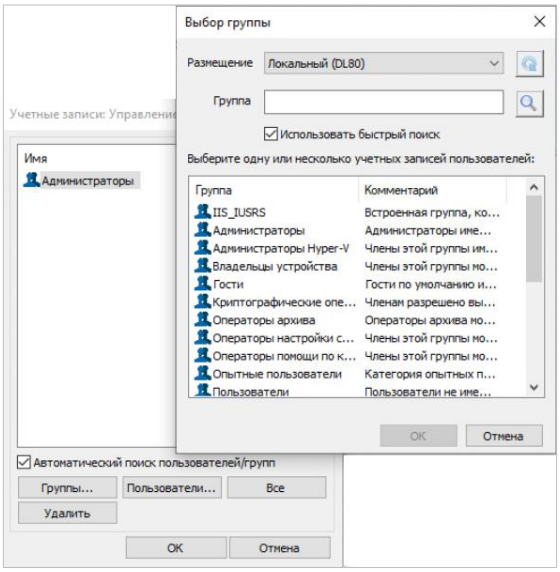


Рис. 30. Назначение пользователей

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

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

3.6.2 Полномочия на просмотр параметров безопасности

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

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

автоматически.

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

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

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

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

3.6.3 Полномочия на управление параметрами безопасности

Данные полномочия позволяют изменять параметры безопасности **СЗИ**.

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

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

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

3.6.4 Полномочия на управление дискреционным доступом

Дискреционный доступ подробно рассмотрен в главе 5 Разграничение доступа к объектам ФС данного руководства. Дискреционный доступ основывается на предоставлении пользователю прав на определенные операции с объектами ФС.

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

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

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

3.6.5 Полномочия на управление мандатным доступом

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

Мандатный доступ подробно рассмотрен в главе 5 Разграничение доступа к объектам ФС данного руководства. Данной политикой пользователю предоставляются полномочия на управление мандатным доступом.

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

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

3.6.6 Полномочия на управление контролем целостности

Механизм контроля целостности подробно рассмотрен в главе 9 Подсистема обеспечения целостности данного руководства. Предоставление пользователю полномочий на управление контролем целостности позволяет назначить или отменить контроль целостности любому объекту ФС.

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

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

3.6.7 Полномочия на деактивацию системы защиты

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

Процесс удаления описан в разделе 2.3 Удаление системы защиты. По умолчанию этим правом обладает только пользователь, установивший систему (администратор безопасности или суперадминистратор). Для назначения данного права другим пользователям необходимо выбрать параметр **Деактивация системы защиты**.

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



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

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

4 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ

4.1 Управление учетными записями

В **Dallas Lock 8.0** возможна регистрация пользователей следующих видов:

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

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

Для просмотра и редактирования учетных записей пользователей в оболочке администратора системы защиты необходимо выбрать вкладку *Учетные записи* (рис. 31):

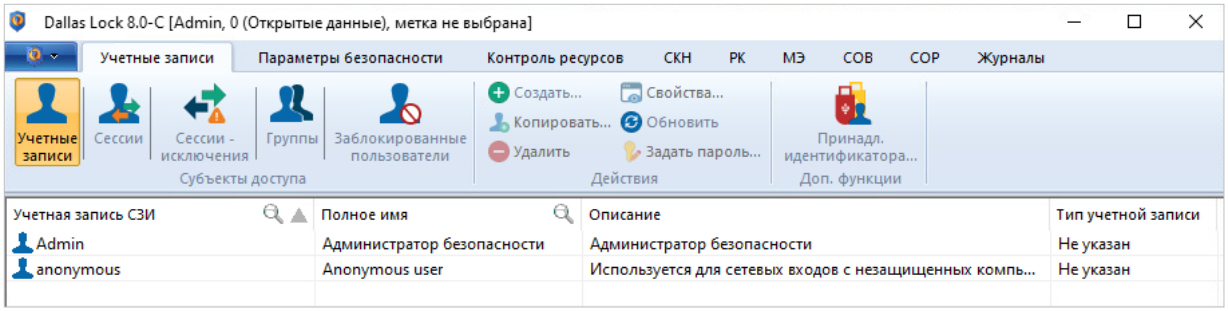


Рис. 31. Вкладка Учетные записи

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

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

- *суперадминистратор* — учетная запись пользователя, установившего **СЗИ** (запись невозможно удалить из системы).
- *anonymous* — учетная запись для проверки входов с незащищенной системой машин (запись невозможно удалить из системы, но можно отключить, при этом следует помнить, что учетная запись anonymous на контроллере домена всегда должна быть включена).
- ** — специальная учетная запись, разрешающая всем доменным пользователям вход на защищенный системой компьютер, подраздел 4.1.3 Регистрация доменных пользователей. Создается только на ПК, которые в момент установки **СЗИ** входят в домен AD. Запись можно удалить или отключить.

Зарегистрированные, но отключенные учетные записи выделяются иконкой .

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

4.1.1 Полномочия на управление учетными записями

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

Полномочиями для создания, удаления и изменения учетных записей пользователей в системе защиты обладают: суперадминистратор и пользователи (группы пользователей), указанные в списке разрешенных параметра **Учетные записи: Управление** на вкладке **Права пользователей** (рис. 32). По умолчанию это администраторы.

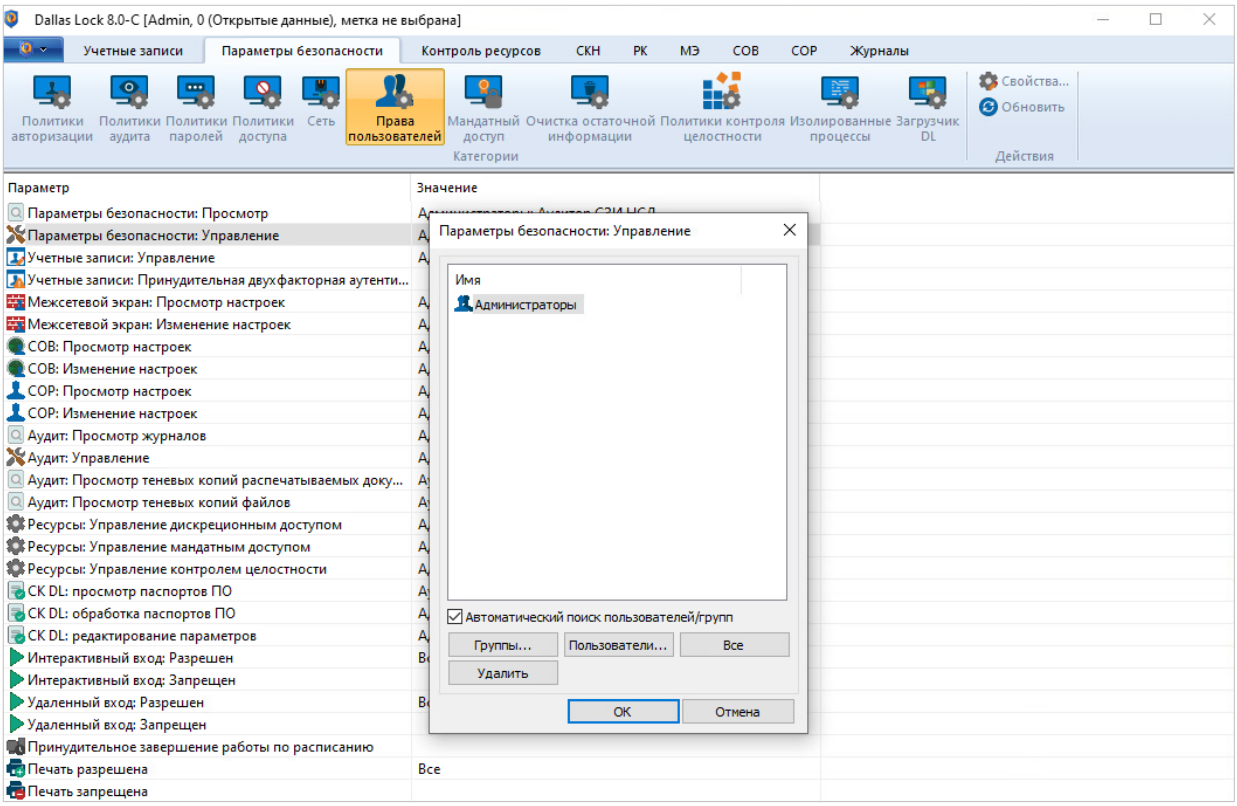


Рис. 32. Параметр, определяющий полномочия на управление учетными записями

4.1.2 Создание и удаление локальных пользователей

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

Создание пользователей

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

Для создания нового пользователя в системе защиты необходимо:

1. Выделить категорию **Учетные записи** в оболочке администратора.
2. Нажать кнопку **Создать** в категориях **Действия** или выбрать соответствующую из контекстного меню, нажав правую кнопку мыши.
3. На экране появится окно создания новой учетной записи (рис. 33).

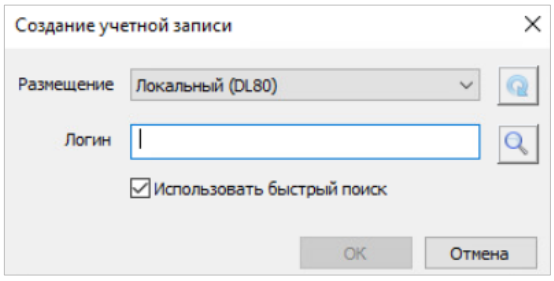


Рис. 33. Окно создания учетной записи

4. В поле *Размещение* необходимо выбрать значение *Локальный*.
5. В поле *Логин* необходимо ввести логин (имя) регистрируемого пользователя. При вводе имени в системе существуют следующие правила:
   - максимальная длина имени — 20 символов;
   - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных ОС: " / \ [ ] : | < > + = ; , ? @ *);

- разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть прописные и строчные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

Кнопка поиска, расположенная рядом с полем логина, разворачивает список учетных записей пользователей, зарегистрированных в ОС данного ПК, и позволяет выбрать пользователя из уже существующих (рис. 34).

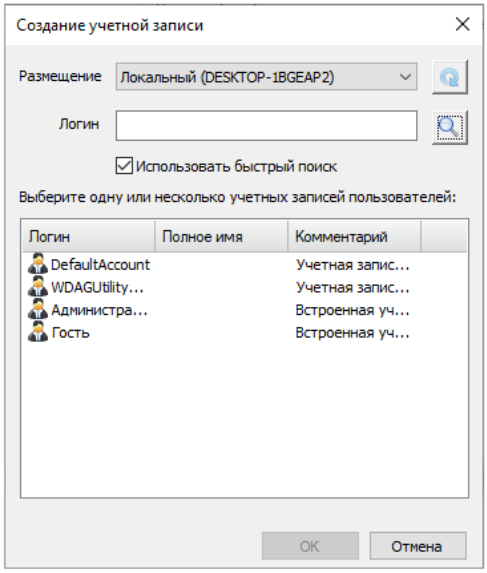


Рис. 34. Учетные записи, зарегистрированные в ОС компьютера

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

6. После нажатия **OK** появится окно редактирования параметров учетной записи (рис. 35).

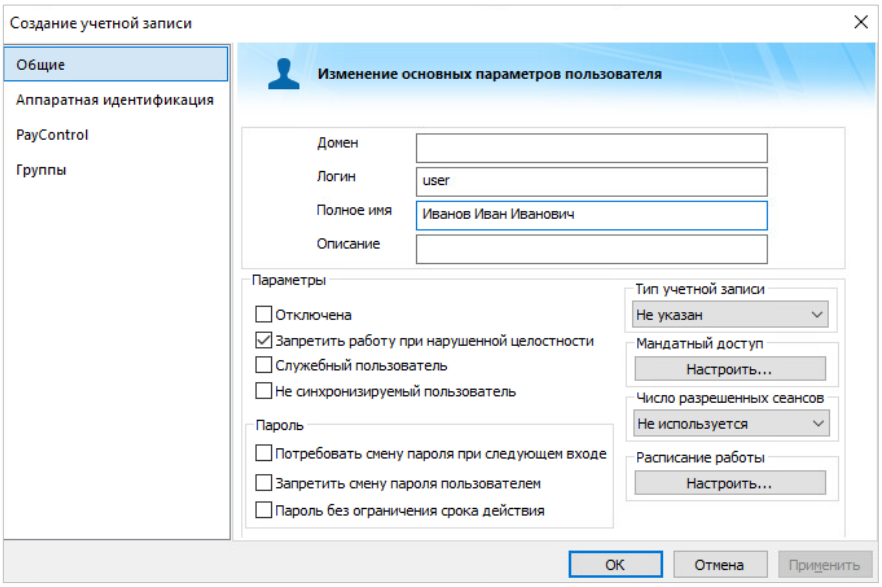


Рис. 35. Окно редактирования параметров новой учетной записи

На вкладке *Общие* предлагается заполнить следующие учетные данные и параметры:

- Заполнить *Полное имя* пользователя.
- В поле *Описание* ввести любой комментарий. Длина комментария не более 256 символов. Вводить комментарий и полное имя не обязательно.
- Политики *Отключена* и *Запретить работу при нарушенной целостности* задаются при необходимости:
    a. Администратор имеет возможность отключить учетную запись любого пользователя, после чего пользователь не сможет войти на ЗАРМ до тех пор, пока администратор не деактивирует эту опцию.

b. Система защиты обеспечивает проверку целостности программно-аппаратной среды ПК, объектов ФС и реестра. Если для пользователя опция «Запретить работу при нарушении целостности» активизирована, то при обнаружении нарушения целостности выдается соответствующее предупреждение и вход в ОС блокируется до тех пор, пока администратор не разблокирует учетную запись. Если же эта опция не включена, то при обнаружении нарушения целостности будет отображено только предупреждение.

- Флаг в поле *Служебный пользователь* предоставляет данной учетной записи особый статус, подраздел 5.3.8 Служебный пользователь.
- Необходимо выбрать *Тип учетной записи***.** Для типа *Временный* обязательным условием является настройка расписания работы пользователя (см. ниже). По умолчанию тип учетной записи будет иметь значение *Не указан*.
- Необходимо выбрать уровень доступа для пользователя в поле *Мандатный доступ* (только для Dallas Lock 8.0 редакции «С»)**,** под которым пользователь сможет работать, раздел 5.3 Мандатный доступ.
- Необходимо выбрать значение в поле *Число разрешенных сеансов*, подраздел 4.1.6 Число разрешенных сеансов.
- Необходимо задать *Расписание работы* пользователя, выбрать период и время. Вне указанного периода пользователь не сможет зайти на АРМ. По окончании времени работы ПК пользователя будет заблокирован при условии включения параметра безопасности **Принудительное завершение работы по расписанию** (**Параметры безопасности** → **Права пользователей**).

В **Dallas Lock 8.0** реализована функциональная возможность создания нескольких пользователей, используя символ «;» в качестве разделителя. При вводе логины пользователей указываются без пробела.
При назначении имени и параметров, данные будут автоматически применены ко всем пользователям, аналогично добавлению пользователей в группы. При этом пароль назначается каждому пользователю индивидуально.

Расписание работы пользователя может быть определено с дискретностью 30 минут.

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

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

Далее, в процессе создания или регистрации нового локального пользователя администратор имеет возможность включить его в определенную группу. В окне закладки *Группы* отображены названия групп, в которые включен пользователь (рис. 36). По умолчанию каждый новый пользователь входит в группу *Пользователи*.

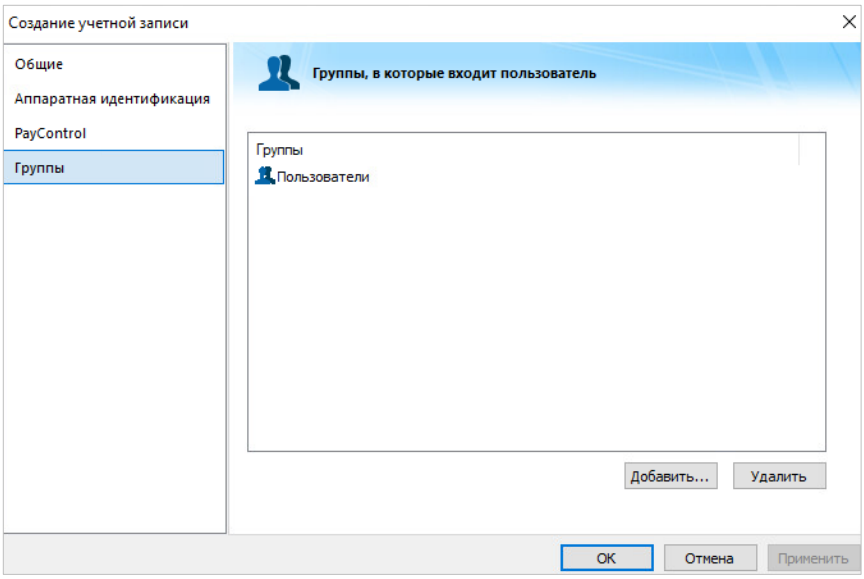


Рис. 36. Окно редактирование списка групп пользователя

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

7. Чтобы включить пользователя в определенную группу, необходимо нажать **Добавить**. Появится список всех групп пользователей, имеющихся в системе (кроме тех, в которые пользователь уже включен) (рис. 37).

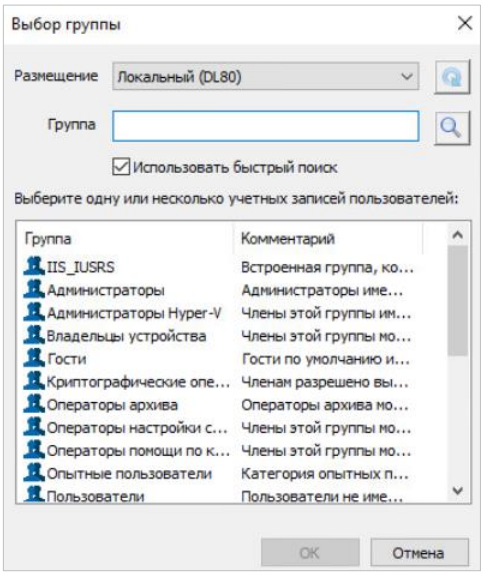


Рис. 37. Окно выбора групп для учетной записи

8. В поле *Размещение* необходимо оставить значение *Локальный*. В списке групп нужно выбрать необходимую. Одновременно можно выделить несколько групп в списке.

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

9. Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания учетной записи и нажатия кнопки **ОК** (рис. 38).

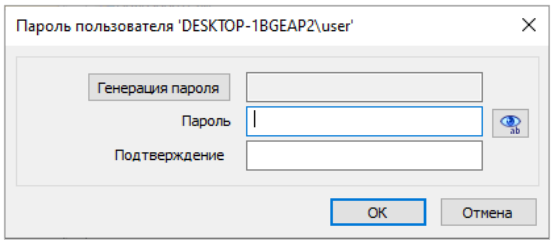


Рис. 38. Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- максимальная длина пароля составляет 31 символ;
- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности **Необходимо наличие спецсимволов**, подраздел 4.5.3 Настройка политик паролей;
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором, подраздел 4.5.3 Настройка политик паролей.

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

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

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

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

Также следует учесть, если учетная запись (в том числе в составе группы) отмечена в значении для параметра **Учетные записи: Принудительная двухфакторная аутентификация**, то присвоение аппаратного идентификатора станет обязательным условием, иначе при завершении ее регистрации или редактировании в **СЗИ** появится предупреждение об ошибке, подраздел 4.3.3 Принудительная двухфакторная аутентификация. Это правило распространяется для вновь создаваемых учетных записей пользователей.

Удаление пользователей

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

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

Создание учетной записи путем копирования

При создании учетной записи пользователя, которая имеет одинаковые свойства с другой учетной записью, можно воспользоваться функцией копирования. Для этого необходимо выбрать учетную запись в списке и нажать **Копировать** на панели действий (рис. 39).

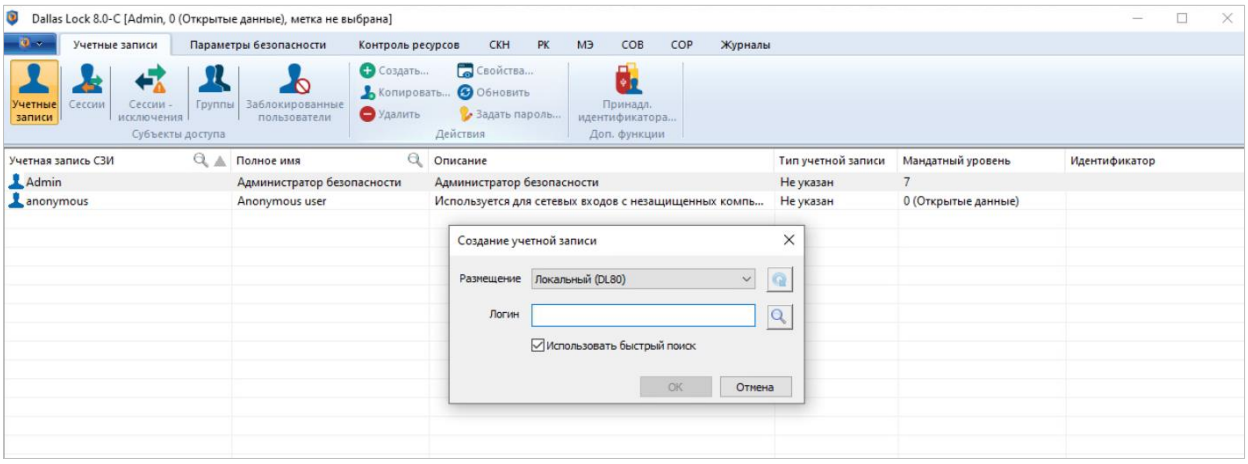


Рис. 39. Создание новой учетной записи с копированием свойств уже созданной

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

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

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

4.1.3 Регистрация доменных пользователей

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

1. Получить список доменных пользователей. Для этого, при создании учетной записи, в выпадающем меню размещения необходимо выбрать имя домена и нажать кнопку поиска (рис. 40).

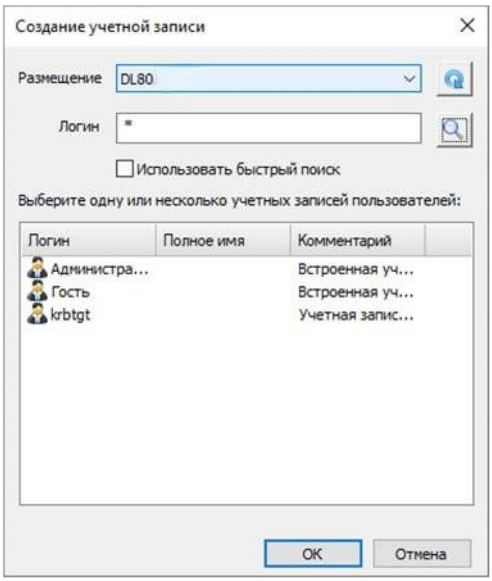


Рис. 40. Заполнение имени учетной записи

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

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

В системе защиты автоматически сформируется учетная запись пользователя с теми параметрами, которые соответствуют ей на контроллере домена (имя домена, логин, пароль, полное имя,

название групп на контроллере домена). Автоматически учетная запись пользователя в списке учетных записей будет иметь вид: *имя домена/имя пользователя*.

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

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

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

По умолчанию используется алгоритм быстрого поиска учетных записей. При определенных настройках Active Directory данный алгоритм вследствие отсутствия необходимых привилегий может возвращать неполный список доменных учетных записей.
В этом случае необходимо выключить опцию *Использовать быстрый поиск*. Время выполнения операции увеличится, однако при этом гарантируется, что все учетные записи будут найдены и отображены.

С зарегистрированными в **СЗИ** доменными пользователями можно проводить любые операции по реализации политик безопасности, однако нельзя менять пароль средствами системы. При попытке изменить пароль будет выведено предупреждение (рис. 41).



Рис. 41. Сообщение системы при попытке смены пароля

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

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

4.1.4 Регистрация доменных учетных записей по маске

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

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

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

По такой маске возможна регистрация только доменных учетных записей, для локальных это невозможно, и каждая запись должна быть создана отдельно.

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

Механизм регистрации доменных учетных записей системы с использованием масок позволяет

привести систему входа к строгому виду.

Каждая учетная запись может быть в состоянии *вход разрешен* и *вход запрещен*. Чтобы запретить вход под соответствующей учетной записью, необходимо, чтобы был поставлен флаг в поле *Отключена* в окне параметров учетных записей (рис. 42).

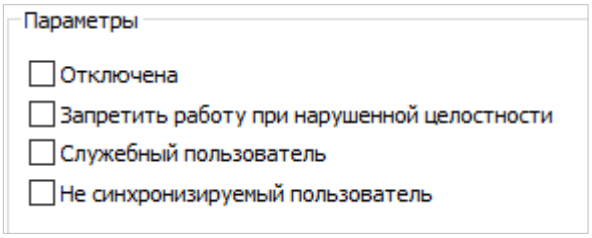


Рис. 42. Параметры учетной записи

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

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

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

4.1.5 Создание и удаление групп пользователей

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

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

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

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

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

При установке **Dallas Lock 8.0** по умолчанию реализовано автоматическое создание двух групп пользователей с предустановленными правами: группа **Аудитор СЗИ НСД** и группа **Аудитор журналов СЗИ НСД**, подраздел 6.1.2 Полномочия на просмотр и управление параметрами аудита.

В главном окне оболочки администратора вкладка *Группы* имеет следующий вид (рис. 43):

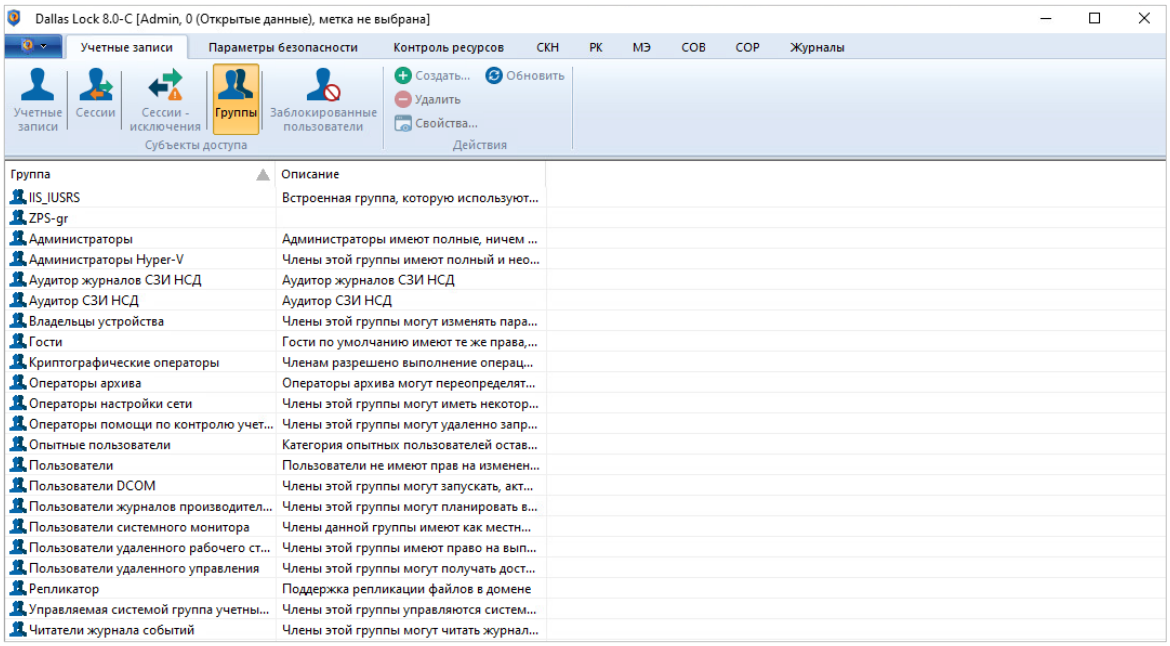


Рис. 43. Общий вид закладки «Группы»

Для создания новой группы необходимо:

1. В разделе **Группы** на вкладке *Учетные записи* нажать **Создать** (или выбрать данное действие из контекстного меню). Откроется окно, содержащее две вкладки: *Общие* и *Пользователи*. Вкладка *Общие* имеет два поля: *Группа, Описание* (рис. 44).

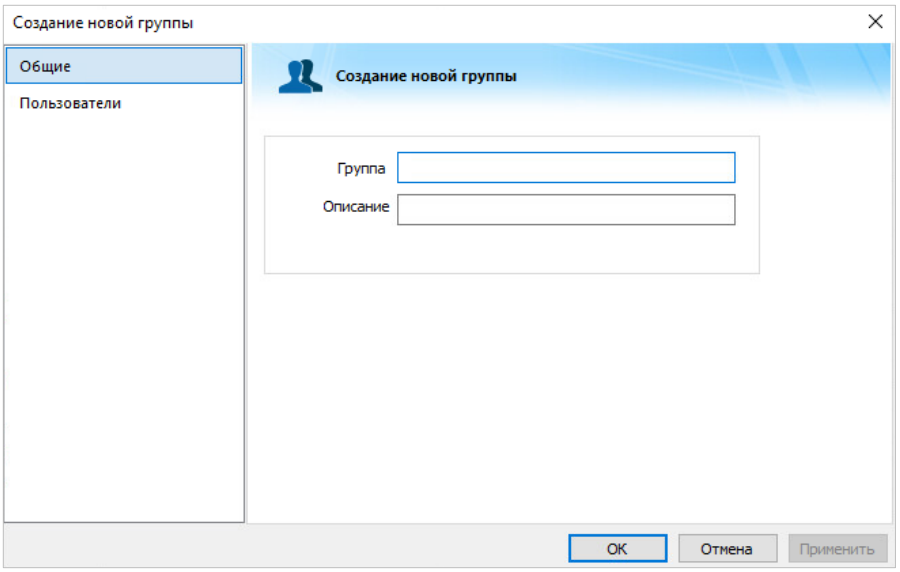


Рис. 44. Окно создания новой группы

2. В поле *Группа* следует ввести название группы, в поле *Описание* — назначение группы или комментарий (необязательное поле). Нажать **Применить**.
3. На вкладке *Пользователи* можно добавить/удалить пользователей, входящих в группу. Для добавления пользователя в группу необходимо нажать **Добавить**. Откроется дополнительное окно (Рис. 45).

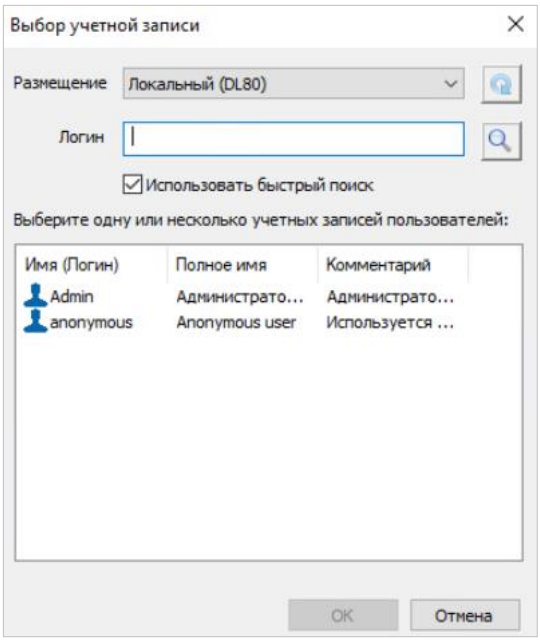


Рис. 45. Выбор учетной записи для добавления в группу

4. В поле *Логин* следует ввести имя учетной записи, для ускоренного поиска включить чекбокс *Использовать быстрый поиск*, выбрать нужные учетные записи и нажать **ОК**.
5. В окне *Создание новой группы* нажать **Применить** и **ОК**.

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

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

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

4.1.6 Число разрешенных сеансов

При настройке свойств учетной записи имеется возможность определить число разрешенных сеансов для данной учетной записи (рис. 46).

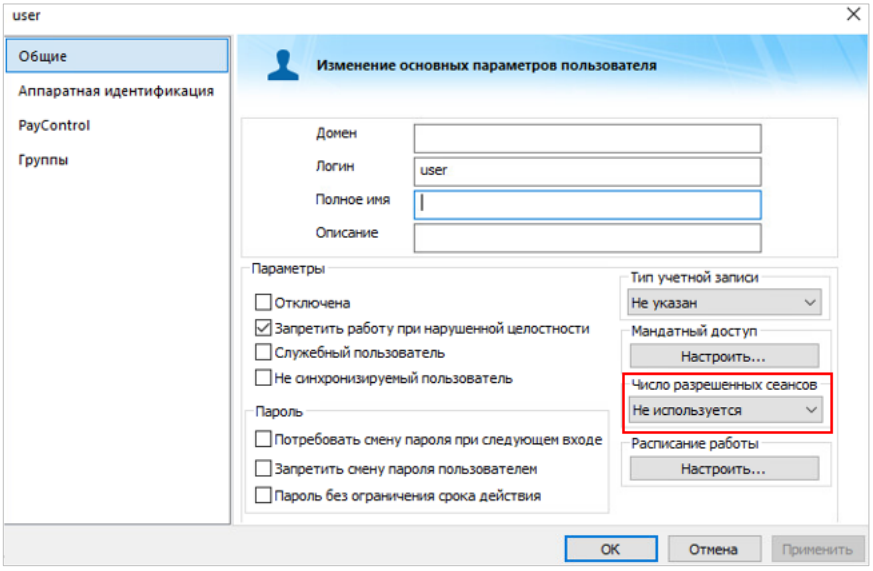


Рис. 46. Свойства учетной записи. Параметры сеансов доступа

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

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

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

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

4.1.7 Смена пароля пользователя

Смена пароля средствами ОС

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

1. После входа в ОС пользователю необходимо нажать комбинацию клавиш **Ctrl+Alt+Del** и в списке операций выбрать **Изменить пароль**.

   На экране появится диалоговое окно с полями для заполнения (рис. 47).

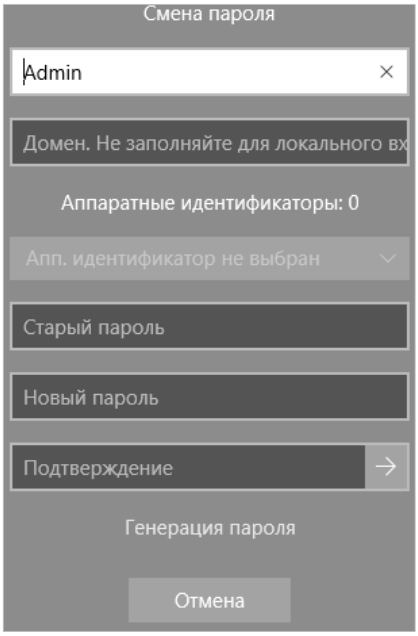


Рис. 47. Поля заполнения при смене пароля

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

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

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

В соответствии с политиками безопасности в системе могут быть включены настройки сложности

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

Смена пароля с помощью оболочки администратора

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

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

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

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

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

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

4.1.8 Сессии-исключения

Для корректной работы в режиме совместимости со сторонним ПО в **Dallas Lock 8.0** реализован механизм регистрации сессий, которым в качестве исключения разрешается работа с ФС, несмотря на отсутствие явного санкционированного входа.

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

Чтобы просмотреть список сессий-исключений и добавить новые, необходимо в оболочке администратора на вкладке *Учетные записи* раскрыть категорию **Сессии-исключения** (рис. 48).

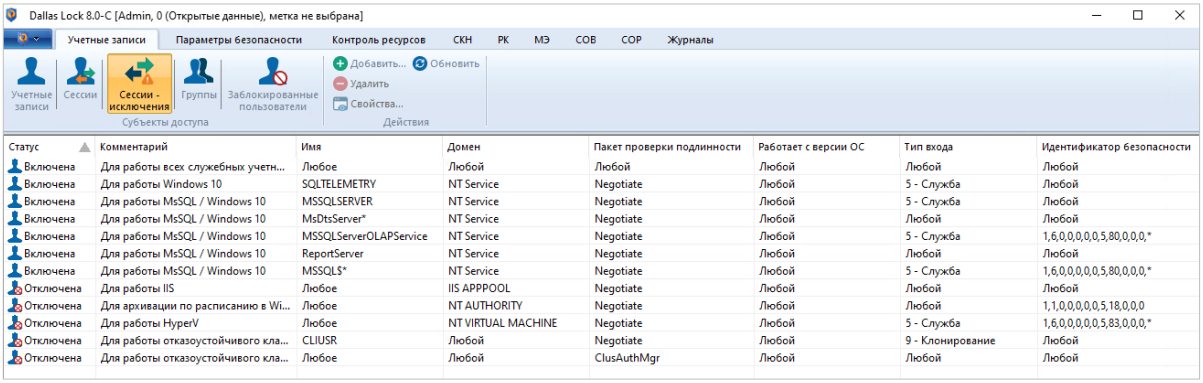


Рис. 48. Окно со списком сессий для работы ПО

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

Добавленную в список сессию можно временно отключить, не удаляя из списка, и заново включить. Для этого в окне параметров сессии необходимо отметить флагом поле *Исключение активно* (рис. 49).

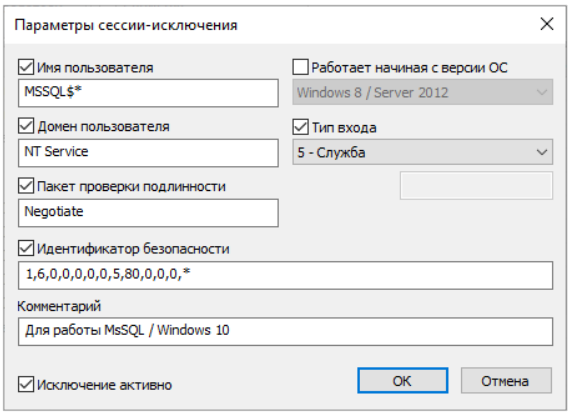


Рис. 49. Редактирование параметров сессии-исключения

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

4.2 Заблокированные пользователи

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

Чтобы открыть список заблокированных пользователей, необходимо на вкладке основного меню *Учетные записи* выбрать категорию **Заблокированные пользователи** (рис. 50).

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

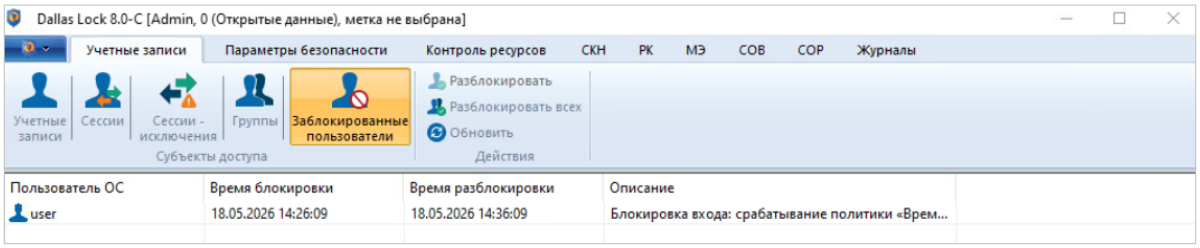


Рис. 50. Действия со списком заблокированных пользователей

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

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

4.3 Аппаратная идентификация пользователя

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

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

4.3.1 Назначение аппаратной идентификации

Перед назначением аппаратного идентификатора следует:

1. Установить драйвер соответствующего идентификатора (установка драйверов возможна как перед установкой **СЗИ** на ТС, так и после).

2. Настроить в системе защиты его считыватель.

Подробное описание настройки считывателей приведено в разделе 4.3.2 Настройка считывателей аппаратной идентификации данного руководства.

Для назначения идентификатора пользователю необходимо в окне создания или редактирования учетной записи пользователя открыть закладку *Аппаратная идентификация* (рис. 51).

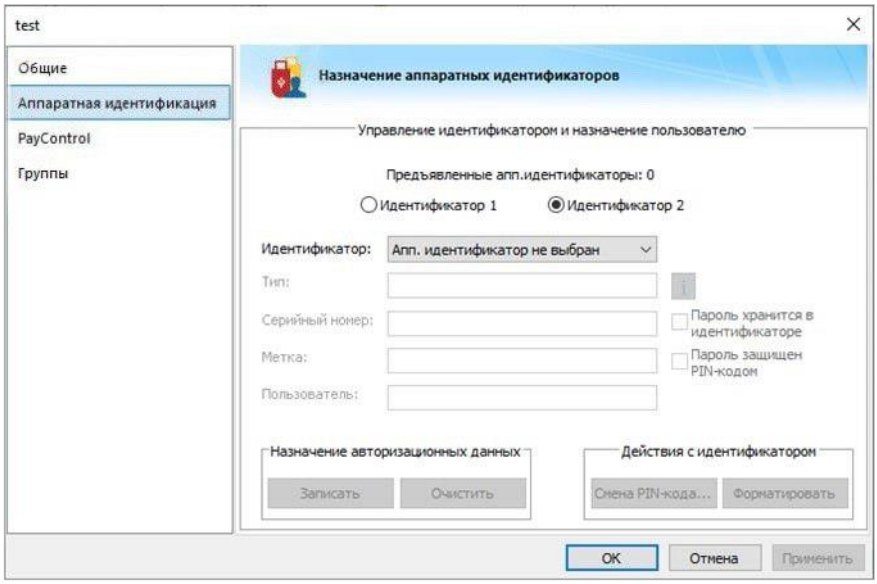


Рис. 51. Вкладка назначения аппаратных идентификаторов пользователю

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

После выбора идентификатора в полях с параметрами появятся: наименование его типа, номер, изображение, и для некоторых видов идентификаторов[8] станут доступны дополнительные функции (рис. 52).

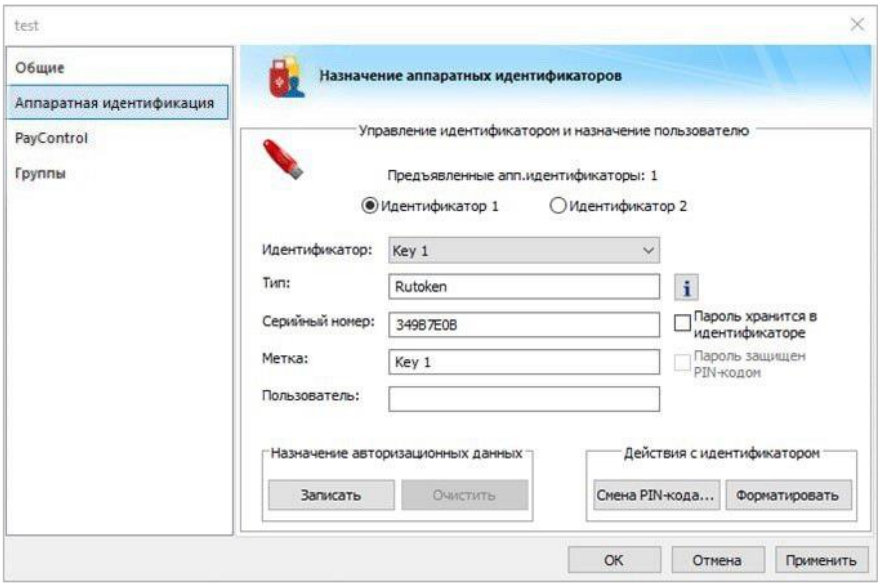


Рис. 52. Параметры назначенного идентификатора

После выбора идентификатора для пользователя необходимо нажать **Применить** и **OK**. Для установки второго идентификатора следует проделать действия выше с активным полем *Идентификатор 2*. Таким образом, после назначения идентификатора для учетной записи для

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

входа в ОС помимо ввода авторизационной информации, станет необходимо предъявить и назначенный аппаратный идентификатор.

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

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

4.3.2 Настройка считывателей аппаратной идентификации

Система **Dallas Lock 8.0** позволяет в качестве средства опознавания пользователей системы использовать аппаратные идентификаторы: **USB-Flash-накопители, электронные ключи Touch Memory (iButton), HID Proximity-карты, USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ; USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП PKI, Рутокен S, Рутокен ЭЦП 2.0 3000, Рутокен ЭЦП 2.0 Flash, Рутокен Lite 1000, Рутокен Lite 1010, Рутокен ЭЦП 3.0 3100, Рутокен ЭЦП 3.0 3200, Рутокен ЭЦП 3.0 3220, Рутокен ЭЦП Bluetooth, Рутокен Web, Рутокен PINPad, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X), Guardant ID 2.0.**

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

Общие сведения об идентификаторах

Электронный ключ Touch Memory представляет собой микросхему, размещенную в прочном корпусе из нержавеющей стали, по размерам и форме напоминающем батарейку от электронных часов (рис. 53).



Рис. 53. Touch Memory

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

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

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

Из-за особенностей работы драйверов считывателей Touch Memory есть техническое ограничение на использование данного типа считывателей при авторизации через удаленный рабочий стол.

Бесконтактная HID Proximity-карта представляет собой пластиковую карту со встроенной микросхемой и индивидуальным идентификационным кодом (рис. 54). Предназначена для контроля доступа и безопасной идентификации.

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



Рис. 54. Бесконтактная HID Proximity-карта

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

USB-ключ Aladdin eToken Pro/Java представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 55). USB-ключ eToken PRO/Java архитектурно реализован как USB-картридер с встроенной в него микросхемой (чипом) смарт-карты. Ключ выполнен в виде брелока и напрямую подключается к USB-порту компьютера, при этом не требует для своей работы каких-либо дополнительных устройств, кроме USB-порта.



Рис. 55. Aladdin eToken Pro/Java

Смарт-карта Aladdin eToken PRO/SC представляет собой пластиковую карту со встроенной микросхемой (рис. 56). Она предназначена для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами.



Рис. 56. Смарт-карта Aladdin eToken PRO/SC

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

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

USB-ключи и смарт-карты Рутокен (Rutoken) и Рутокен ЭЦП, Рутокен ЭЦП 2.0 — это компактное устройство, которое служит для авторизации пользователя в сети или на локальном компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных (рис. 57).



Рис. 57. Rutoken

Dallas Lock 8.0 поддерживает работу с моделями Рутокен: Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП PKI, Рутокен S, Рутокен ЭЦП 2.0 3000, Рутокен ЭЦП 2.0 Flash, Рутокен Lite 1000, Рутокен Lite 1010, Рутокен ЭЦП 3.0 3100, Рутокен ЭЦП 3.0 3200, Рутокен ЭЦП 3.0 3220, Рутокен ЭЦП Bluetooth, Рутокен Web, Рутокен PINPad, Рутокен 2151.

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

частных пользователей. Подобно ПК устройства JaCarta содержат процессор и модули памяти, функционируют под управлением своей ОС, выполняют необходимые прикладные программы и хранят информацию. Микроконтроллеры для JaCarta проектируются для решения задач информационной безопасности: они обладают встроенной защищенной памятью, средствами противодействия атакам по питанию, криптографическим акселератором (рис. 58).



Рис. 58. USB-ключ JaCarta

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

Для всех поддерживаемых устройств JaCarta рекомендуется использовать считыватель JaCarta GOST, подраздел 4.3.2 Настройка считывателей аппаратных идентификаторов. Не рекомендуется совместное использование считывателей JaCarta GOST и JaCarta PKI.

Смарт-карта ESMART Token представляет собой пластиковую карту со встроенной микросхемой (рис. 59). Смарт-карта обеспечивает безопасное хранение и использование цифровых сертификатов, ключей шифрования и электронной подписи. Для работы со смарт-картой ESMART Token требуется наличие считывателя контактных смарт-карт и свободный USB-порт или RS-232 для подключения считывателя.



Рис. 59. Смарт-карта ESMART Token

USB-ключ ESMART Token представляет собой защищенное устройство, предназначенное для строгой аутентификации и безопасного хранения секретных данных (рис. 60). USB-ключ ESMART Token ГОСТ представляет собой комбинацию считывателя и чипа смарт-карты в виде миниатюрного устройства. Устройство подключается к ПК напрямую, отдельный считыватель смарт-карт не требуется.



Рис. 60. USB-ключ ESMART Token

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

Guardant ID 2.0 — это устройство, подключаемое к USB-порту компьютера и предназначенное для использования в качестве персонального идентификатора администратора и пользователей информационной системы. Представляет собой электронный USB-идентификатор с установленной микропрограммой.



Рис. 61. USB-ключ Guardant ID

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

Таблица 1. Список директорий с драйверами на диске с дистрибутивом

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

Настройка считывателей аппаратных идентификаторов

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

Для дальнейшей работы необходима регистрация или настройка считывателей в **СЗИ**.

1. После того, как считыватель аппаратного идентификатора и драйверы к нему установлены, необходимо войти в оболочку администратора, открыть **Параметры безопасности** → **Политики авторизации** → **Аппаратная идентификация**. На экране отобразится окно настройки (рис. 62).

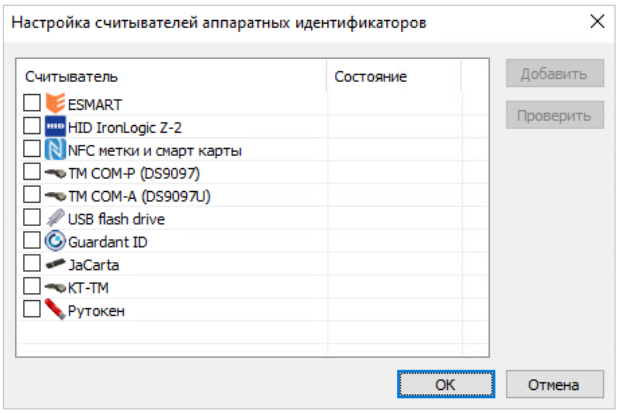


Рис. 62. Окно настройки считывателей аппаратной идентификации

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

Для работы с идентификаторами JaCarta и/или eToken в настройках необходимо выбрать тип считывателя «JaCarta».

2. Выделив необходимый идентификатор, нужно нажать **Добавить** или поставить флаг. Кнопка **Проверить** станет активной.
3. Перед проверкой готовности идентификатора необходимо его предъявить или настроить:
   - Для настройки аппаратных идентификаторов типа Touch Memory и HID необходимо подключить аппаратный считыватель к компьютеру через COM-порт (или USB для HID считывателя) и определить с помощью Диспетчера устройств Windows номер соответствующего COM-порта (рис. 63).

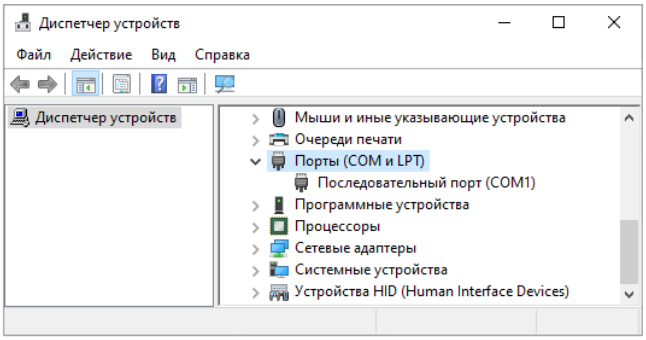


Рис. 63. Окно Диспетчера устройств Windows

   - В окне настройки считывателей аппаратной идентификации нужно выбрать название аппаратного идентификатора в списке и нажать кнопку **Добавить**. На экране появится окно для выбора, соответствующего COM-порта для подключенного идентификатора (рис. 64). В окне со списком COM-портов нужно установить соответствующий флаг и нажать **ОК**.

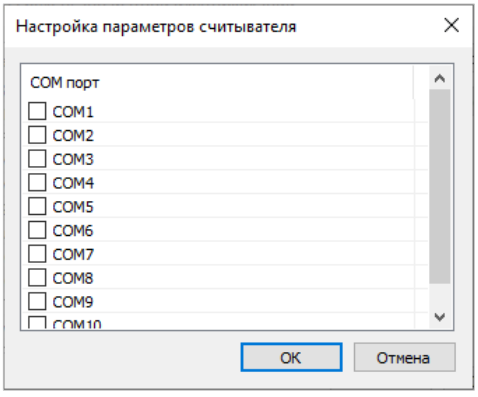


Рис. 64. Выбор COM-порта подключенного считывателя идентификатора

   - Для настройки аппаратного идентификатора типа смарт-карта eToken Pro/SC

к соответствующему порту необходимо подключить считыватель смарт-карты.

- Для идентификатора типа смарт-карта eToken Pro/SC флаг необходимо поставить в поле «eToken».
- Для идентификатора типа USB-ключ JaCarta флаг необходимо поставить в соответствующее идентификатору поле.
- Для идентификатора типа Рутокен флаг необходимо поставить в поле *Рутокен*.
- Для настройки аппаратного идентификатора типа смарт-карта ESMART Token ГОСТ к соответствующему порту необходимо подключить считыватель смарт-карты.
- Для идентификатора типа смарт-карта ESMART Token ГОСТ флаг необходимо поставить в поле «ESMART».
- Для идентификатора типа USB-ключ ESMART Token ГОСТ флаг необходимо поставить в поле «ESMART».
- Для идентификатора типа NFC метки флаг необходимо поставить в поле «NFC метки и смарты карты»;
- Для идентификатора типа USB-ключ Guardant ID 2.0 флаг необходимо поставить в поле «Guardant ID».

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

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

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

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

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

Из-за технических особенностей существует ограничение на использование считывателей USB-flash-drive при авторизации через удаленный рабочий стол.

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

При работе с аппаратными идентификаторами существуют следующие ограничения:

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

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

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

4.3.3 Принудительная двухфакторная аутентификация

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

Функционально для обязательной двухфакторной аутентификации необходимо выполнение двух условий:

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

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

4.3.4 Снятие аппаратной идентификации

Для того, чтобы снять назначение аппаратного идентификатора для учетной записи отдельного пользователя, необходимо на закладке *Аппаратная идентификация* окна параметров учетной записи в меню отображения имени идентификатора выбрать значение *Аппаратный идентификатор не назначен*, нажать **Применить** и **ОК**.

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

4.3.5 Действия с идентификатором

Для идентификаторов типа **USB-ключи и смарт-карты Aladdin eToken Pro (Java), eToken NG-FLASH (Java), eToken NG-OTP (Java), eToken Pro Anywhere, eToken ГОСТ; USB-ключи и смарт-карты Рутокен ЭЦП Flash, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП PKI, Рутокен S, Рутокен ЭЦП 2.0 3000, Рутокен ЭЦП 2.0 Flash, Рутокен Lite 1000, Рутокен Lite 1010, Рутокен ЭЦП 3.0 3100, Рутокен ЭЦП 3.0 3200, Рутокен ЭЦП 3.0 3220, Рутокен ЭЦП Bluetooth, Рутокен Web, Рутокен PINPad, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X), Guardant ID 2.0** доступны дополнительные расширенные возможности аппаратной идентификации.

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

Для обеспечения требуемого уровня безопасности данные PIN-коды следует изменить. Это можно также сделать, воспользовавшись специальной утилитой для идентификатора, либо используя окно

параметров назначенного пользователю идентификатора в оболочке администратора системы защиты. Для этого в поле *Действия с идентификатором* необходимо выбрать кнопку **Смена PIN-кода** или кнопку **Форматировать**.

По нажатию кнопки **Смена PIN-кода** откроется окно, в котором необходимо ввести значения PIN-кода пользователя: старое (текущее) значение, новое значение и повтор. Дополнительные кнопки рядом с полями ввода позволят изменить скрытые под звездочками символы на явные, повтор ввода PIN-кода в этом случае не потребуется (рис. 65).

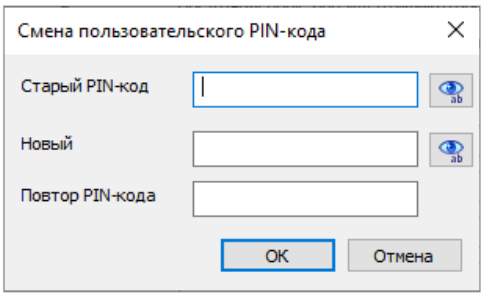


Рис. 65. Окно смены PIN-кода

По нажатию кнопки **Форматировать** откроется окно форматирования аппаратного идентификатора (рис. 66), в котором необходимо заполнить следующие поля:

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

Ввести новые данные:

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

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

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

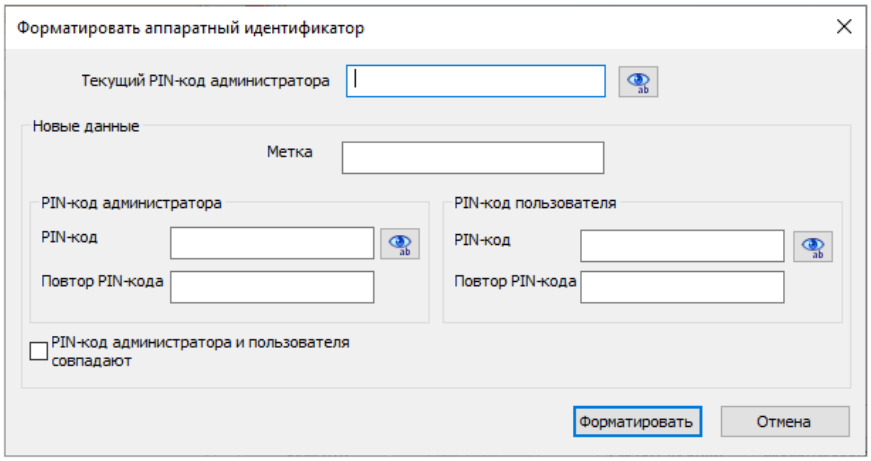


Рис. 66. Окно форматирования идентификатора

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

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

4.3.6 Поддержка биометрии

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

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

Для обеспечения требуемого уровня безопасности данные PIN-коды следует изменить, подраздел 4.3.5 Действия с идентификатором.

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

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

Далее откроется окно форматирования аппаратного идентификатора (рис. 66), поля в котором надо заполнить способом, приведенным в разделе 4.3.5 Действия с идентификатором.

После завершения форматирования появится окно регистрации отпечатков (рис. 67).



Рис. 67. Окно регистрации отпечатков

Порядок регистрации отпечатков:

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

Также доступны для изменения параметры качества сканирования[9] и вероятности ложного

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

допуска[10]. Данные параметры можно выбрать в выпадающем меню.

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

Запись биометрических данных в идентификатор

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

1. После выбора в выпадающем списке необходимого идентификатора отметить флагом поле *Пароль хранится в идентификаторе*. Поле *Пароль защищен PIN-кодом* выделится автоматически. Далее — нажать кнопку **Записать** (рис. 68).

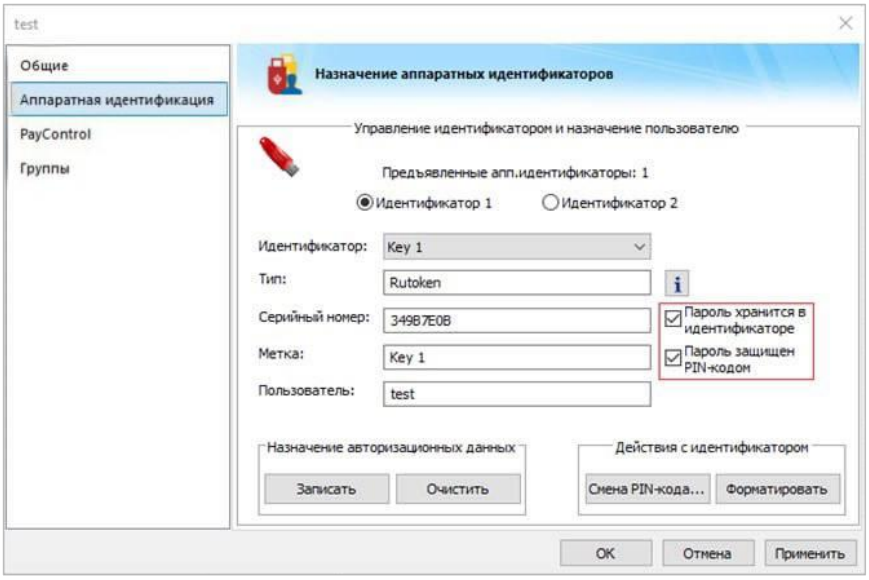


Рис. 68. Запись биометрических данных

2. В появившемся окне ввести дополнительную информацию: пароль пользователя (рис. 69), нажать **OK**.

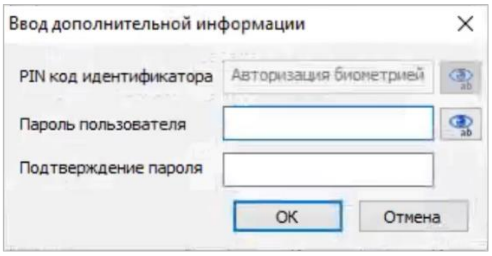


Рис. 69. Ввод дополнительной информации

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

Теперь для входа в ОС после предъявления идентификатора пользователю необходимо заполнить только поле ввода PIN-кода и выполнить проверку биометрических данных в зависимости от типа установленной авторизации, подраздел 2.6.2 Вход с аппаратным идентификатором.

4.3.7 Запись авторизационных данных в идентификатор

Запись авторизационных данных в память идентификатора доступна для следующих типов: **USB-**

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

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 Touch, Рутокен ЭЦП PKI, Рутокен S, Рутокен ЭЦП 2.0 3000, Рутокен ЭЦП 2.0 Flash, Рутокен Lite 1000, Рутокен Lite 1010, Рутокен ЭЦП 3.0 3100, Рутокен ЭЦП 3.0 3200, Рутокен ЭЦП 3.0 3220, Рутокен ЭЦП Bluetooth, Рутокен Web, Рутокен PINPad, Рутокен 2151; USB-ключи и смарт-карты JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta PKI, JaCarta PKI/BIO, JaCarta PRO, JaCarta LT, Jacarta-2 ГОСТ, Jacarta-2 PKI/ГОСТ, Jacarta-2 PKI/BIO/ГОСТ, Jacarta-2 PRO/ГОСТ, JaCarta-2 SE, Jacarta PKI/Flash, Jacarta PKI/ГОСТ, Jacarta PKI/ГОСТ/Flash; USB-ключи и смарт-карты ESMART Token ГОСТ, ESMART 64; NFC-метки и смарт-карты семейства MIFARE (Ultralight C, Classic 1K, ID, Plus SE, Plus S, Plus X, DESFiere EV1, ICODE SLI X), Guardant ID 2.0.

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

1. Записать в память идентификатора логин и пароль пользователя, и хранение данных защитить PIN-кодом. Для этого необходимо выполнить следующее. После выбора в выпадающем списке необходимого идентификатора отметить флагом поле *Пароль хранится в идентификаторе*. Поле *Пароль защищен PIN-кодом* выделится автоматически. Далее — нажать кнопку **Записать** (рис. 70).

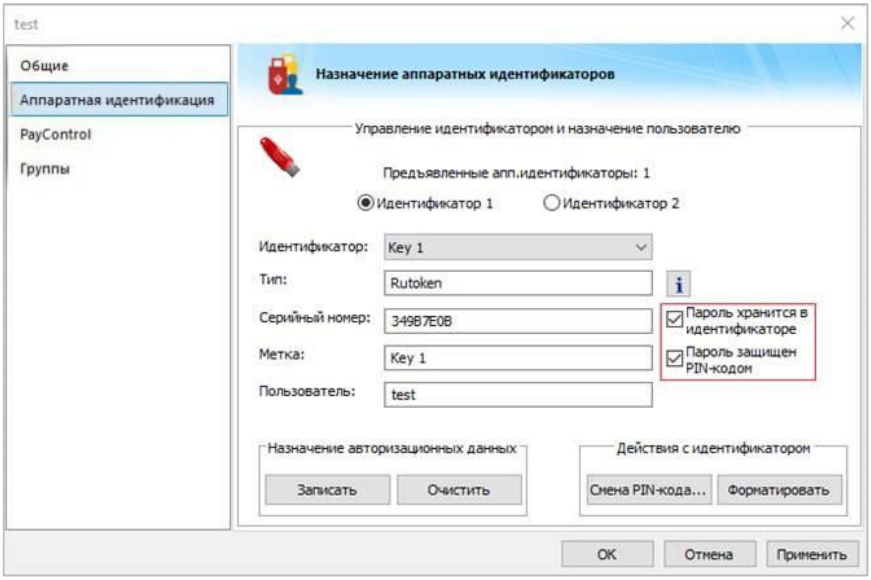


Рис. 70. Запись авторизационной информации в идентификатор

В появившемся окне ввести дополнительную информацию: PIN-код пользователя идентификатора и пароль пользователя (рис. 71), нажать **OK**.

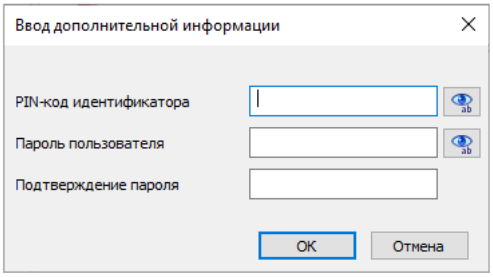


Рис. 71. Ввод дополнительной информации

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

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

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

2. Записать в память идентификатора логин и пароль учетной записи. Для этого необходимо выполнить следующее. В поле *Пароль защищен PIN-кодом* снять флаг, и таким образом записать авторизационные данные (кнопка **Записать**). Но в этом случае пароль учетной записи в идентификаторе будет незащищен, и система выдаст предупреждение. Таким образом, для входа в ОС пользователю станет достаточным только предъявление идентификатора (логин и

пароль считаются автоматически).

3. Записать в память идентификатора только логин учетной записи пользователя. Для этого не требуется выделение полей хранения паролей. Достаточно нажатия кнопки **Записать**. Система потребует ввести дополнительно только PIN-код пользователя данного идентификатора. При входе в ОС после предъявления идентификатора учетная запись будет однозначно идентифицирована с логином данного конкретного пользователя, остальные авторизационные поля пользователю необходимо будет ввести самостоятельно.

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

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

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

Вход в ОС ЗАРМ с использованием аппаратного идентификатора — 2.6.2 Вход с аппаратным идентификатором.

4.3.8 Определение принадлежности идентификатора

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

Чтобы открыть окно с информацией об идентификаторе, необходимо сначала его предъявить (приложить к считывателю или вставить в USB-порт). Далее в оболочке администратора на вкладке *Учетные записи* необходимо нажать кнопку **Принадл. идентификатора…** (рис. 72).

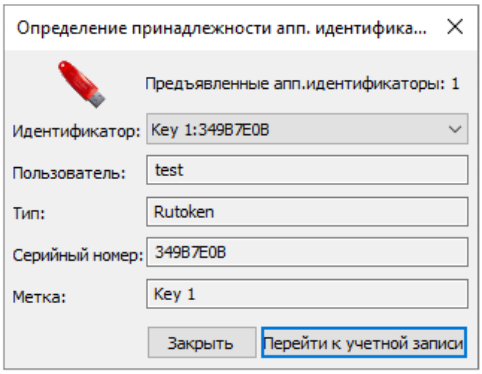


Рис. 72. Окно свойств предъявленного идентификатора

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

4.4 Аутентификация с PayControl

4.4.1 Подключение сервера PayControl

Для назначения многофакторной аутентификации для пользователей с помощью PayControl необходимо на вкладке **Параметры безопасности** → **Политики авторизации** → **Аутентификация с PayControl** открыть окно **Редактирование параметров безопасности**, двойным нажатием на параметр, ввести URL-адрес для подключения сервера PayControl (Рис. 73). Нажать кнопку **ОК** для сохранения URL-адреса.

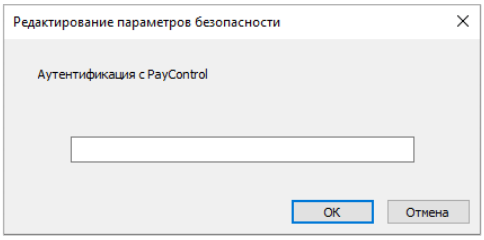


Рис. 73. Редактирование параметров безопасности

Если по указанному URL-адресу отсутствует подключение, то появится сообщение: «*Невозможно подключиться к серверу PayControl*». При этом значение политики не изменится.

При изменении или удалении URL-адреса сервера PayControl появится предупреждение о том, что все пользователи, которые были ранее зарегистрированы в системе будут разрегистрированы (рис. 74).

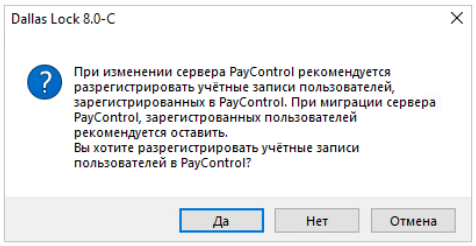


Рис. 74. Предупреждение о разрегистрации пользователей при изменении сервера PayControl

4.4.2 Настройка идентификатора PayControl для пользователя

Для нового пользователя или ранее созданного в окне **Изменения параметров пользователя**/**Создание нового пользователя** на вкладке *PayControl* (рис. 75) администратором регистрируется уникальный для каждого пользователя идентификатор.

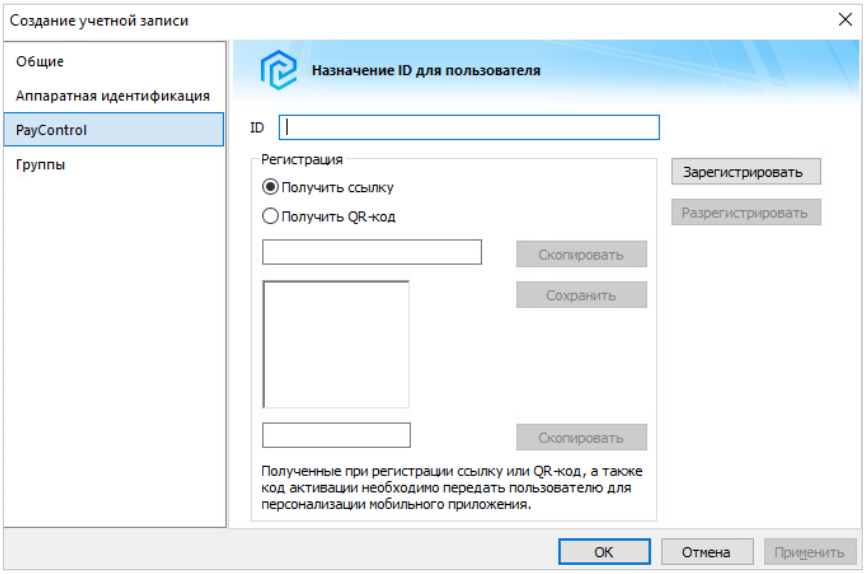


Рис. 75. Вкладка «PayControl»

Для подтверждения учетной записи необходимо выбрать желаемый способ получения информации: с помощью ссылки или QR-кода. Полученные при регистрации ссылку или QR-код, а также код активации необходимо передать пользователю для персонализации мобильного приложения.

При выборе *Получить ссылку* в пустом поле отображается ссылка, которую необходимо скопировать с помощью кнопки **Скопировать** и передать на мобильное устройство. Полученный код (рис. 76) необходимо скопировать и передать пользователю.

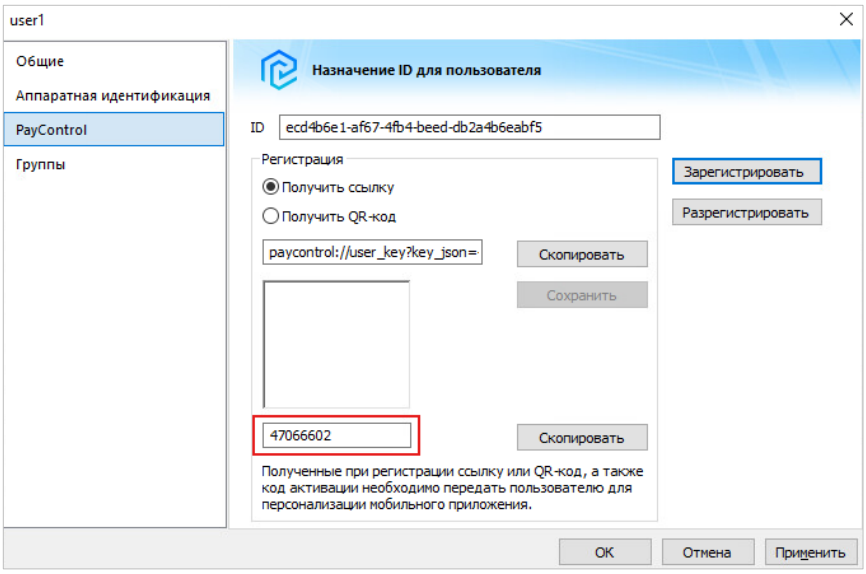


Рис. 76. Код активации по ссылке

При выборе *Получить QR-код* в пустом окне отображается код, при нажатии на область картинки с QR-кодом, он отображается в удобном формате, чтобы сканировать его с телефона (рис. 77).

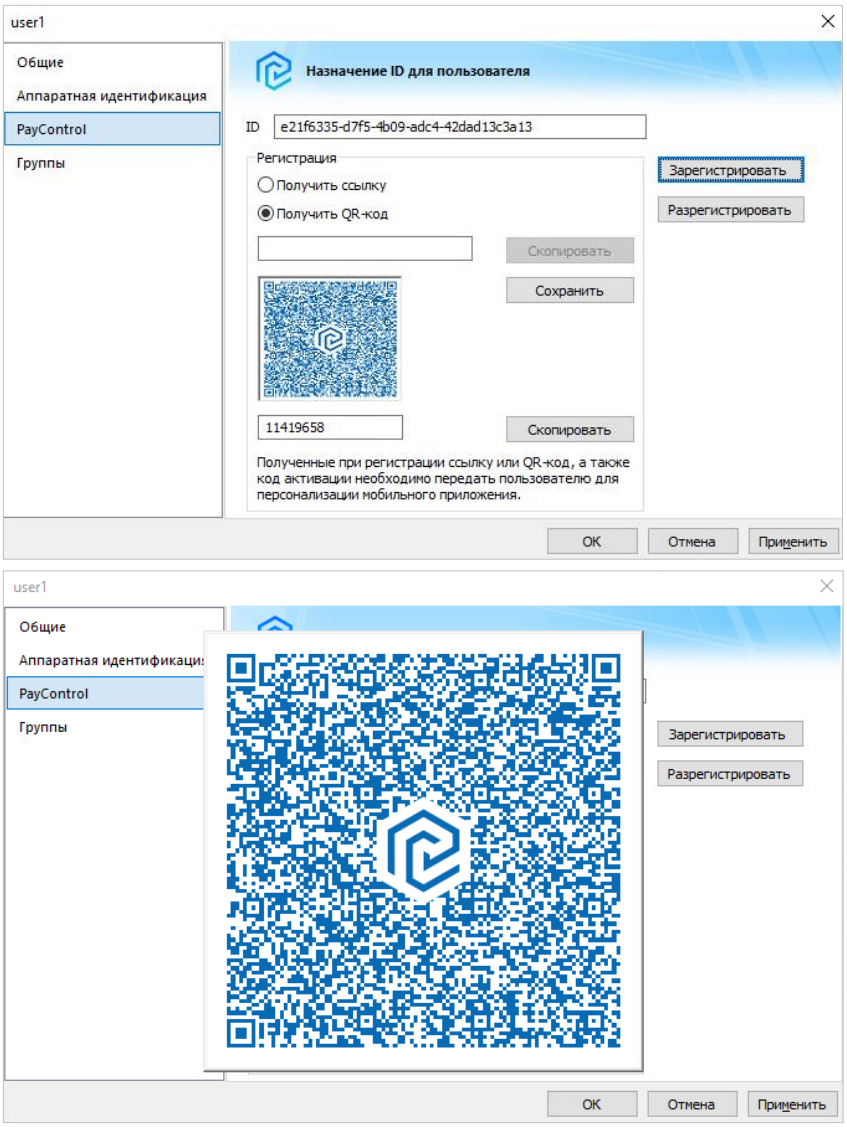


Рис. 77. Код активации по QR-коду

Полученный код (рис. 76) необходимо скопировать и передать пользователю. Для этого необходимо нажать кнопку **Зарегистрировать**.

После передачи пользователю ссылки или QR-кода, а также кода активации, пользователю

необходимо скачать приложение **PayControl** и пройти регистрацию. Пользователю необходимо ввести код активации, который был передан администратором информационной безопасности, нажать кнопку **Далее** (рис. 78).

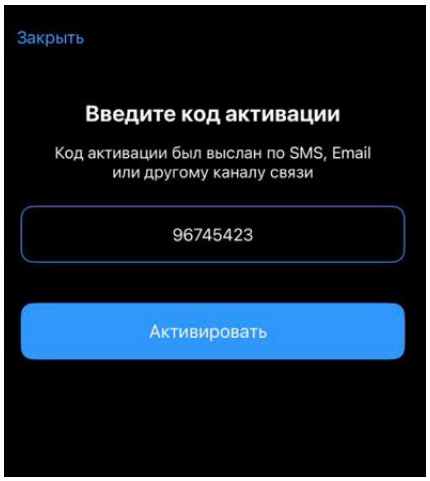


Рис. 78. Код активации

На следующей странице приложения необходимо ввести имя ключа (может быть несколько ключей) для дальнейшей авторизации, нажать кнопку **Далее** (рис. 79).

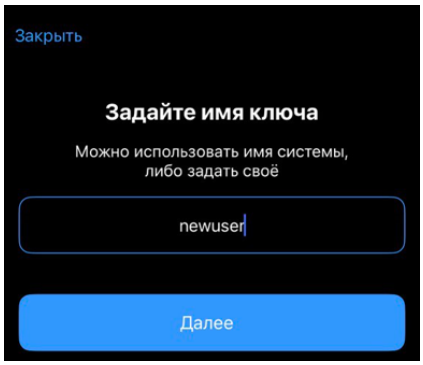


Рис. 79. Имя ключа

На следующей странице приложения пользователю необходимо придумать пароль не менее 6 символов (рис. 80). После проделанной операции пользователем, он будет окончательно занесен в реестр сервера подключения PayControl.

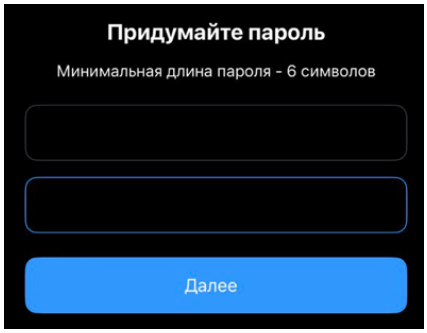


Рис. 80. Пароль для ключа

В поле *ID* автоматически заполняется после ответа от сервера. Если ID пользователю задан, но ссылка, QR-код или код активации не сохранены, то при закрытии окна отображается предупреждение (рис. 81).

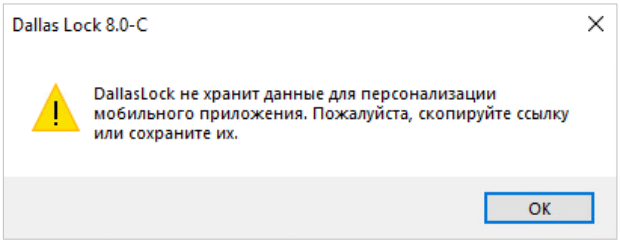


Рис. 81. Предупреждение о не сохраненных данных PayControl

При авторизации пользователя в системе появится сообщение о подтверждении авторизации

пользователя в мобильном приложении PayControl (рис. 82).

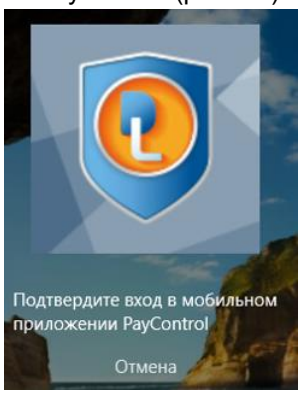


Рис. 82. Подтверждение входа в мобильном приложении PayControl

На мобильном устройстве пользователю необходимо подтвердить вход в систему (рис. 83).

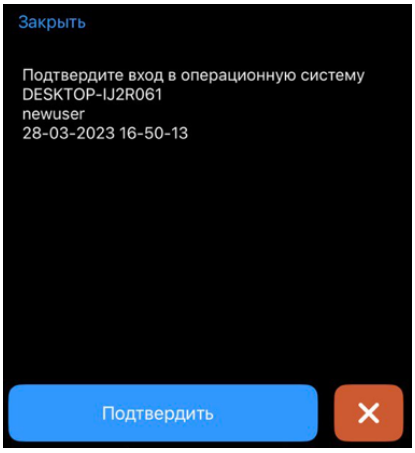


Рис. 83. Подтверждение авторизации на мобильном устройстве

При ошибке или не подтверждении операции входа, будет отображено соответствующее сообщение (рис. 84).

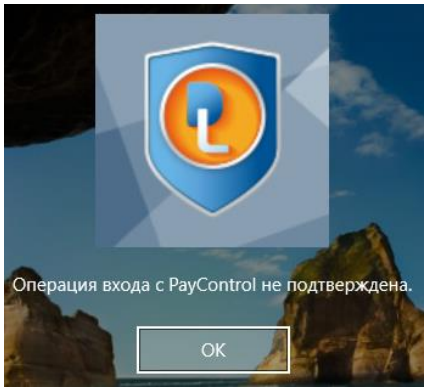


Рис. 84. Ошибка подтверждения входа

4.5 Параметры входа

4.5.1 Разрешение и запрет интерактивного и удаленного входов в ОС

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

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

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

При настройке следует учесть, что установленный параметр запрета имеет более высокий

приоритет перед установленным параметром разрешения. Также следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

Правило разрешения и запрета действий следующее:

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

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

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

Пример:

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

Для запрета входа локальных пользователей необходимо изменить параметр «Интерактивный вход: разрешен» убрать учетную запись «*Все*» и добавить учетную запись «*****». Если есть необходимость разрешения входа для пользователей определенного домена, то предварительно нужно создать учетную запись в виде «Имя_домена*», подраздел 4.1.4 Регистрация доменных учетных записей по маске.

4.5.2 Настройка политик авторизации

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

Для этого необходимо выбрать вкладку *Параметры безопасности*.

Настройки, касающиеся входа в систему, регулируются в категории **Политики авторизации** (рис. 85).

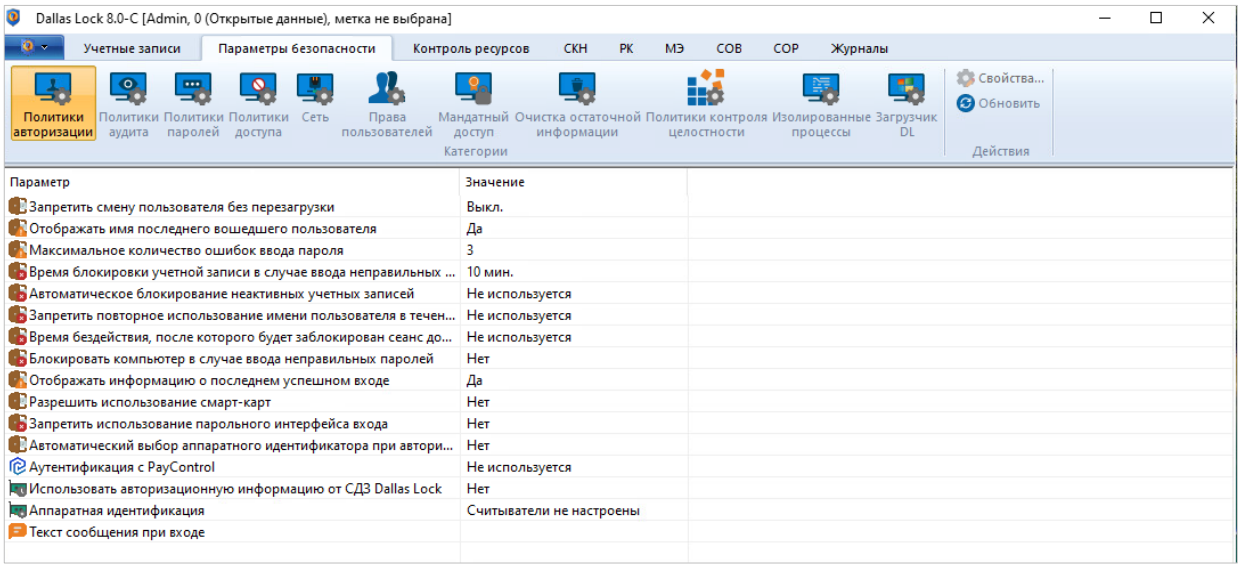


Рис. 85. Список политик авторизации

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметры политик авторизации.

Таблица 2. Настраиваемые параметры политик авторизации

Запретить смену пользователя без перезагрузки
Включение данного параметра не позволит осуществлять смену учетных записей пользователей без перезагрузки ПК. Если параметр имеет значение «Вкл.», то при выборе завершения сеанса

или смены пользователя ПК автоматически уходит в перезагрузку. Если параметр имеет значение «*Выкл.*», то при выборе завершения сеанса или смены пользователя ПК выйдет из учетной записи и предложит снова ввести авторизационные данные, раздел 8.4 Запрет смены пользователя без перезагрузки.

Отображать имя последнего пользователя

Включение данного параметра позволяет отображать в окне авторизации имя учетной записи последнего пользователя, осуществлявшего вход в ОС.

Если параметр имеет значение «*Да*», то в поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет отображаться имя последнего пользователя данного ПК. Если параметр имеет значение «*Нет*», то поле, в котором требуется ввести имя пользователя при авторизации на ПК, будет пустым.

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

Максимальное количество ошибок ввода пароля

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

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

Способы блокировки описаны в разделе 4.2 Заблокированные пользователи.

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

Время блокировки учетной записи в случае ввода неправильных паролей

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

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

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

Автоматическое блокирование неактивных учетных записей пользователей

Данный параметр позволяет настроить и выполнить автоматическую блокировку неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования. По умолчанию значение данного параметра: «*Не используется*».

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

Запретить повторное использование имени пользователя в течение

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

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

Время бездействия, после которого будет заблокирован сеанс доступа

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

По умолчанию значение данного параметра: «*Не используется*».

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

Блокировать компьютер в случае ввода неправильных паролей

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

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

После включения данного параметра безопасности при вводе неправильных паролей компьютер блокируется. В таком случае авторизоваться на этом компьютере может только суперадминистратор. Чтобы разблокировать компьютер, необходимо через контекстное меню BlockIcon выполнить команду **Разблокировать компьютер** (рис. 86).

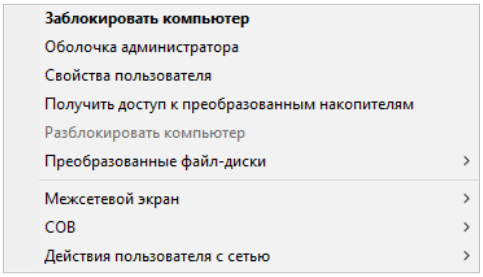


Рис. 86. Контекстное меню BlockIcon

Отображать информацию о последнем успешном входе

При включении данного параметра входа (значение «*Да*») после загрузки ОС в области уведомлений Windows на панели задач будет появляться сообщение с информацией о дате последнего входа пользователя на данный компьютер, типе входа: сетевой, локальный, терминальный, неуспешных попытках входа и состоянии параметров учетной записи пользователя (рис. 87).

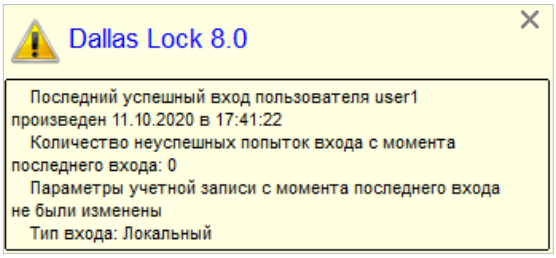


Рис. 87. Всплывающее уведомление о последнем успешном входе

Разрешить использование смарт-карт

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

Запретить использование парольного интерфейса входа

При использовании смарт-карт для авторизации в ОС возможно отключить интерфейс входа по имени пользователя и пароля при включении данного параметра.

Автоматический выбор аппаратного идентификатора при авторизации

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

Аутентификация с PayControl

Включение данного параметра позволяет подключиться к серверу PayControl. В открывшемся окне ввести URL-адрес для подключения к серверу PayControl. После активации данной политики администратор может назначать пользователям ID. Пока политика не активна такой возможности нет.

Изменения политики, связанные с изменением или удалением URL-адреса сервера, приведут к разрегистрации всех пользователей на сервере PayControl.

Использовать авторизационную информацию от СДЗ Dallas Lock

При включении данного параметра автоматически используется авторизационная информация от **СДЗ Dallas Lock**. Параметр доступен только при установленной аппаратной плате. Для работы параметра необходимо в ОС установить драйвер для **СДЗ**.
Аппаратная идентификация
С помощью данного параметра производится настройка считывателей электронных идентификаторов. Предварительно необходимо установить соответствующие драйверы и предъявить идентификаторы.
Текст сообщения при входе
В окне данного параметра имеется возможность ввести текст предупреждения, которое будет отображаться пользователю до входа в ОС. Смысл данного текста должен предупреждать о реализации мер по обеспечению безопасности информации, и о необходимости соблюдения установленных правил обработки информации. Нажатие **ОК** пользователем будут означать подтверждение ознакомления.

4.5.3 Настройка политик паролей

Политики паролей задают минимальные требования к длине пароля, его сложности, сроке действия, а также включают другие настройки (рис. 88).

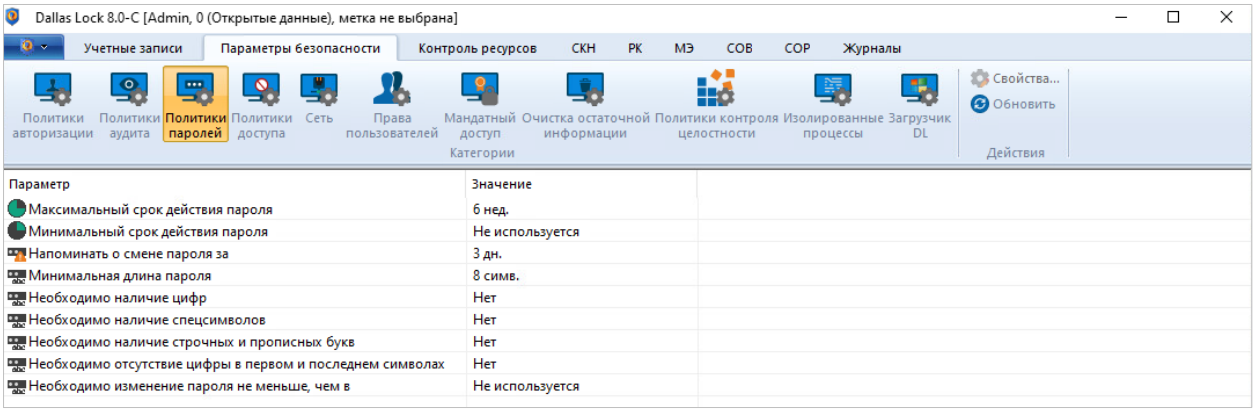


Рис. 88. Список политик паролей

Для настройки доступны следующие параметры:

Таблица 3. Настраиваемые параметры политики паролей

Максимальный срок действия пароля
Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока **СЗИ** автоматически предложит пользователю сменить пароль при входе в ОС. Если выбрано значение *Не используется*, то время действия пароля не ограничено. В тоже время, данный параметр не является приоритетным. Он действует, только если для пользователя не указано никаких иных значений срока действия пароля. Максимальный срок действия пароля для каждого конкретного пользователя определяется по следующей схеме: • Если администратор установил для конкретного пользователя принудительную смену пароля при следующем входе на компьютер, то в процессе очередной загрузки компьютера этим пользователем система защиты обязательно потребует сменить пароль, даже если срок действия пароля не истек (наивысший приоритет). • Если администратором для конкретного пользователя ***установлено*** значение: **Пароль без ограничения срока действия**, и отсутствует требование смены пароля при следующем входе, то СЗИ не потребует смены пароля даже в случае превышения максимального срока действия пароля. • Если администратором для конкретного пользователя ***не установлено*** значение: **Пароль без ограничения срока действия**, и отсутствует требование смены пароля при следующем входе, то СЗИ потребует от данного пользователя сменить пароль по истечении максимального срока действия пароля (низший приоритет).
Минимальный срок действия пароля
Данным параметром устанавливается минимальный срок действия пароля для всех

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

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

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

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

Напоминать о смене пароля за

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

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

Параметры, устанавливающие срок действия пароля, действуют независимо от аналогичных параметров ОС Windows. В Windows действуют свои политики безопасности, которые также могут потребовать смены пароля, независимо от **Dallas Lock 8.0**.

В **Dallas Lock 8.0** и ОС Windows совпадают следующие парольные политики:

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

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

Минимальная длина пароля

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

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

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

По умолчанию минимальная длина пароля составляет 8 символов.

Необходимо наличие цифр

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

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

Необходимо наличие спецсимволов

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

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

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

Необходимо наличие строчных и прописных букв

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

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

Необходимо отсутствие цифры в первом и последнем символах

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

Необходимо изменение пароля не меньше, чем в

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

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

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

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



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

4.5.4 Настройка политик доступа

Политики доступа позволяют устанавливать параметры блокировки для ЗАРМ, устройств и файлов по расширению (рис. 89).

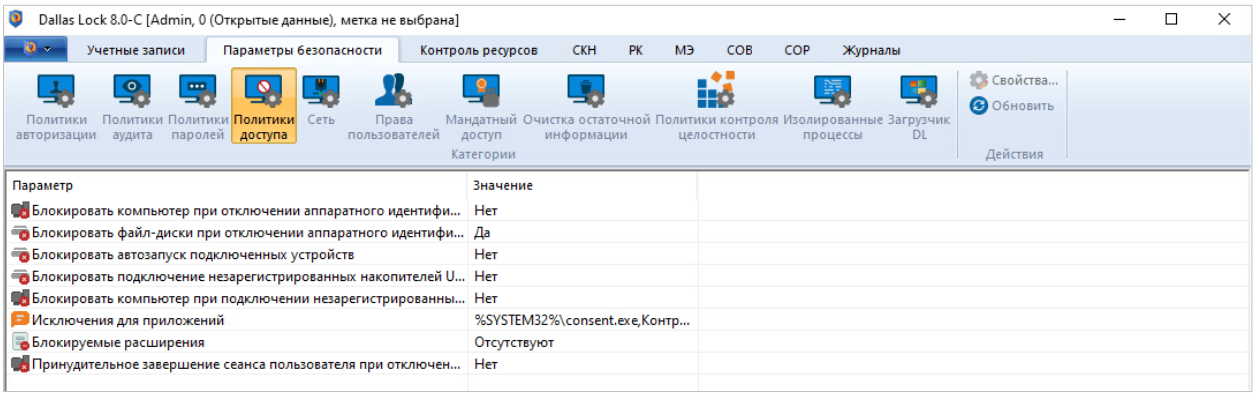


Рис. 89. Список политик доступа

Для настройки доступны следующие параметры:

Таблица 4. Настраиваемые параметры политики доступа

Блокировать компьютер при отключении аппаратного идентификатора
При включении данного параметра всем пользователям, которым назначен аппаратный идентификатор, работа на данном ПК при отключении идентификатора будет заблокирована. Параметр не распространяется на идентификаторы, предъявляемые по касанию.
Блокировать файл-диски при отключении аппаратного идентификатора
Если при создании файл-диска, раздел 12.3 Преобразованные файл-диски, помимо пароля, используется аппаратный идентификатор, то при отключении идентификатора от ПК, файл-диск также будет отключен. Стоит учитывать, что при изменении настроек аппаратного идентификатора необходимо начать новый сеанс работы пользователя для выполнения корректной блокировки. Параметр не распространяется на идентификаторы, предъявляемые по касанию.
Блокировать автозапуск подключенных устройств
При включении данного параметра автоматически блокируется возможность запуска без команды пользователя (автозапуска) устройства при подключении. По умолчанию установлено значение «*Нет*».
Блокировать подключение незарегистрированных накопителей USB Flash
Данный параметр позволяет блокировать незарегистрированные USB-Flash накопители. Возможные значения параметра: «*Да*» или «*Нет*» (установлено по умолчанию). При включении политики пользователю не предоставляется доступ к накопителям, в систему не устанавливаются драйверы накопителей и в реестре не регистрируется информация о подключении, в проводнике пользователь их не увидит.
Блокировать компьютер при подключении незарегистрированных накопителей USB Flash
Данный параметр позволяет блокировать компьютер при подключении незарегистрированных USB-Flash накопителей. Возможные значения параметра: «*Да*» или «*Нет*» (установлено по умолчанию). Если данная политика включена, то при подключении незарегистрированных USB-Flash накопителей выполняется блокировка компьютера. В таком случае авторизоваться на этом компьютере может только суперадминистратор. Чтобы разблокировать компьютер, необходимо через контекстное меню BlockIcon выполнить команду **Разблокировать компьютер**. Действие данной политики не распространяется на учетную запись суперадминистратора.
Исключения для приложений
Список файлов, для которых не производится контроль приложений, печати и изолированных процессов. Список — содержит имена и названия исключений, перечисленные через ";". Имена могут не содержать пути, либо включать в себя последнюю часть пути или полный путь (этот вариант наиболее безопасен). Формат значения параметра: **имя (путь)**, **исключение**.

Список исключений:

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

Если в любом элементе списка в качестве имени указано «*» — настройка будет активной для всех исключений.

Чтобы добавить исключение для процесса необходимо:

1. Перейти на вкладку **Параметры безопасности** → **Политики доступа** → **Исключения для приложений**. При двойном нажатии на параметр открывается окно **Редактирование параметров безопасности** (рис. 90).

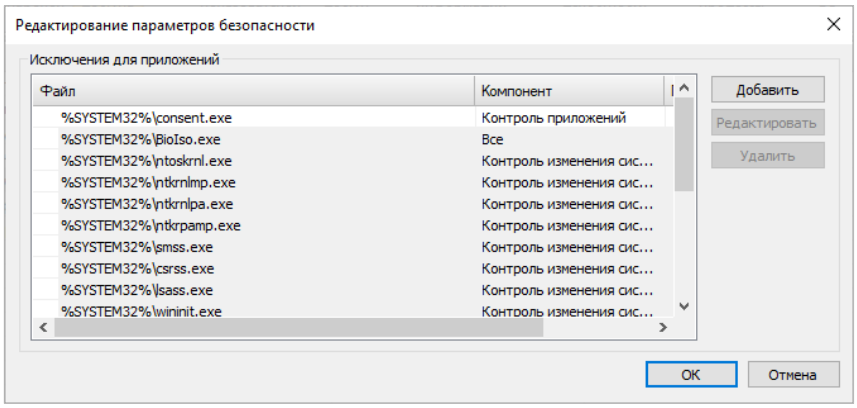


Рис. 90. Редактирование параметров безопасности

Каждое исключение имеет два признака: **Локальное исключение** и **По пути**. Локальные исключения применяются только на конкретном устройстве и не синхронизируются при централизованном управлении, в то время как исключения **по пути** управляются централизованно и применяются ко всем устройствам в сети.
При создании исключения через оболочку администратора, по умолчанию оно является локальным, а параметр **По пути** отключен.

2. Нажать кнопку **Добавить**, в окне **Исключение для компонента** выбрать файл, для которого создается исключение, и тип исключения (рис. 91). Нажать **ОК**.

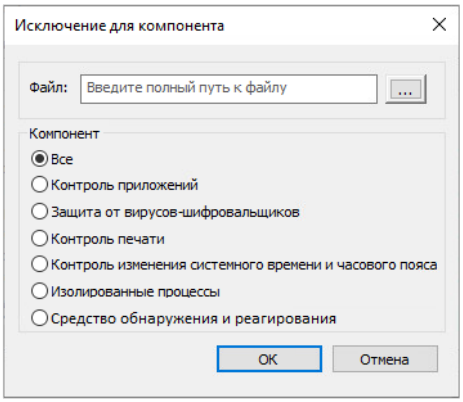


Рис. 91. Исключение для компонента

Dallas Lock 8.0 блокирует попытку изменения системного времени и часового пояса, если приложение, с помощью которого выполняется операция, или пользователь, из-под которого запущено это приложение, не добавлены в исключения.

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

В строке *Значение* параметра **Исключения для приложений** будет отображаться выбранный файл и тип исключения.

Для добавления в исключения всех файлов необходимо ввести символ «*» в параметр файл. Данное действие эквивалентно отключению соответствующего компонента защиты.

Чтобы отредактировать файл исключения, нужно открыть окно **Редактирование параметров безопасности**, выделить необходимый файл, где требуется изменить тип исключения, и нажать кнопку **Редактировать**. Чтобы удалить процесс, в окне **Редактирование параметров безопасности** следует выделить файл, нажать кнопку **Удалить**, подтвердить удаление и нажать **ОК**. Также добавить процесс в исключения можно, выбрав его во вкладке **Журналы** → **Журнал процессов**, и нажав правой кнопкой на процесс **Добавить в исключения** и выбрать для какого компонента создается исключение.

Пример:

«ViPNet Client\Monitor.exe,all;»

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

«*, a»

Блокируемые расширения

В системе защиты **Dallas Lock 8.0** реализована функция блокировки доступа к файлам по их расширению. Эта функция может быть полезна, к примеру, для того чтобы запретить сотрудникам работу с файлами, не имеющими отношения к их профессиональным обязанностям (mp3, avi и т. д.).

Для того, чтобы добавить расширение, на которое распространяется запрет, необходимо:

1. Запустить оболочку администратора и на вкладке *Параметры безопасности* зайти в категорию **Политики доступа**, выбрать **Блокируемые расширения**.
2. Правой кнопкой мыши два раза щелкнут по политике, в результате чего откроется окно **Блокируемые расширения** (рис. 92).

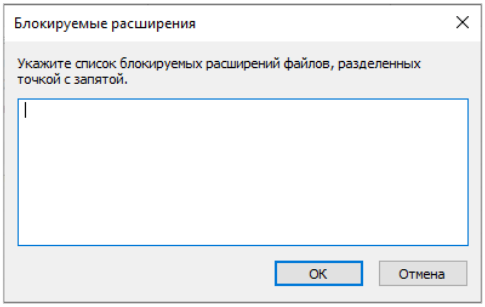


Рис. 92. Окно задания блокировки расширения

3. В данном окне нужно ввести необходимое расширение и нажать кнопку **ОК**.

Функция **Блокируемые расширения** будет распространяться на всех пользователей кроме пользователя, выполнившего установку **СЗИ**, суперадминистратора. При попытке пользователя открыть файл с заблокированным расширением, появится соответствующее предупреждение.

Следует учесть, что добавление в список блокируемых расширений, таких как exe, dll, sys, может привести к неработоспособности ОС (исключение составит работа под учетной записью суперадминистратора).

Принудительное завершение сеанса пользователя при отключении аппаратного идентификатора

При включении данного параметра при извлечении аппаратного идентификатора принудительно будет заблокирован компьютер пользователя.

4.5.5 Настройка политик сети

В категории **Сеть** доступны параметры для настройки централизованного управления посредством **СБ Dallas Lock** и **ЕЦУ Dallas Lock**, а также настройки ввода и вывода ПК из **СК Dallas Lock** и другие сетевые настройки (рис. 93).

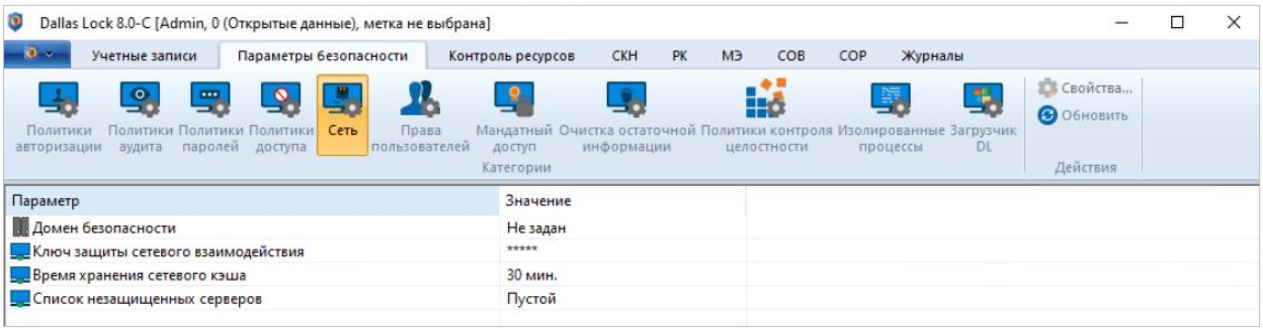


Рис. 93. Список политик сети

Доступны следующие параметры:

Таблица 5. Настраиваемые параметры политик сети

Домен безопасности
Данный параметр позволяет вводить и выводить ПК из **ДБ**, раздел Ввод защищенного компьютера в ДБ. Если ПК не введен в **ДБ**, то параметр имеет значение «*Не задан*». В свойствах параметра необходимо ввести имя ПК, на котором размещен **ЕЦУ**, и ключ доступа (по умолчанию имеет пустое значение). После ввода в **ДБ** значение параметра принимает имя **ЕЦУ**. Для вывода из **ДБ** необходимо ввести ключ доступа к **ЕЦУ**.
Ключ защиты сетевого взаимодействия
Данным параметром устанавливается значение ключа защиты сетевого взаимодействия для удаленного входа на другие ЗАРМ, раздел 11.4 Ключи защиты сетевого взаимодействия.
Время хранения сетевого кэша
Для увеличения скорости работы по сети система защиты **Dallas Lock 8.0** предоставляет возможность сохранения сетевого кэша с информацией об имеющихся в сети тех компьютеров, которые защищены **Dallas Lock 8.0**, и к которым уже было произведено обращение с данного ПК. В выпадающем списке данного параметра можно выбрать время хранения такого сетевого кэша.
Список незащищенных серверов
С помощью данного параметра для увеличения скорости работы по сети, чтобы сократить количество обращений, **СЗИ** предоставляет возможность сохранить постоянный список ПК, которые не защищены **СЗИ**. Вводятся имена ПК и серверов или их IP-адреса через точку с запятой.

4.6 Изолированные процессы

Для исключения потенциального канала утечки конфиденциальной информации через программы-клиенты терминального доступа в **СЗИ** реализован механизм изолированных процессов.

Если процесс помечен как изолированный, то в этот процесс нельзя ничего скопировать через буфер обмена и из него нельзя ничего скопировать в другой процесс. Таким образом, механизм изолированных процессов позволяет исключить ситуацию, в которой злоумышленник использует терминальное подключение к какому-либо удаленному ПК и через буфер обмена копирует информацию.

Для контроля уровня доступа данных, находящихся в буфере обмена, применяется мандатный принцип (только для Dallas Lock 8.0 редакции «С») разграничения доступа, раздел 5.3 Мандатный доступ.

Чтобы пометить процесс как изолированный, необходимо в основном меню оболочки администратора на вкладке *Параметры безопасности* выбрать категорию **Изолированные процессы** (рис. 94).

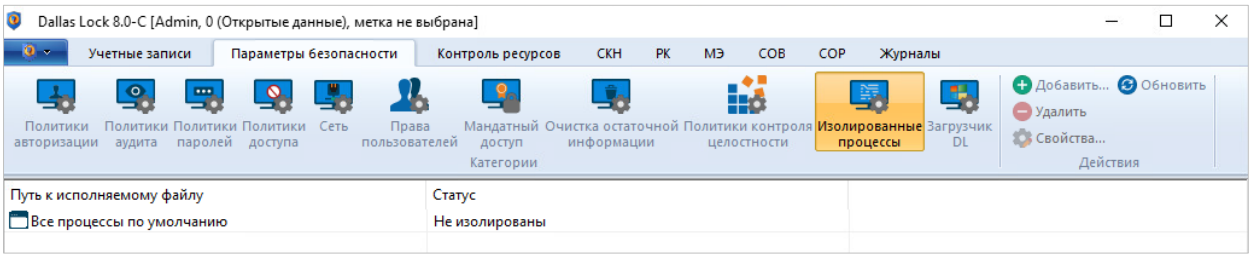


Рис. 94. Категория параметров безопасности «Изолированные процессы»

В окне программы появится поле со списком изолированных процессов и панель действий, содержащая инструменты по добавлению, удалению или редактированию пути к процессу, который необходимых изолировать.

В списке процессов первым всегда стоит глобальный параметр, определяющий политику для всех процессов на данном ПК — все процессы являются изолированными или не изолированными. Также данным списком через заданный полный путь к соответствующему исполняемому файлу определяются отдельные процессы.

Механизм настройки политики изолированных процессов, следующий:

1. Устанавливается, что все процессы по умолчанию изолированы, и есть список не изолированных процессов.
2. Или устанавливается, что все процессы по умолчанию не изолированы, и есть список изолированных процессов.

По умолчанию активен режим, в котором все процессы не изолированы. Чтобы изменить его, необходимо кликнуть на параметр **Все процессы по умолчанию** и в окне изменения свойств отметить поле *Все процессы по умолчанию изолированы*.

Чтобы добавить новый процесс в список, необходимо выбрать действие **Добавить**. Появится проводник программы, с помощью которого необходимо выбрать исполняемый файл процесса и нажать **Выбрать**, после чего он появится в списке изолированных/не изолированных (в зависимости от выбранной политики безопасности).

Также можно изолировать процесс, выбрав его в журнале процессов и нажав действие **Добавить в список изолированных** (рис. 95). Путь к исполняемому файлу данного процесса также появится в списке на вкладке **Параметры безопасности** → **Изолированные процессы**.

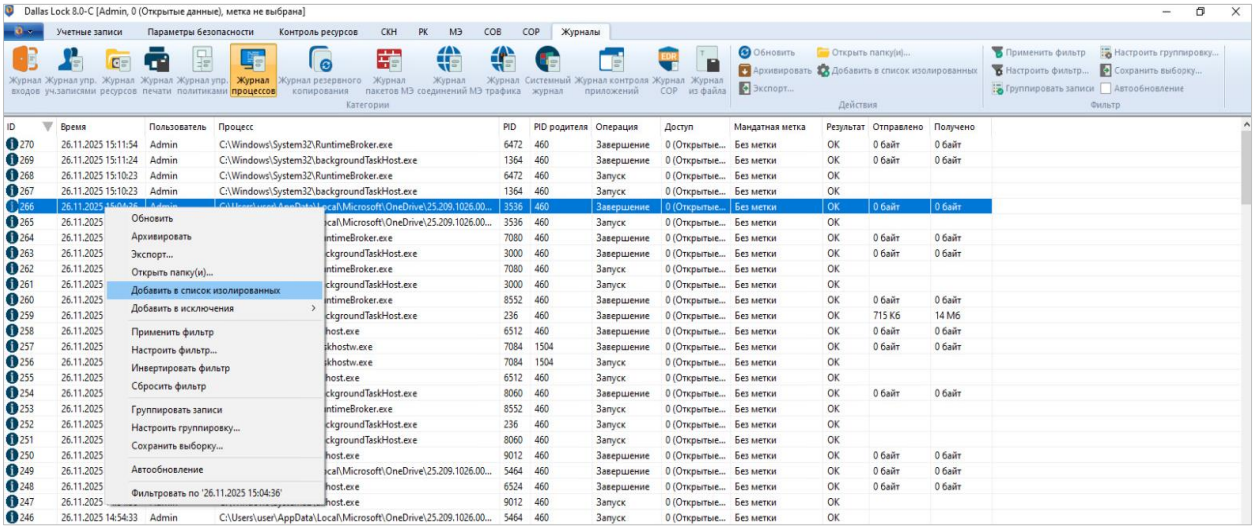


Рис. 95. Определение изолированного процесса через журнал процессов

После редактирования списка изолированных процессов новая конфигурация будет применена только для последующих сеансов работы пользователей.

Действия по изменению списка изолированных процессов фиксируются в журнале управления политиками.

4.7 Загрузчик DL

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

Модуль **Загрузчик DL** нужен для предотвращения несанкционированного запуска компьютера до

этапа загрузки ОС. Модуль обеспечивает высокую степень защищенности секретной и конфиденциальной информации.

Активированный модуль **Загрузчик DL** позволяет следующее:

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

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

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

4.7.1 Включение модуля «Загрузчик DL»

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

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

Поддержка программного RAID загрузчиком DL не осуществляется.

Для активации модуля **Загрузчик DL**, необходимо в оболочке администратора выбрать вкладку *Параметры безопасности* основного меню, далее — категорию **Загрузчик DL** и нажать кнопку **Включить** (рис. 96).

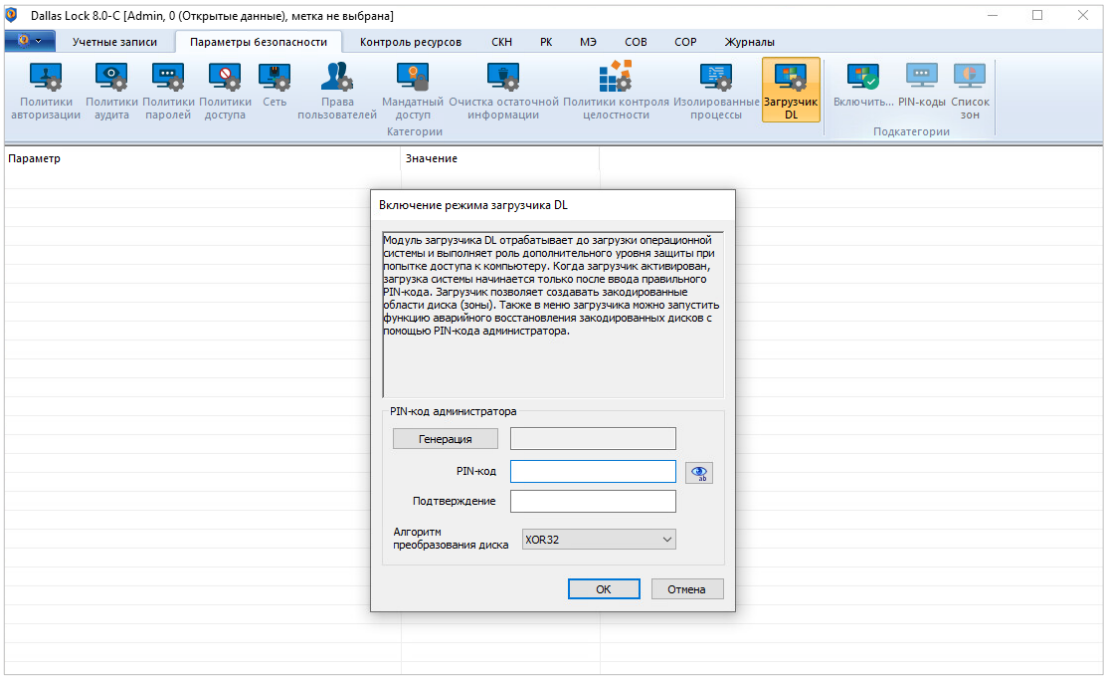


Рис. 96. Включение механизма загрузчика DL

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

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

   В качестве PIN-кодов может использоваться любая комбинация символов, удовлетворяющих установленным политикам назначения пароля, подраздел 4.5.3 Настройка политик паролей. Можно воспользоваться генератором паролей и ввести сформированный **СЗИ** пароль в соответствующие поля. При нажатии кнопки скрытые символы изменятся на явные,

подтверждение пароля в этом случае не потребуется и заблокируется.

2. Определить алгоритм преобразования дисков, выбрав его из выпадающего списка. После включения алгоритм изменить не удастся.
3. После установки параметров необходимо нажать **ОК**. Появится сообщение об успешном включении модуля загрузки и требовании перезагрузить компьютер. Следующий вход на АРМ осуществится с предварительной авторизацией в загрузчике.

Включение загрузчика DL может занять до 10 минут.

Для выключения модуля **Загрузчик DL**, необходимо на панели подкатегории нажать кнопку **Выключить**. Система защиты выключит **Загрузчик DL** и попросит перезагрузить ПК. Записи о созданных в системе PIN-кодах, подраздел 4.7.2 Создание PIN-кода пользователя, удалятся.

Выключение модуля возможно при условии отсутствия преобразованных областей жесткого диска, раздел 12.1 Прозрачное преобразование дисков.

4.7.2 Создание PIN-кода пользователя

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

На вкладке *Параметры безопасности* в категории **Загрузчик DL** в списке основного окна присутствуют записи о созданных PIN-кодах для авторизации в модуле **Загрузчик DL**.

Чтобы создать новый PIN-код пользователя, необходимо нажать на панели действий кнопку **Добавить PIN**. Откроется окно создания PIN-кода (рис. 97).

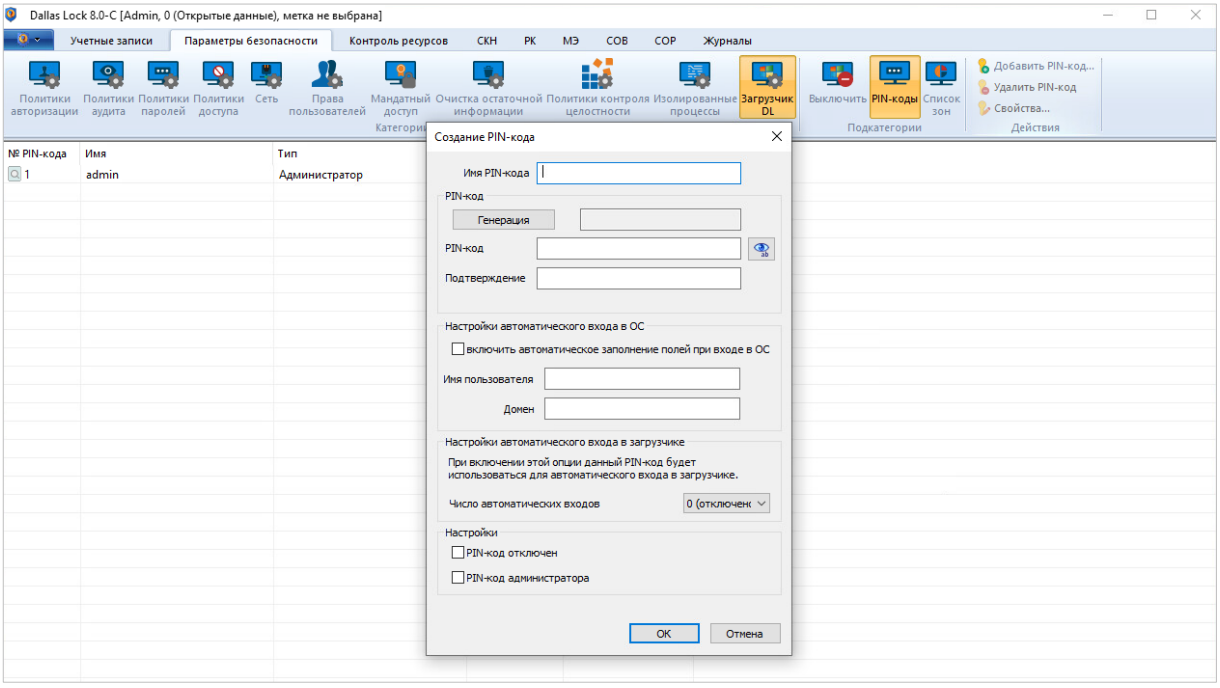


Рис. 97. Окно создания PIN-кода для загрузчика

Окно создания PIN-кода содержит следующие заполняемые поля:

Наименование	Описание
Имя PIN-кода	Произвольное название для идентификации в списке
PIN-код	Значение PIN-кода, которое должно соответствовать установленным в **СЗИ** парольным политикам. Для изменения PIN-кода необходимо отметить поле *Смена PIN-кода*
Подтверждение	Значение PIN-кода должно совпадать с введенным ранее в поле *PIN-код*

Наименование	Описание
Настройка автоматического входа в ОС	При включении и заполнении параметров этого блока для пользователя, при вводе данного PIN-кода поля для авторизации в Windows («Имя пользователя» и «Домен») будут автоматически заполнены указанными в блоке
Настройка автоматического входа в загрузчике	Данное Включение путем выбора числа входов позволит осуществлять вход в ОС, минуя заполнение поля ввода PIN-кода, т.е. автоматически через загрузчик, но с теми параметрами, которые указаны для данного PIN-кода
PIN-код отключен	Отмеченное флагом поле позволит вместо удаления временно отключить выбранный PIN-код
PIN-код администратора	Отмеченное флагом поле установит статус, с которым для данного PIN-кода станет доступна функция аварийного преобразования в загрузчике, раздел 21.1 Обратное преобразование жесткого диска в аварийном режиме.

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

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

Редактирование параметров PIN-кода доступно после двойного клика по имени необходимого PIN-кода в списке. При редактировании откроется окно свойств PIN-кода (рис. 98). В данном окне станет доступным замена старого PIN-кода на новый.

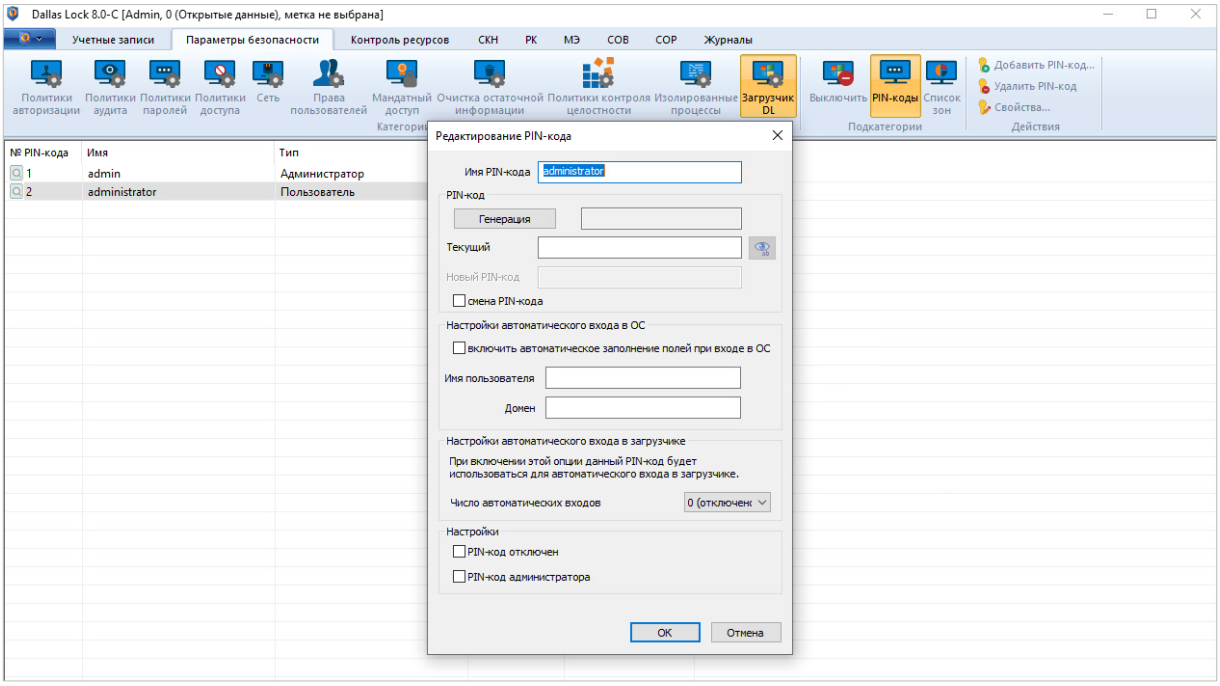


Рис. 98. Окно редактирования PIN-кода

Окно свойств PIN-кода содержит следующие заполняемые поля:

Наименование	Описание
Имя PIN-кода	Произвольное название для идентификации в списке
Текущий PIN-код	Поле доступно при редактировании уже созданного PIN-кода
Новый PIN-код	Значение PIN-кода, которое должно соответствовать установленным в СЗИ парольным политикам. Для изменения PIN-кода необходимо отметить поле *Смена PIN-кода*
Настройка автоматического	При включении и заполнении параметров этого блока для

Наименование	Описание
входа в ОС	пользователя, при вводе данного PIN-кода, поля для авторизации в Windows (*Имя пользователя* и *Домен*) будут автоматически заполнены указанными в блоке
Настройка автоматического входа в загрузчике	Данное Включение путем выбора числа входов позволит осуществлять вход в ОС, минуя заполнение поля ввода PIN-кода, т.е. автоматически через загрузчик, но с теми параметрами, которые указаны для данного PIN-кода
PIN-код отключен	Отмеченное флагом поле позволит вместо удаления временно отключить выбранный PIN-код
PIN-код администратора	Отмеченное флагом поле установит статус, с которым для данного PIN-кода станет доступна функция аварийного преобразования в загрузчике, раздел 21.1 Обратное преобразование жесткого диска в аварийном режиме.

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

4.7.3 Вход на компьютер при активном загрузчике

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

Вход на АРМ при активном модуле загрузчика происходит с предварительной авторизацией в загрузчике (рис. 99).

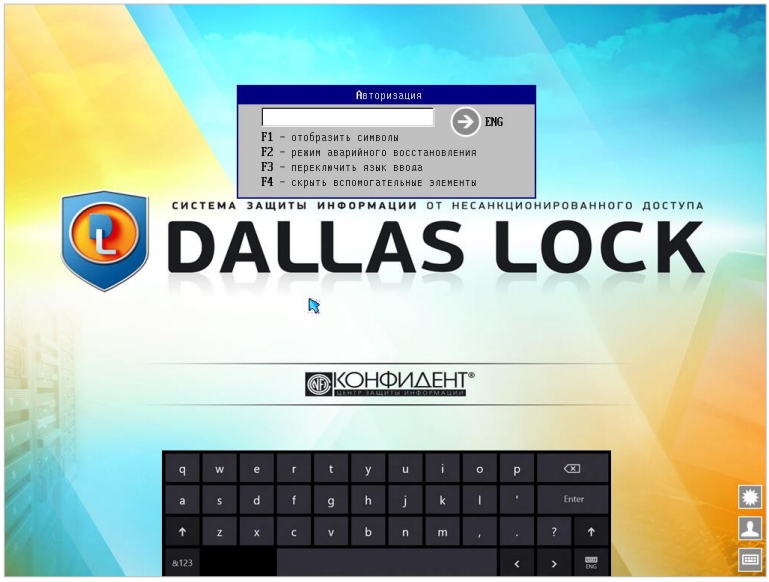


Рис. 99. Вход в модуле «Загрузчик DL»

Авторизация в загрузчике происходит без использования устройства «мышь». Для авторизации в загрузчике доступны только клавиши букв и цифр основной, цифр дополнительной клавиатуры, клавиши **Esc**, **Backspace**, **Enter**, **F1**, **F2**. Переключение раскладки клавиатуры происходит нажатием клавиши **F3**.

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

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

Далее вход на ПК будет осуществляться под индивидуальной учетной записью пользователя, раздел 2.6 Вход на защищенный компьютер.

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

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

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

В любом случае загрузка ОС в обход загрузчика **Dallas Lock 8.0** невозможна, если системный диск был преобразован 12.1 Прозрачное преобразование дисков.

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

4.7.4 Дополнительные условия работы модуля «Загрузчик DL»

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

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

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

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

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

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

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

В случае непредвиденной активации загрузчика на планшетном компьютере, не поддерживающем сенсорный ввод в BIOS, можно обойти ввод PIN-кода в загрузчике, активировав функцию автоматического входа в загрузчике для определенного PIN-кода через оболочку администратора, подраздел 4.7.2 Создание PIN-кода пользователя. Но следует учесть, что установленное ограничение количества срабатываний автоматического входа в загрузчике может полностью заблокировать вход на данный планшетный ПК.

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

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

5 РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ФС

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

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

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

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

Dallas Lock 8.0 позволяет разграничивать доступ к подключаемым устройствам, глава 10 КОНТРОЛЬ УСТРОЙСТВ.

5.1 Дескрипторы объектов

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

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

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

Дескрипторы объектов в свою очередь делятся на:

- дескрипторы дискреционного доступа — это дескрипторы, содержащие только параметры дискреционного доступа;
- дескрипторы мандатного доступа — это дескрипторы, содержащие только параметры мандатного доступа (только для Dallas Lock 8.0 редакции «С»);
- дескрипторы аудита — это дескрипторы, содержащие только параметры аудита;
- дескрипторы контроля целостности — это дескрипторы, содержащие только параметры контроля целостности.

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

В контексте данного руководства под понятием «дескриптор» будет пониматься окно с параметрами доступа выбранного объекта (рис. 100).

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

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

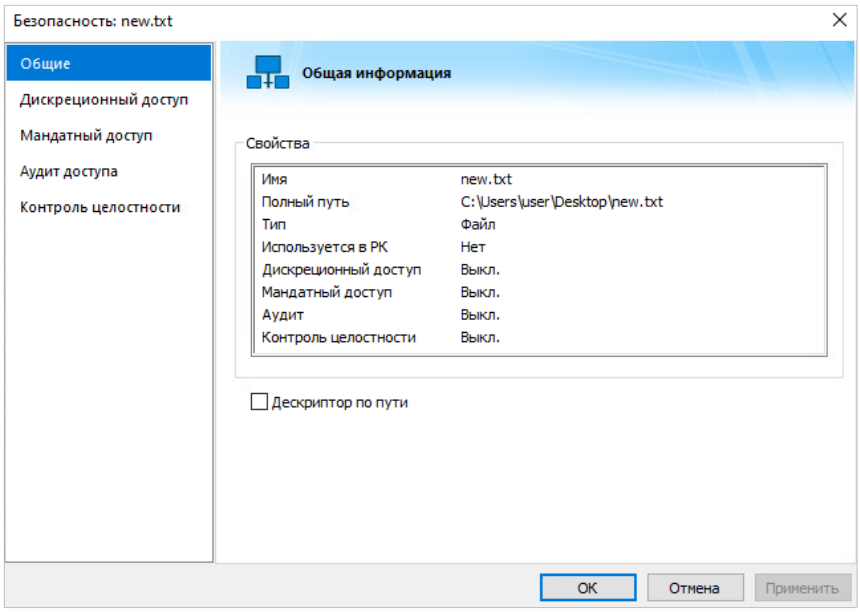


Рис. 100. Дескриптор объекта ФС

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

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

5.2 Дискреционный доступ

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

5.2.1 Права доступа

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

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

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

Каждый объект системы защиты характеризуется набором параметров безопасности. Каждый параметр безопасности контролирует определенную операцию (удаление, выполнение, изменение и другие), которая может быть произведена с объектом. Любая операция с объектом может быть разрешена либо запрещена пользователю. Соответственно каждый параметр может иметь значение *разрешить* или *запретить* (флаги в соответствующих полях).

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

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

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



Операции **Чтение разрешений** и **Изменение разрешений** доступны текущему пользователю, только если он обладает соответствующими полномочиями на просмотр параметров ресурсов и управление дискреционным доступом соответственно, раздел 3.6 Полномочия пользователей на администрирование системы защиты.

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

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

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

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



Если для какого-то объекта назначить параметры безопасности (права доступа, аудит или контроль целостности) и этот ресурс переименовать, то параметры безопасности сохранятся (за исключением случая назначения дескрипторов для пути, раздел 5.2.7 Дескрипторы по пути.



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



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

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

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

5.2.2 Механизм определения прав доступа пользователя к ресурсам ФС

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

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

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

Приоритеты параметров в **Dallas Lock 8.0** представляют собой следующую иерархию:

Таблица 6. Приоритеты параметров дескрипторов

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

Отдельными категориями в списке параметров выделены преобразованные (только для Dallas Lock 8.0 с модулем СКН) и открытые съемные накопители (FDD-диски, USB-Flash накопители). Данное разграничение имеет смысл, если в **Dallas Lock 8.0** настраивается доступ к преобразованным съемные накопителям, раздел 13.3 Преобразование съемных накопителей. В случае, когда нет преобразованных накопителей, все съемные накопители считаются открытыми и права должны назначаться именно для таких параметров.

В системе защиты реализован механизм назначения дискреционных прав как на глобальные параметры, раздел 5.2.3 Дискреционный доступ для глобальных параметров, так и на локальные объекты ФС, раздел 5.2.4 Дискреционный доступ для локальных объектов ФС и веток реестра.

Таким образом, система защиты последовательно выполняет следующие действия проверки:

1. Если для данного объекта ФС пользователю назначены права, то возможность совершения запрошенной операции устанавливается исходя из этих прав. Если параметру, контролирующему данную операцию, присвоено значение *Разрешить*, то операция выполняется. Если параметру присвоено значение *Запретить*, операция блокируется.
2. Если для данного объекта ФС не назначены права для данного пользователя, но права назначены для одной из групп, в которую входит пользователь, то для определения возможности совершения запрашиваемой операции аналогично используются права этой группы.
3. Если для данного объекта ФС не назначены права ни конкретно для данного пользователя, ни для какой-либо из групп, в которые входит этот пользователь, то для определения возможности совершения запрошенной операции используются права, назначенные группе «Все».
4. Если же права не назначены ни для пользователя, ни для какой-либо группы, куда этот пользователь входит, ни для группы «*Все*», то система защиты проверяет, входит ли данный объект в состав другого объекта (папка/диск). Если входит, то повторяются действия 1-3 для объекта, содержащего данный объект. Если объект не входит в состав другого объекта ФС,

то система защиты переходит к проверке глобальных параметров по иерархии, представленной в таблице.

5. Анализ глобальных параметров осуществляется по той же самой схеме, что и локальных. Проверяются права, назначенные для пользователя. Если они не назначены, то для групп, куда этот пользователь входит, и если права не назначены для таких групп, то проверяются права группы «*Все*». Если же и для группы «*Все*» не назначены права, то аналогично проверяются права глобальных параметров, имеющих более низкий приоритет. Если осуществлялась проверка глобальных параметров самого низкого приоритета, то выполнение операции разрешается.

Пример

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

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

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

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

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

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

5.2.3 Дискреционный доступ для глобальных параметров

Список глобальных параметров ФС расположен на вкладке **Контроль ресурсов** → **Глобальные** оболочки администратора **Dallas Lock 8.0** (рис. 101).

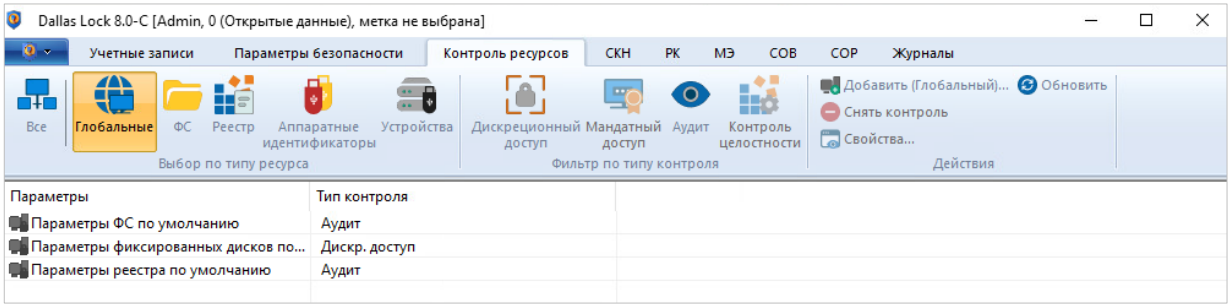


Рис. 101. Назначение глобальных параметров безопасности

Глобально права дискреционного доступа можно назначить:

Таблица 7. Глобальные дескрипторы

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

Назначение	Название параметра в Dallas Lock 8.0
на все приводы компакт-дисков на данном компьютере	«Параметры CD-ROM дисков по умолчанию»
на все съемные USB-Flash накопители, которые не были преобразованы (по умолчанию)	«Параметры открытых USB-Flash накопителей по умолчанию»
на все Floppy-диски на данном компьютере, которые не были преобразованы (по умолчанию)	«Параметры открытых FDD-дисков по умолчанию»
на все типы съемных накопителей, которые были преобразованы	«Параметры преобразованных съемных накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все съемные USB-Flash накопители, которые были преобразованы в **Dallas Lock 8.0**	«Параметры преобразованных USB-Flash накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все Floppy-диски на данном компьютере, которые были преобразованы в **Dallas Lock 8.0**	«Параметры преобразованных FDD-дисков по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
для всего реестра	«Параметры реестра по умолчанию»
на все типы аппаратных ключей	«Параметры аппаратных ключей по умолчанию»

Чтобы установить дискреционный доступ, необходимо выделить параметр и нажать кнопку **Свойства** на панели действий. Откроется окно редактирования параметров безопасности — дескриптор объекта, в котором необходимо выбрать закладку *Дискреционный доступ* (рис. 102).

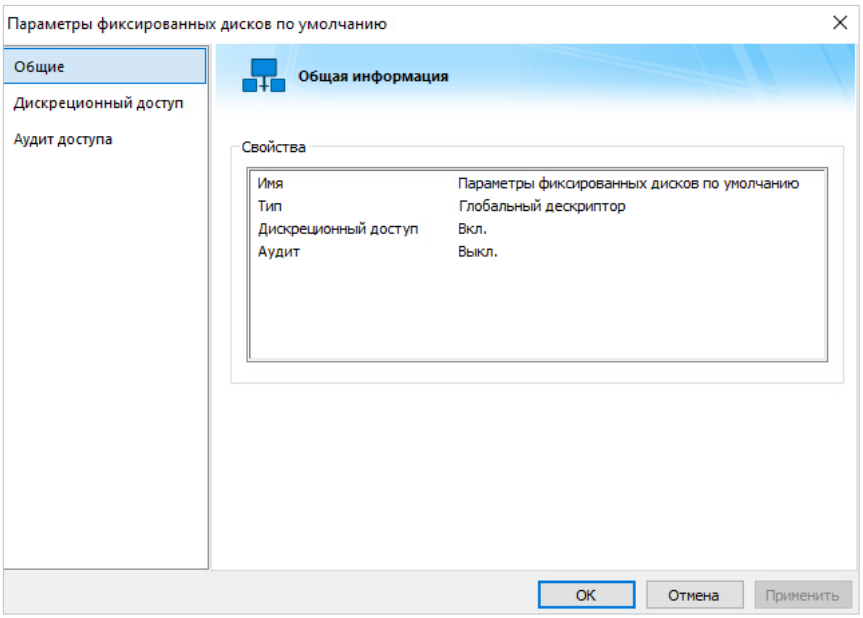


Рис. 102. Назначение прав дискреционного доступа

Чтобы назначить определенные дискреционные права для пользователей, необходимо:

1. Выбрать определенные учетные записи пользователей или групп. После нажатия кнопок **Пользователи** или **Группы** появятся типовые диалоговые окна с возможностью поиска учетных записей. Для выбора доменных учетных записей в поле *Размещение* необходимо выбрать имя домена, после чего появится список всех доменных учетных записей, зарегистрированные в **Dallas Lock 8.0** будут выделены особенным образом.
2. Для каждой учетной записи, пользователя или группы в списке необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту ФС (рис. 103).

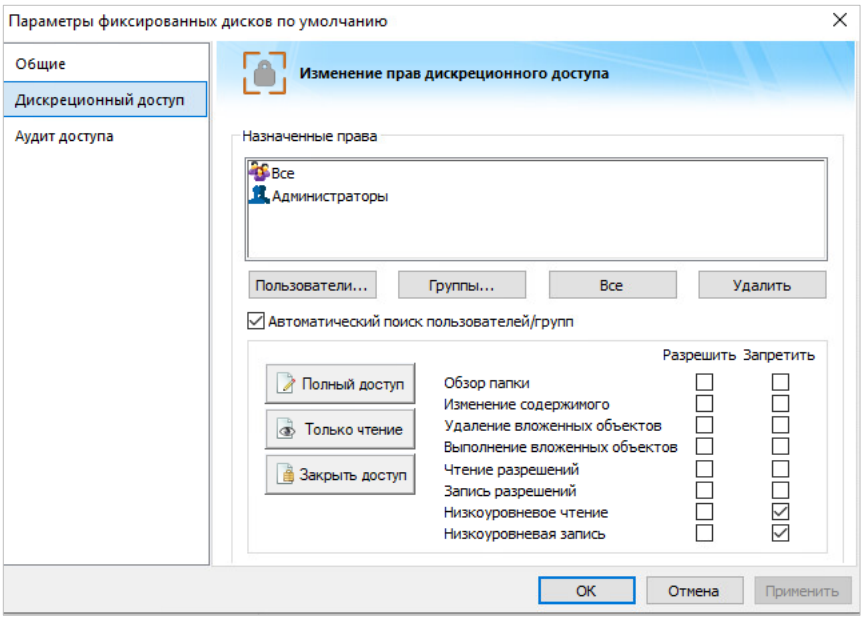


Рис. 103. Список прав дискреционного доступа

3. Далее нажать **Применить** и **ОК**.

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

5.2.4 Дискреционный доступ для локальных объектов ФС и веток реестра

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

1. Открыть его дескриптор безопасности, используя оболочку администратора **Dallas Lock 8.0** или контекстное меню объекта (для объектов ФС).
   - Открыть дескриптор с помощью контекстного меню значка объекта ФС можно, выбрав пункт меню **DL8.0: Права доступа** (рис. 104).



Рис. 104. Контекстное меню

   - Открыть дескриптор безопасности объекта ФС или ветки реестра через оболочку администратора **Dallas Lock 8.0.** Для фильтра *Дискреционный доступ* на вкладке *Контроль ресурсов* в меню действий выбрать **Добавить (Глобальный)**, **Добавить (ФС)** или **Добавить (Реестр)** в зависимости от типа ресурса (рис. 105).

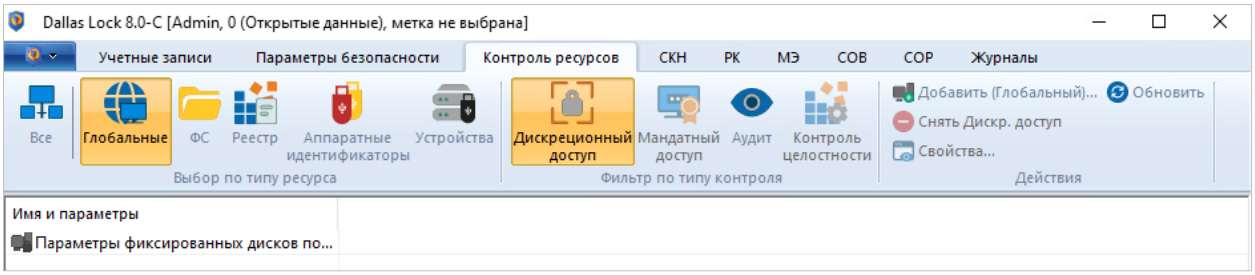


Рис. 105. Окно дискреционного доступа

В появившемся окне проводника (как в проводнике Windows) необходимо найти нужный ресурс, объект ФС или выбрать ветку реестра и нажать кнопку **Выбрать** или **Принять** (рис. 106,рис. 107, рис. 108). Для выбранного объекта откроется окно дескриптора.

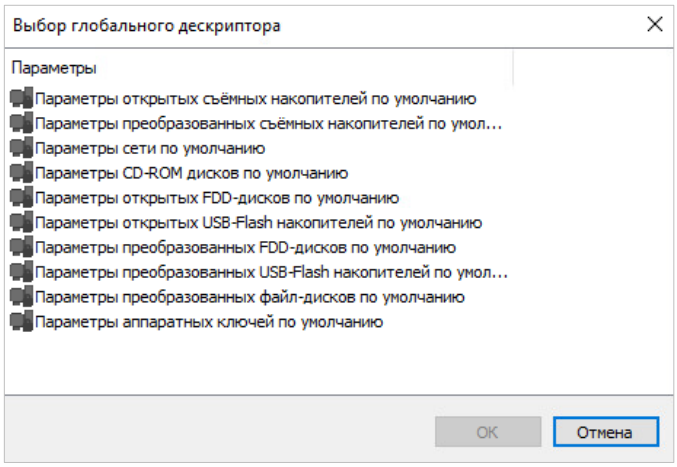


Рис. 106. Окно выбора глобального дескриптора

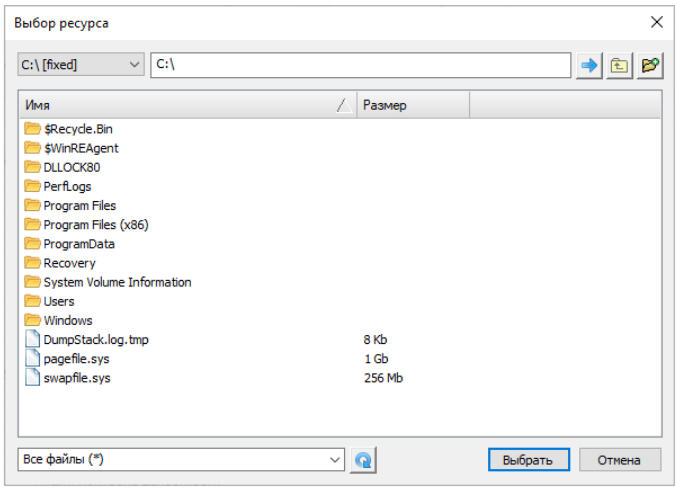


Рис. 107. Окно выбора объекта ФС

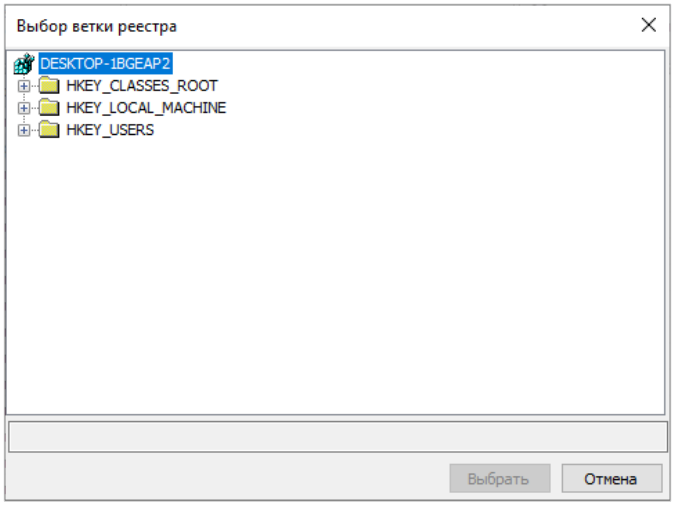


Рис. 108. Окно выбора ветки реестра

2. В окне дескриптора безопасности необходимо выбрать закладку *Дискреционный доступ* (рис. 109).

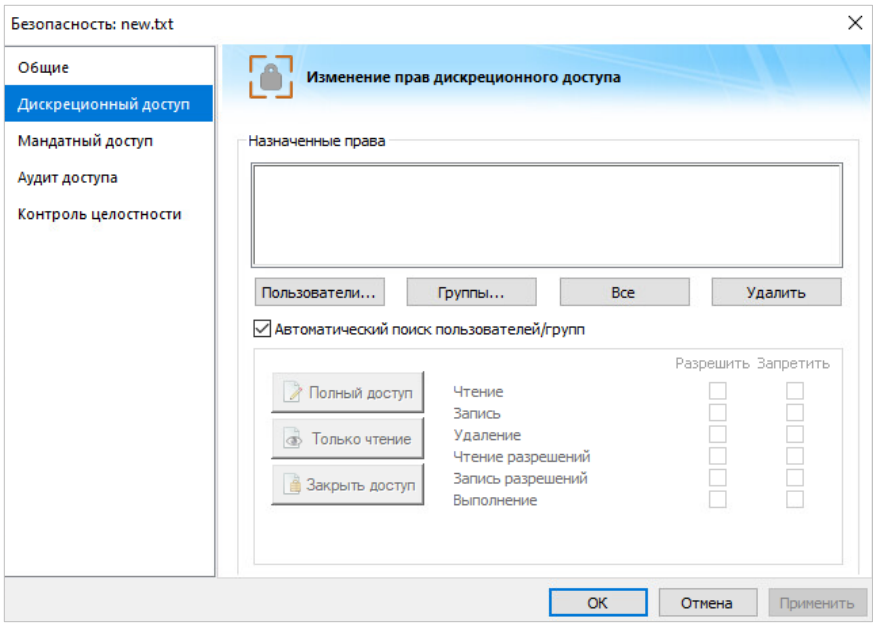


Рис. 109. Назначение прав дискреционного доступа

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

3. Чтобы назначить определенные дискреционные права для определенных пользователей, необходимо при помощи кнопок **Пользователь**, **Группы**, **Все**, **Удалить** выбрать определенные учетные записи пользователей или групп.
4. Для выбранных пользователей/групп необходимо задать набор разрешений/запретов, который будет определять права по доступу к данному объекту (рис. 110).

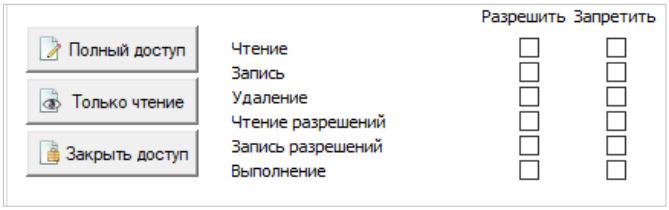


Рис. 110. Список прав дискреционного доступа

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

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

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

Права доступа к сетевым ресурсам

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

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

Локально установленная ОС Windows контролирует только локальные ресурсы. Система защиты **Dallas Lock 8.0** позволяет ограничивать доступ также и к сетевым ресурсам. Причем, если на удаленном компьютере, на который идет запрос, тоже установлена система защиты **Dallas Lock 8.0**, то права доступа будут проверяться два раза. Первый раз — локально установленной системой защиты **Dallas Lock 8.0** перед тем, как запрос отправится в сеть, и второй раз — удаленно установленной **Dallas Lock 8.0**, на которую придет запрос из сети.

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

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

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

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

Но с точки зрения **Dallas Lock 8.0** это разные пути, и поэтому, если назначены права на один из них, при обращении по другому пути права действовать не будут.

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

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

5.2.5 Дискреционный доступ к аппаратным идентификаторам

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

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

1. В оболочке администратора перейти на вкладку *Контроль ресурсов* и выбрать тип ресурса **Все** или **Аппаратные идентификаторы**. Выбрать фильтр по типу контроля **Дискреционный доступ** и нажать кнопку **Добавить (Апп. ид.)** (рис. 111).

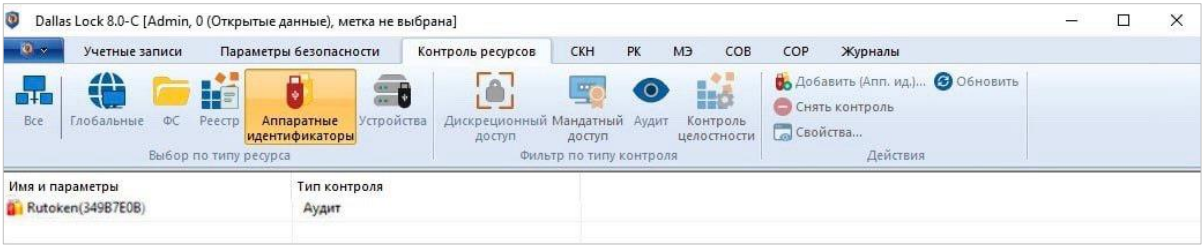


Рис. 111. Дискреционный доступ к аппаратным идентификаторам

В появившемся окне из выпадающего списка выбрать аппаратный идентификатор (рис. 112).

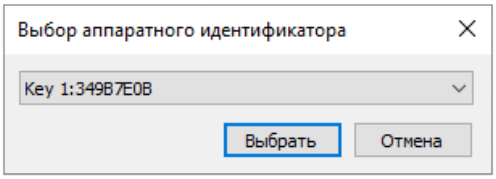


Рис. 112. Выбор аппаратного идентификатора

2. В окне дескриптора безопасности необходимо выбрать закладку *Дискреционный доступ* (рис. 113).

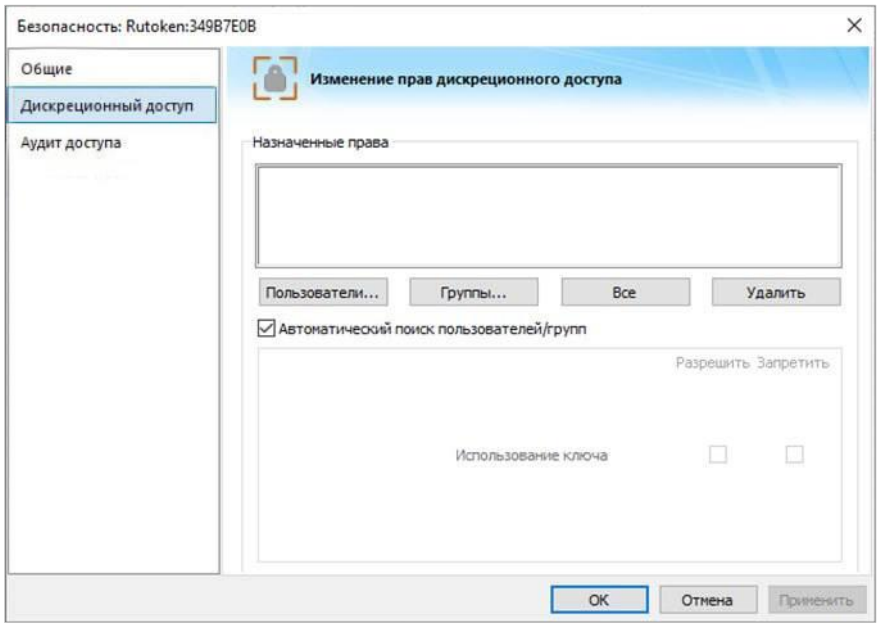


Рис. 113. Назначение прав дискреционного доступа

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

3. Чтобы назначить определенные дискреционные права для определенных пользователей, необходимо при помощи кнопок **Пользователь**, **Группы**, **Все**, **Удалить** выбрать определенные учетные записи пользователей или групп.
4. Для выбранных пользователей/групп необходимо указать, разрешено или запрещено использование ключа.

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

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

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

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

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

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

5.2.6 Низкоуровневый доступ к диску и съемным накопителям

Если пользователю не разрешен низкоуровневый доступ к диску и съемным накопителям, то он не сможет запускать программы, использующие прямой доступ к данным носителям информации на

ЗАРМ. Тем самым обеспечивается предотвращение НСД к информации и к работе с данными носителями информации при помощи таких программ.

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

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

Для того, чтобы назначить дискреционные права на низкоуровневый доступ к диску или съемному накопителю, необходимо установить соответствующий набор разрешений/запретов для дескриптора или глобального параметра (рис. 114).

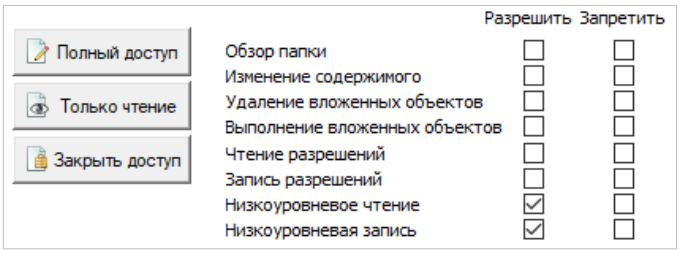


Рис. 114. Список прав дискреционного доступа

5.2.7 Дескрипторы по пути

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

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

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

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

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

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

Для того, чтобы создать дескриптор по пути, нужно в окне редактирования параметров объекта на вкладке *Общие* установить флаг в поле *Дескриптор по пути* (рис. 115).

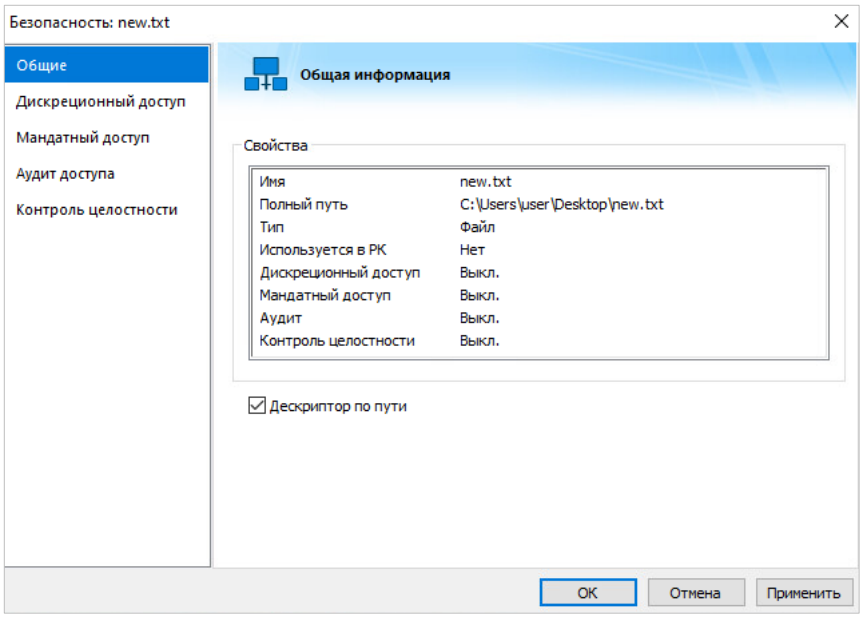


Рис. 115. Назначенный дескриптор по пути

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

Без необходимости использовать дескрипторы по пути не рекомендуется.

5.3 Мандатный доступ

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

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

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

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

   Согласно данному присвоению уровней доступа, пользователь, имеющий допуск уровня «Конфиденциальные данные», не может получить доступ к объекту с уровнем доступа «Секретные данные». В то же время, пользователь с допуском уровня «Секретные данные» имеет право доступа к объекту с уровнем «Конфиденциальные данные».
2. Неиерархическая категория — осуществляется сравнение мандатных меток объекта и пользователя. В случае совпадения мандатных меток объекта и пользователя пользователь получает доступ к объекту. В случае несовпадения мандатных меток объекта и пользователя доступ блокируется. Например, пользователь, имеющий мандатную метку «Метка 1», не может получить доступ к объектам с мандатными метками «Метка 2», «Метка 3» и т. д. Данный пользователь может получить доступ только к объектам с мандатной меткой «Метка 1». По умолчанию в **Dallas Lock 8.0** мандатные метки отсутствуют.

5.3.1 Настройки параметров мандатного доступа

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

Для настройки политик мандатного доступа необходимо на вкладке *Параметры безопасности* перейти в категорию **Мандатный доступ** и выбрать подкатегорию *Политики* (Рис. 116).

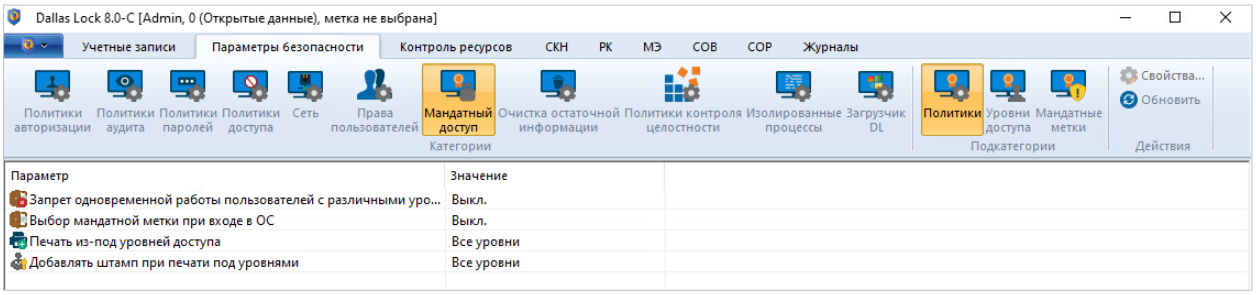


Рис. 116. Список политик мандатного доступа

Для настройки доступны следующие параметры:

Таблица 8. Настраиваемые параметры политик мандатного доступа

Запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа
При включении запрета одновременной работы пользователей с различными уровнями или метками мандатного доступа на данном ПК будет возможна одновременная работа нескольких интерактивных пользователей, зашедших только под одним уровнем доступа или мандатной метки. Причем данный уровень будет определяться по уровню или метке первого пользователя, зашедшего на данный компьютер. Если при включении запрета, есть уже запущенные сессии с различными уровнями доступа или мандатными метками, рекомендуется выполнить перезагрузку компьютера. Если не следовать данной рекомендации, может получиться, что суперадминистратор при блокировании своей запущенной сессии не сможет ее разблокировать в виду вступления в действия имеющегося ограничения.
Выбор мандатной метки при входе в ОС
Включение данного параметра разрешает использование мандатных меток для авторизации в ОС Windows.
Печать из-под уровней доступа
Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа, работая под которыми, пользователи могут осуществлять печать документов.
Добавлять штамп при печати под уровнями
Настройка данного параметра в дополнительном окне позволяет выбрать уровни мандатного доступа пользователей, при работе под которыми на распечатываемые документы будет добавляться штамп, который настроен параметром **Печатать/редактировать штамп.**

5.3.2 Переименование уровней доступа и мандатных меток

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

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

Для того, чтобы переименовать уровень доступа, необходимо в оболочке администратора на вкладке основного меню *Параметры безопасности* выбрать категорию **Уровни доступа**. Далее необходимо выделить уровень и с помощью кнопки или контекстного меню выбрать действие **Свойства** (рис. 117). В появившемся окне нужно ввести новое наименование и нажать **ОК**.

Переименование мандатных меток производится аналогичным образом в категории **Мандатные метки**.

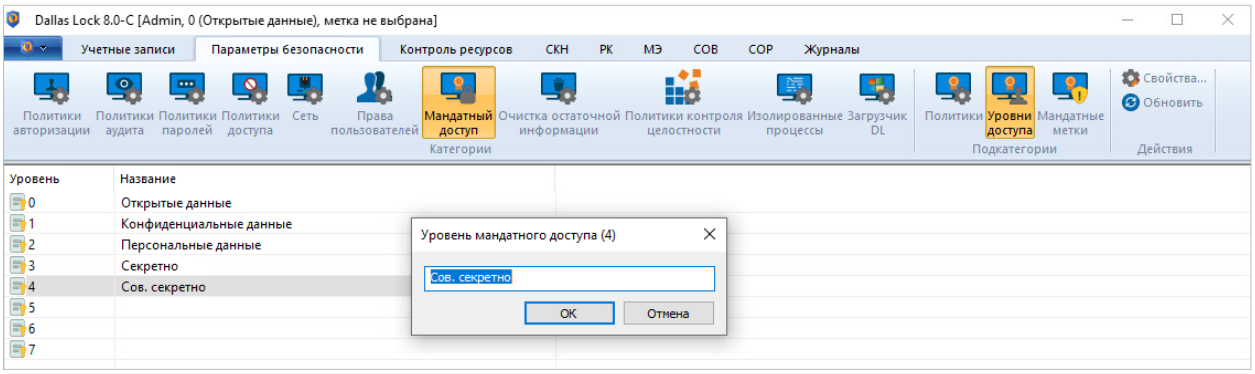


Рис. 117. Список уровней мандатного доступа

5.3.3 Уровни и метки доступа пользователей

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

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

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

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

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

Также следует учесть, что для работы с конфиденциальной информацией следует установить уровень или метку доступа на все ресурсы, необходимые пользователю для доступа к работе.

Для корректного отображения рабочего стола, возможно, потребуется сделать некоторые папки разделяемыми, раздел Настройка мандатного доступа с помощью механизма разделяемых папок.

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

5.3.4 Назначение мандатного доступа на объекты

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

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

1. Открыть его дескриптор безопасности, используя оболочку администратора **Dallas Lock 8.0** (на вкладке основного меню *Контроль ресурсов* выбрать тип ресурса и двойным кликом на объекте вызвать окно дескриптора или через контекстное меню объекта (пункт **Права доступа**).

   В дескрипторе объекта необходимо открыть вкладку *Мандатный доступ* (рис. 118).

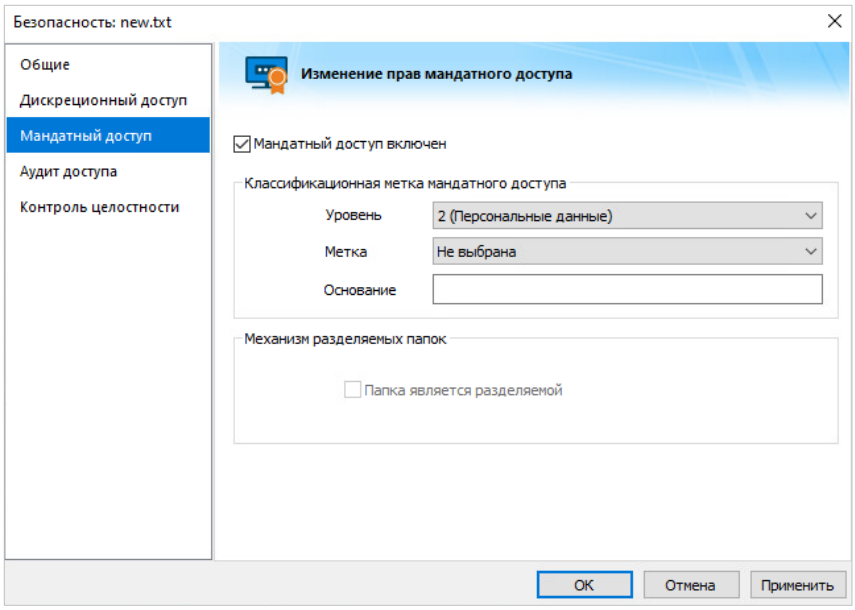


Рис. 118. Назначение прав доступа на объект ФС

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

Если мандатный доступ назначается на папку, то Включение механизма разделяемых папок (флаг в поле *Папка является разделяемой*) определит для этой папки особый статус, подраздел 5.3.6 Механизм разделяемых папок.

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

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

В окне категории **Мандатный доступ** (**Контроль ресурсов** → **Мандатный доступ**) контроля ресурсов формируется список всех установленных дескрипторов мандатного доступа на любых ресурсах (локальных, сетевых, съемных), установленных на данном защищенном ПК (рис. 119).

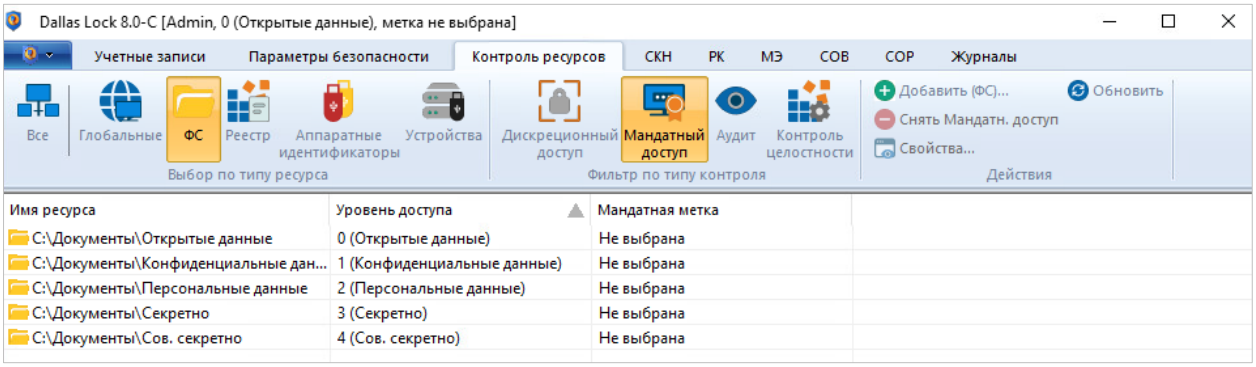


Рис. 119. Окно установленных дескрипторов мандатного доступа

5.3.5 Механизм разграничения мандатного доступа

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

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

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

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

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

5.3.6 Механизм разделяемых папок

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

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

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

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

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

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

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

Для того, чтобы пометить папку как разделяемую, нужно в контекстном меню «Права доступа» данной папки выбрать вкладку *Мандатный доступ*, включить мандатный доступ и поставить флаг в поле *Папка является разделяемой* (рис. 120), нажать кнопки **Применить** и **OK**.

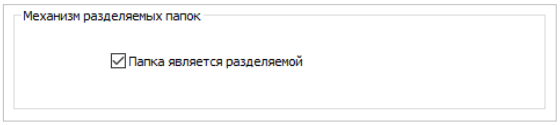


Рис. 120. Включение механизма разделяемой папки

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

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

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

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

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

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

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

5.3.7 Текущий уровень и метка доступа пользователя

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

При входе в ОС пользователь может выбрать:

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

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

1. Завершить текущий сеанс работы пользователя, и начать новый, выбрав при входе соответствующий уровень и метку доступа.
2. Воспользоваться пунктом **Свойства пользователя** из контекстного меню значка блокировки на панели задач BlockIcon (рис. 121).

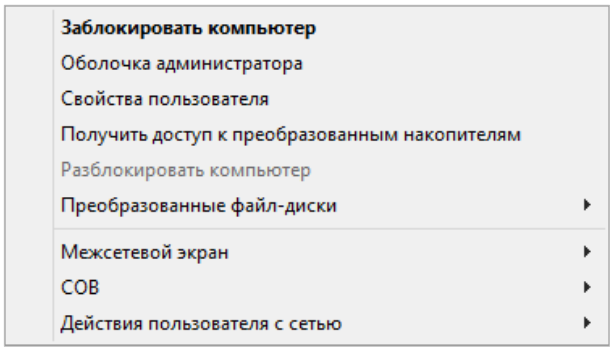


Рис. 121. Контекстное меню значка блокировки

Переключение мандатной метки через BlockIcon доступно только для суперадминистратора.

Смена мандатного уровня возможна в появившемся окне свойств текущего пользователя в поле выбора уровня доступа (рис. 122).

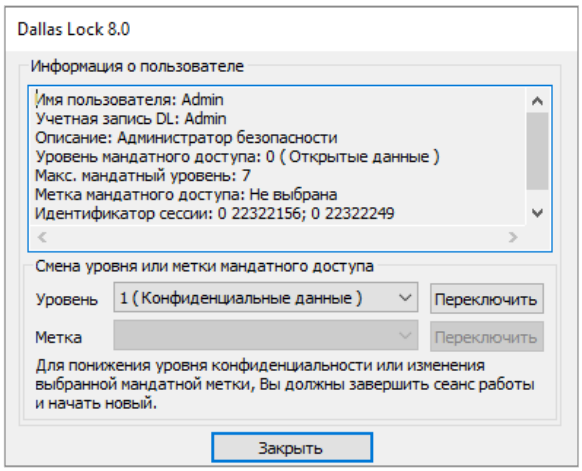


Рис. 122. Выбор уровня доступа в дополнительном окне значка блокировки

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

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

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

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

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

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

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

5.3.8 Служебный пользователь

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

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

С помощью соответствующего параметра в параметрах мандатного доступа[11] можно включить запрет на одновременную работу нескольких интерактивных пользователей, зашедших под разными уровнями или метками мандатного доступа.

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

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

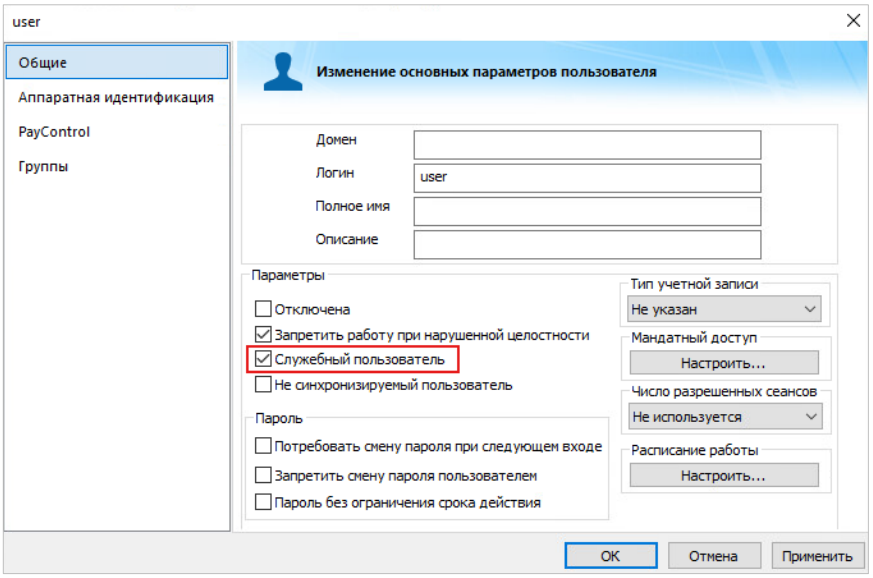


Рис. 123. Включение параметра «Служебный пользователь»

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

[11] «Запрет одновременной работы пользователей с различными уровнями или метками мандатного доступа».

5.3.9 Пример настройки мандатного доступа по сети

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

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

Для этого необходимо на сетевом ресурсе назначить мандатный доступ к данной папке «Secretno» (рис. 124).

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

Рис. 124. Пример настроенной сетевой папки на локальном ресурсе для мандатного доступа

На удаленном компьютере для сетевой папки «…\\имя_сетевого_ресурса\Secretno» назначить такой же мандатный доступ (рис. 125).

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

Рис. 125. Пример настроенной сетевой папки для мандатного доступа на удаленном ПК

На рис. 125 для папки по пути «NET:\\SECURITYS\Secretno\» присвоен уровень доступа 3 «Секретно», а мандатная метка не выбрана. В данном случае для пути прописано NetBIOS-имя ПК. Проверка доступа будет происходить по строке, и поэтому, если будут назначены права, используя путь с IP-адресом компьютера, то для пути с использованием NetBIOS-имени эти права работать не будут, необходимо дополнительно назначить мандатный доступ на данную папку, открыв ее по IP-адресу компьютера (рис. 126). И наоборот.

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

Рис. 126. Сетевая папка на клиенте с настроенным мандатным доступом через IP ПК

5.3.10 Настройка мандатного доступа для корректной работы пользователя с ПО

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

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

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

Настройка мандатного доступа с помощью механизма разделяемых папок

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

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

1. Определить уровень доступа для учетной записи пользователя.
2. Включить полный аудит отказов для параметров по умолчанию (вкладка **Контроль ресурсов → Глобальные → Параметры ФС по умолчанию**).

3. Включить «мягкий» режим контроля доступа, для этого нужно:
   - Открыть окно настройки неактивного режима (**кнопка основного меню → Настройка режимов работы → Настроить неактивный режим СЗИ**) и нажать кнопку **Мягкий режим,** раздел Мягкий режим.
4. Перезагрузить компьютер.
5. Зайти под учетной записью выбранного пользователя под его уровнем доступа.
6. Запустить необходимые приложения (например, MS Office Word или Excel) и выполнить необходимые операции.
7. Перезапустить ОС и зайти под учетной записью администратора безопасности.
8. В оболочке администратора открыть **Журнал ресурсов** (вкладка основного меню *Журналы*). В нем настроить и применить фильтр для просмотра отказов доступа необходимого пользователя (рис. 127).

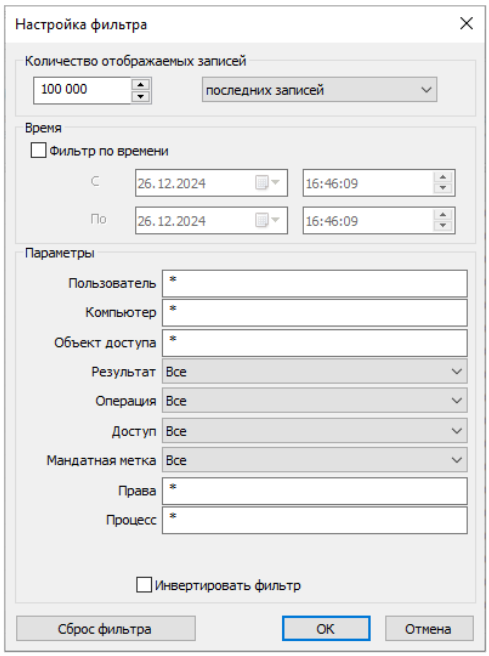


Рис. 127. Фильтр записей журнала доступа к ресурсам пользователя

9. Определить системную папку, из которой запускаются необходимые для пользователя приложения, и на данную папку назначить свойство разделимости, подраздел 5.3.6 Механизм разделяемых папок (рис. 128).

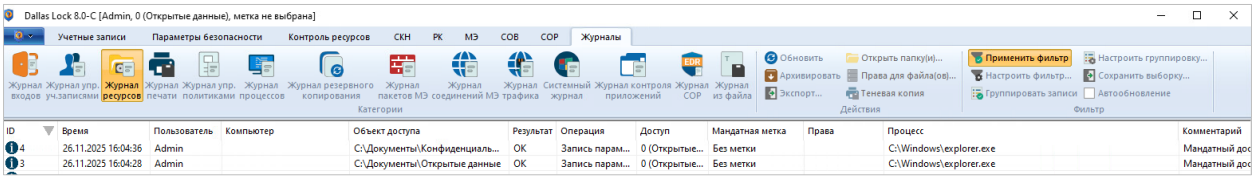


Рис. 128. Записи журнала доступа для определения разделяемой папки

10. Мягкий режим следует отключить.

Автоматическая настройка мандатного доступа

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

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

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

Перед автоматической настройкой мандатного доступа рекомендуется сохранить конфигурацию, глава 19 Сохранение конфигурации.

В отношении пользователей, для которых работа с программами настраивается с помощью мандатного доступа, необходимо выполнение следующих условий:

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

Чтобы применить шаблон мандатного доступа необходимо выполнить следующее:

1. Необходимо нажать кнопку основного меню и в списке дополнительных функций последовательно выбрать **Конфигурация → Шаблоны мандатного доступа** (рис. 129).

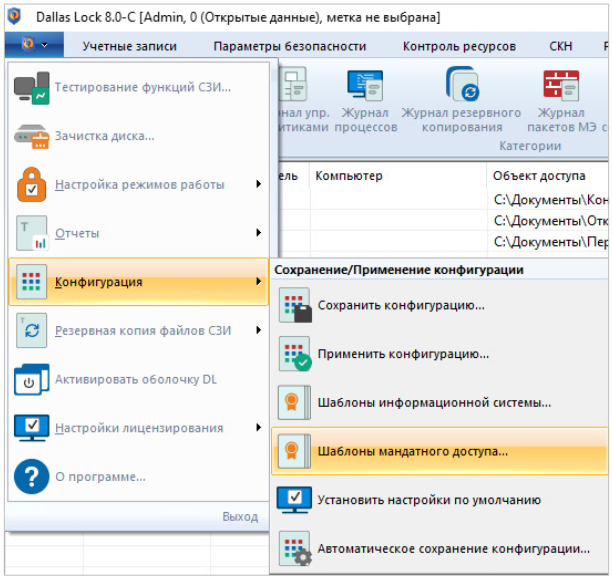


Рис. 129. Выбор автоматической настройки мандатного доступа

2. Появится окно со списком имеющихся шаблонов настройки мандатного доступа для определенных программ (рис. 130). В данном окне необходимо выбрать шаблон и нажать **ОК**.

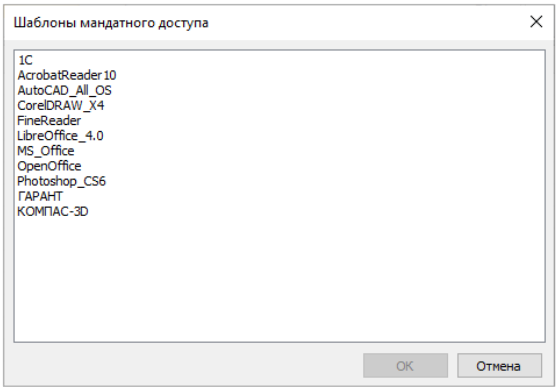


Рис. 130. Выбор шаблона для автоматической настройки

3. После выбора шаблона появится окно со списком учетных записей, для которых возможна настройка выбранного шаблона. Необходимо отметить нужных пользователей и нажать **ОК** (рис. 131).

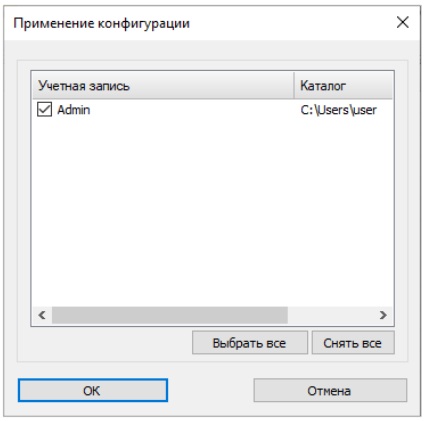


Рис. 131. Выбор учетных записей для настройки шаблона

После этого запустится настройка контроля доступа. В результате появится отчет о настройке.

В итоге применения шаблона выбранный пользователь сможет работать с программой в соответствии с правилами разграничения мандатного доступа, подраздел 5.3.5 Механизм разграничения мандатного доступа.

В списке настроенных ресурсов (**Контроль ресурсов** → **Мандатный доступ**) появятся записи о новых конфигурациях.

Отменить настройки, сформированные для мандатного доступа пользователей и ПО, можно следующими способами:

- применением сохраненного перед настройкой файла конфигурации;
- возвратом к настройкам по умолчанию (в этом случае также будут обновлены и удалены другие настройки параметров);
- сняв свойство разделимости и отключив мандатный доступ для ресурсов, на которые они были назначены в процессе применения шаблона, через список настроенных ресурсов.

5.4 Дополнительные режимы доступа

5.4.1 Режим обучения

В **Dallas Lock 8.0** реализован особый механизм контроля доступа к ресурсам — **режим обучения**. Он позволяет одновременно фиксировать события о запрете доступа и автоматически назначать права на ресурсы, к которым доступ блокируется.

Чтобы включить режим обучения, необходимо нажать кнопку основного меню и в списке дополнительных функций выбрать **Настройка режимов работы** → **Включить режим обучения** (рис. 132).

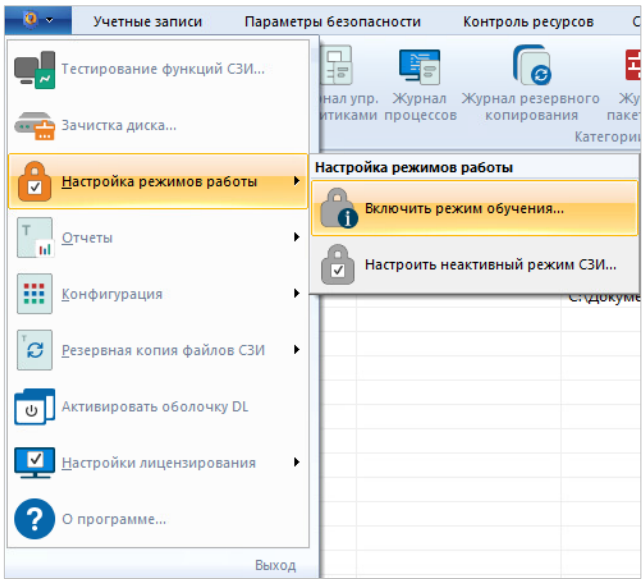


Рис. 132. Включение режима обучения

Появится окно подтверждения включения данного режима (рис. 133).

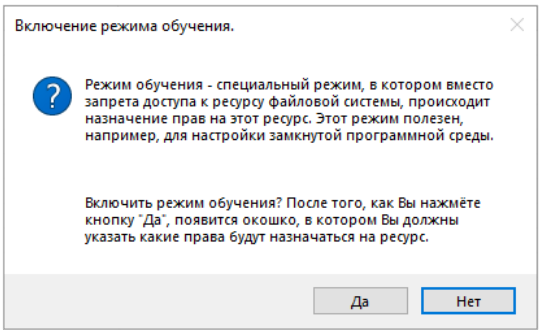


Рис. 133. Включение режима обучения

После включения режима обучения появится окно дескриптора доступа, в котором необходимо указать, какие параметры безопасности и какому пользователю должны быть автоматически назначены на ресурсы, к которым блокируется доступ. В процессе работы на необходимые для работы объекты ФС будет происходить назначение тех дескрипторов, которые настроены при включении режима обучения, тем самым определяется настройка ЗПС, подробный пример подраздел 5.4.3 Замкнутая программная среда.

Для включения/выключения режима обучения пользователь должен быть наделен правами на деактивацию системы защиты (вкладка **Параметры безопасности** → **Права пользователей** → параметр **Деактивация системы защиты**).

Одновременное использование «мягкого» режима и «режима обучения» невозможно.

Событие включения (выключения) режима обучения фиксируется в журнале управления политиками.

5.4.2 Неактивный режим

В **Dallas Lock 8.0** реализован особый механизм контроля доступа к ресурсам — **неактивный режим**. Его суть заключается в полном отключении подсистем **Dallas Lock 8.0**.

Чтобы включить и настроить неактивный режим, необходимо нажать кнопку основного меню и в списке дополнительных функций выбрать **Настройка режимов работы** → **Настроить неактивный режим** (рис. 134).

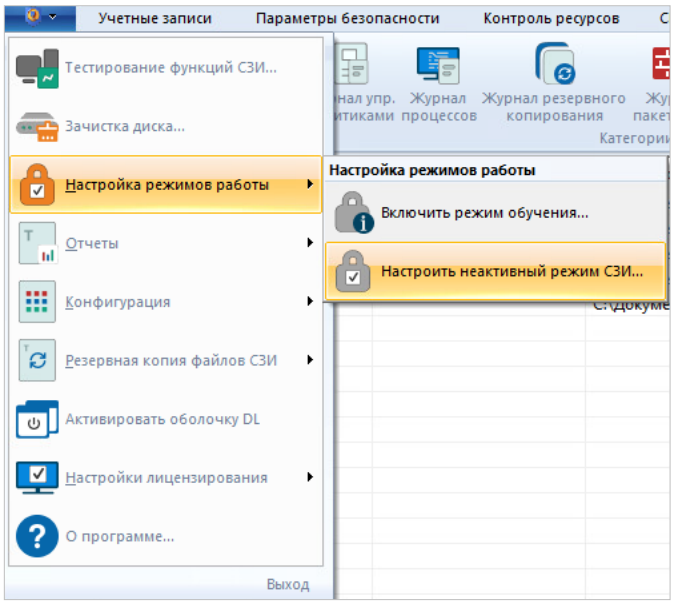


Рис. 134. Включение неактивного режима

Появится окно настройки неактивного режима (рис. 135), в котором необходимо определить, контроль каких подсистем отключить, а каких оставить.

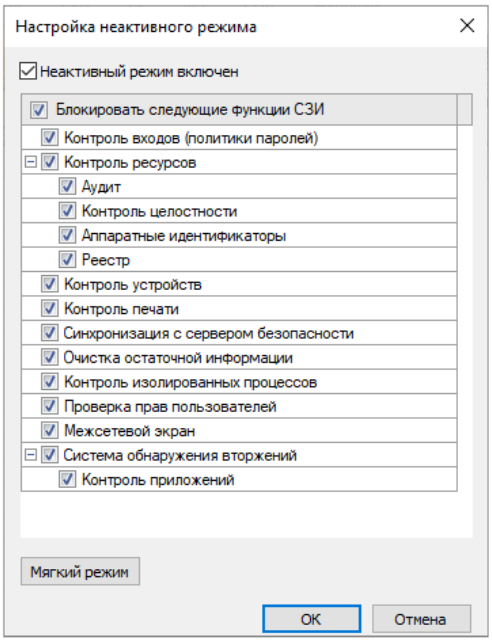


Рис. 135. Настройка неактивного режима

При активации поля *Контроль целостности* деактивируется возможность блокировки изменения файла HOSTS при настройке правил для контроля приложений (вкладка **СОВ → Параметры СОВ → Контроль приложений**).

В неактивном режиме **Dallas Lock 8.0** минимально влияет на работу ОС. Включение данного режима может быть полезно для упрощения диагностики несовместимости **Dallas Lock 8.0** со сторонним программным или аппаратным обеспечением, инфраструктурой сети и т. д.

Для включения/выключения неактивного режима пользователь должен быть наделен правами на деактивацию системы защиты (вкладка **Параметры безопасности → Права пользователей →** параметр **Деактивация системы защиты**).

Мягкий режим

Включение и настройка мягкого режима производится посредством неактивного режима, поэтому для того, чтобы включить и настроить **мягкий режим**, необходимо нажать кнопку основного меню и в списке дополнительных функций выбрать **Настройка режимов работы → Настроить неактивный режим**.

Далее откроется окно **Настройка неактивного режима**, где в правом нижем углу расположена кнопка **Мягкий режим**. Она позволяет включать комбинацию настроек, при которых при обращении к ресурсам, доступ к которым запрещен, доступ все равно разрешается, но в журнал ресурсов заносится сообщение об ошибке. Для этого необходимо настроить права доступа, назначить аудит отказов на необходимые объекты и включить **мягкий режим**.

События включения и выключения неактивного режима фиксируются в журнале управления политиками.

Включение режимов **режим обучения** и **неактивный режим** достаточно рискованно для обеспечения информационной безопасности, так как любой пользователь получает доступ к любому объекту ФС. Поэтому важно отключать эти режимы, когда в них нет необходимости.

Для напоминания о том, что включены данные режимы, при входе пользователя после загрузки ОС в области уведомлений Windows будет появляться всплывающее предупреждение (рис. 136).

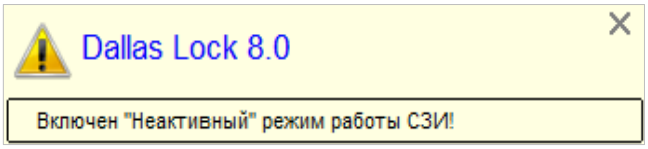


Рис. 136. Предупреждение о включенном неактивном режиме

5.4.3 Замкнутая программная среда

На одной рабочей станции может быть несколько пользователей, которые могут работать с разными программами в соответствии с политиками безопасности.

Для усиленных мер безопасности в системе **Dallas Lock 8.0** существует механизм **Замкнутой программной среды** (**ЗПС**, иногда говорят: **Изолированная программная среда** — **ИПС**), который позволяет явно указать, с какими программами пользователь может работать (соответственно, со всеми остальными программами пользователь работать не может).

Для реализации механизма замкнутой программной среды необходимо произвести ряд настроек. Общий смысл настроек состоит в том, чтобы установить глобальный запрет на выполнение всех программ, а потом разрешить запуск только тех приложений, которые необходимы данному пользователю для работы. Для организации **ЗПС** используются механизмы дискреционного контроля доступа, в частности, право *Выполнение*.

Для создания замкнутой программной среды рекомендуется все права назначать не для конкретного пользователя, а для специально созданной группы. В этом случае, если создать нового пользователя с теми же ограничениями на использования программ, достаточно будет добавить его в ту же самую группу, а не выполнять все настройки заново.

Первый вход только что созданного пользователя должен осуществляться без ограничений **ЗПС**, так как при первом входе в системной папке создается профиль пользователя. Таким же образом, если на компьютере установлен Microsoft Office, то, при первом входе нового пользователя до включения ограничений **ЗПС**, нужно запустить какое-либо приложение Microsoft Office, так как он производит локальную установку в профиль. Только после того, как профиль пользователя создан, нужные приложения установлены и инициализированы, можно начинать настройку **ЗПС** (либо добавлять пользователя в группу с **ЗПС**-ограничениями).

Нужно помнить, что исполняемыми файлами считаются не только файлы с расширениями «*.exe», но и все другие файлы, которые открываются с флагами на выполнение. Это, прежде всего, «*.dll», «*.sys», «*.scr» и прочие. Таким образом, если необходимо разрешить пользователю работать с Microsoft Word, то недостаточно будет ему разрешить запускать файл «WINWORD.EXE». Ведь «WINWORD.EXE» использует также множество «*.dll» файлов, которые тоже нужно разрешить данному пользователю для запуска.



Рекомендуется установить запрет на запись для всех разрешенных к выполнению программ. Тем самым блокируется возможность модификации и удаления этих программ.

Ниже приведены описания настройки **ЗПС** различными способами. Одним из альтернативных способов настройки может быть следующий. После глобального запрета запуска всего в глобальных параметрах, для пользователя (группы) необходимо разрешить запуск всего из папки «C:\WINDOWS». Главное — отключить возможность для этого пользователя (группы) менять содержимое этой папки. В папке Windows находятся важные системные файлы, доступ к которым необходим для корректной работы ОС. При этом способе настройки ничто не мешает отдельно запретить запуск некоторых файлов из папки Windows.

Настройка ЗПС с использованием неактивного режима

Для настройки ЗПС с использованием неактивного режима в системе защиты **Dallas Lock 8.0** существует дополнительный механизм **Права для файлов**. Пример такой настройки **ЗПС** описан ниже.

Пусть пользователь, для которого нужно организовать **ЗПС**, уже создан и инициализирован (к примеру, он называется zps). Далее для настройки **ЗПС** необходимо выполнить следующие шаги по настройке:

1. Создать специальную группу, например, ZPS-gr, и включить пользователя zps в группу ZPS-gr.
2. Для группы ZPS-gr в глобальных настройках запретить запуск всего (вкладка **Контроль ресурсов** → **Глобальные** → **Параметры ФС по умолчанию**») (рис. 137).

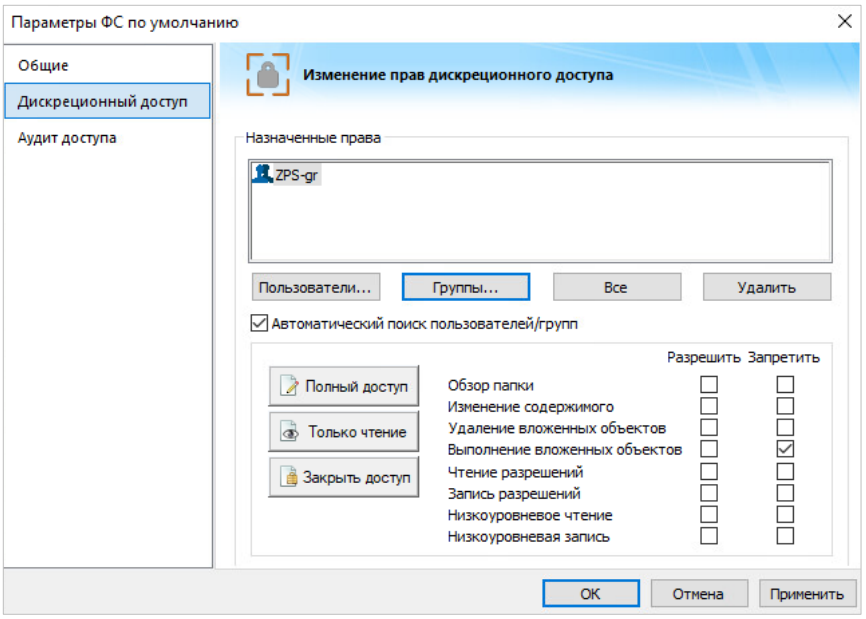


Рис. 137. Глобальный запрет запуска программ для настройки ЗПС

3. В дескрипторе **Параметры ФС по умолчанию** включить полный аудит отказов (рис. 138).

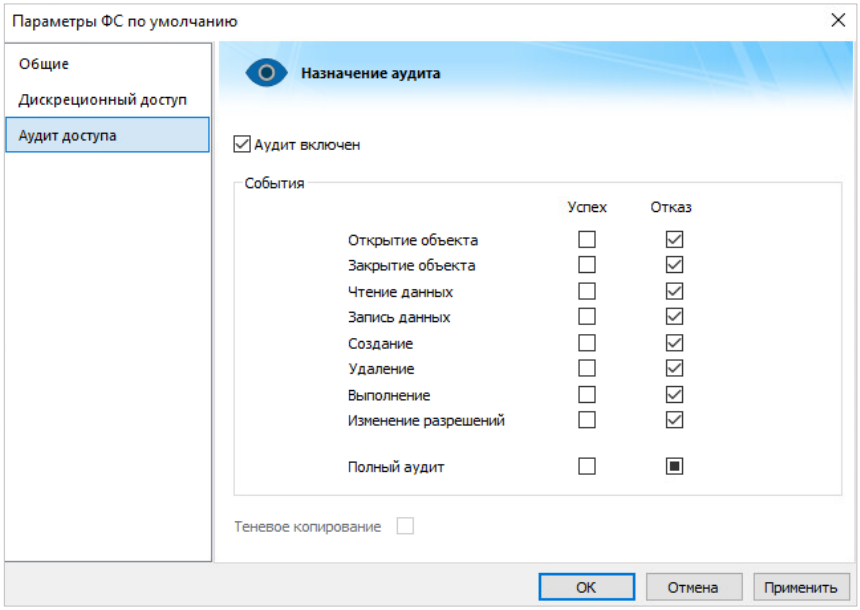


Рис. 138. Включение аудита доступа

4. Далее необходимо настроить неактивный режим работы **СЗИ** (пункт меню кнопки основного меню **Настройка режимов работы** → **Настроить неактивный режим**). В окне настройки необходимо включить Мягкий режим контроля доступа. Дополнительно желательно очистить (архивировать) журнал ресурсов.
5. Отправить компьютер в перезагрузку.

> Необходимо именно перезагрузить компьютер. Просто завершить сеанс работы одного пользователя и зайти под другим недостаточно — при загрузке компьютера используется другой набор исполняемых модулей. При смене пользователя событие загрузки ОС не попадет в журнал ресурсов, и в результате настройки ЗПС данным способом этот пользователь не сможет осуществить вход.

6. Осуществить вход в ОС под учетной записью пользователя zps. Запустить все те приложения, с которыми пользователь имеет право работать (но не запускать ничего лишнего).
7. Следует помнить, что не для всех приложений является достаточным просто их запуск. Некоторые сложные приложения на своем старте загружают не все исполняемые модули, а только необходимые, остальные модули они подгружают динамически, в процессе работы. Поэтому после запуска приложения лучше выполнить все основные действия приложения для работы.

8. На этом этапе в журнале доступа к ресурсам формируется список файлов, которые нужны данному пользователю для работы.
9. Далее следует осуществить смену пользователя и войти под учетной записью администратора безопасности. Запустить оболочку администратора **СЗИ**, открыть журнал ресурсов.
10. Настроить и применить фильтр журнала ресурсов: пользователь — «zps», результат — «*ошибка*» (рис. 139).

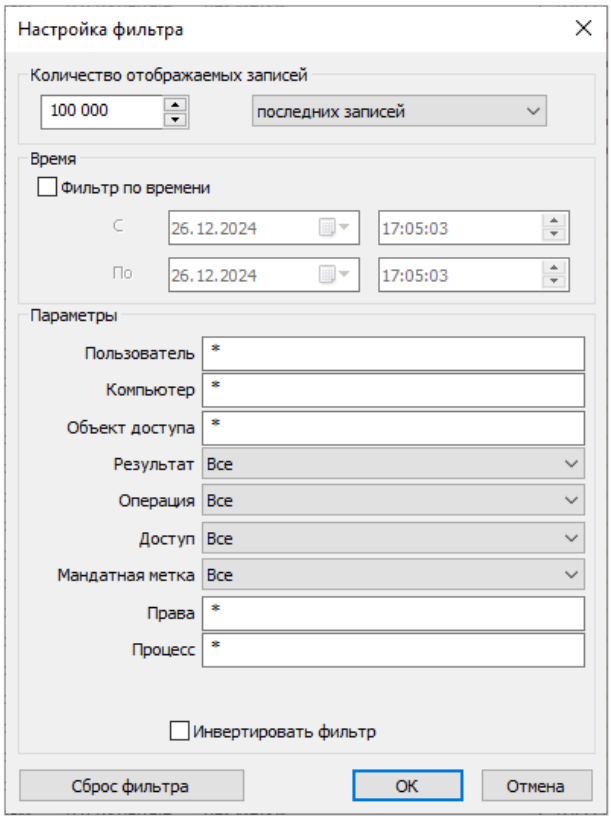


Рис. 139. Фильтр журнала доступа к ресурсам

11. Далее необходимо выделить поле с записями журнала и выбрать на панели действий **Права для файла(ов)** (или нажать эту кнопку в появившемся отдельном окне выбранной записи журнала или выбрать из контекстного меню) (рис. 140).

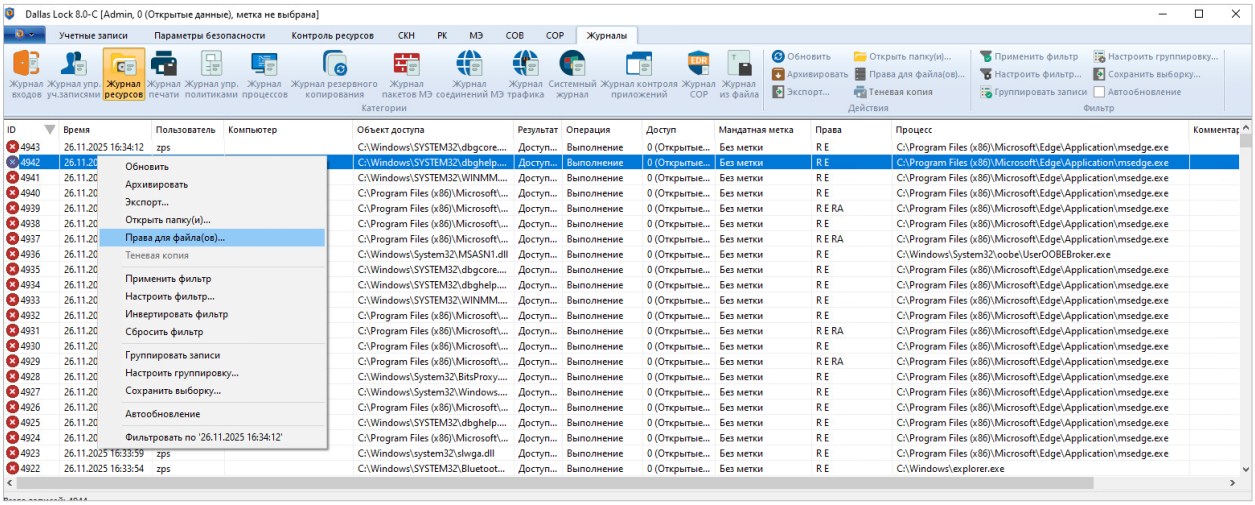


Рис. 140. Контекстное меню в журнале доступа к ресурсам

12. В появившемся окне редактирования дескриптора безопасности назначить дискреционные права для группы ZPS-gr «только чтение» и нажать **ОК** (рис. 141).

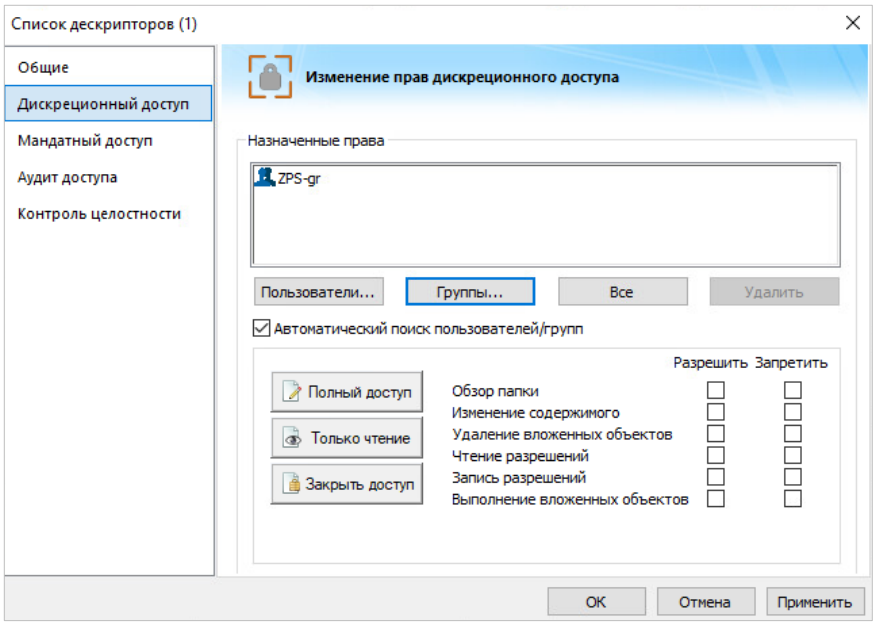


Рис. 141. Назначение дискреционных прав для файлов

После нажатия кнопки **ОК** система защиты попросит пользователя выбрать еще одно действие для настройки параметров безопасности (рис. 142).

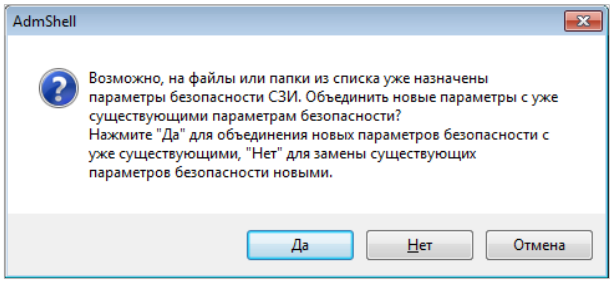


Рис. 142. Настройка параметров безопасности

13. В этом случае, если назначаются права на доступ к ресурсам для группы ZPS-gr впервые, то параметры безопасности будут созданы независимо от выбранного значения «Да» или «Нет». Если же необходимо добавить параметр (например, право запускать еще какую-либо программу), то в этом случае следует нажать кнопку **Да**, чтобы добавить параметр и не потерять существующие.
14. Таким образом, замкнутая программная среда организована. Теперь необходимо отключить **мягкий режим** и зайти пользователем zps. Этот пользователь сможет работать только с необходимыми программами.

Следует помнить, что вполне вероятна ситуация, когда не все нужные для работы пользователя исполняемые файлы занеслись в список. Так как некоторые приложения вызывают какие-либо другие исполняемые файлы только при активизации определенных функций. Если после включения ЗПС у пользователя zps какое-либо приложение стало работать неправильно — это можно сразу же увидеть в журнале доступа к ресурсам. Скорее всего, для какого-либо еще исполняемого файла необходимо добавить право на исполнение (действие **Права для файлов → Только чтение**) для данного пользователя (группы).

Настройка ЗПС с использованием режима обучения

Пусть пользователь, для которого нужно организовать замкнутую программную среду, уже создан и инициализирован (к примеру, он называется zps). Далее для настройки ЗПС, необходимо выполнить следующие шаги по настройке:

1. Как и в примере по настройке ЗПС с использованием неактивного режима описано выше, необходимо создать специальную группу, например, ZPS-gr, включить пользователя zps в группу ZPS-gr и для группы ZPS в глобальных настройках запретить запуск всего (рис. 137).
2. В списке дополнительных функций кнопки основного меню необходимо включить **Настройка режимов работы → Включить режим обучения**.
3. Далее, в появившемся окне дискреционного доступа назначить для выбранной группы параметр безопасности **только чтение**. Это просто сделать, нажав саму кнопку **только чтение**

(рис. 143).

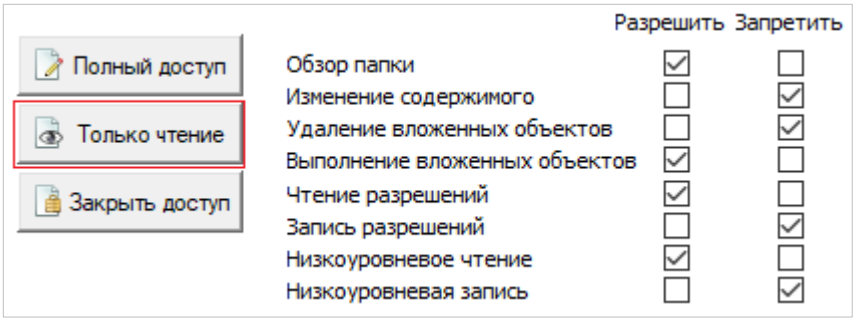


Рис. 143. Настройка прав доступа для режима обучения

4. Теперь необходимо перезагрузить компьютер и осуществить вход под учетной записью пользователя zps.
5. Поработать немного под этим пользователем, запустив необходимые приложения. В процессе работы в режиме обучения на запущенные приложения назначается дескриптор в соответствии с произведенной настройкой при включении режима.
6. В период пока включен режим обучения, пользователю zps становятся доступны для запуска все необходимые приложения.
7. Чтобы выключить режим обучения для пользователя, необходимо завершить его сеанс, зайти под учетной записью администратора и выбрать в дополнительном меню **Настройка режимов работы** → **Выключить режим обучения**. После выключения доступ к приложениям будет определяться в соответствии с назначенными правами в процессе режима обучения.

5.5 Графическая оболочка Dallas Lock

5.5.1 Включение и выключение оболочки

Вместо стандартной графической оболочки пользователя Windows (англ. Windows shell), программы, которая отвечает за создание рабочего стола, панели задач и меню **Пуск**, в **Dallas Lock 8.0** может использоваться специальная защищенная оболочка.

Оболочка **Dallas Lock** позволяет создавать защищенный рабочий стол без меню **Пуск** и панели задач, позволяя пользователю запускать только «ярлыки» приложений, определенные администратором. Такой режим может использоваться в дополнении к режиму Замкнутая программная среда, чтобы предоставить пользователю максимально ограниченный интерфейс, предназначенный только для выполнения профессиональных задач.

Для включения оболочки **Dallas Lock 8.0** необходимо в списке дополнительных функций кнопки основного меню выбрать пункт **Активировать оболочку DL** (рис. 144).

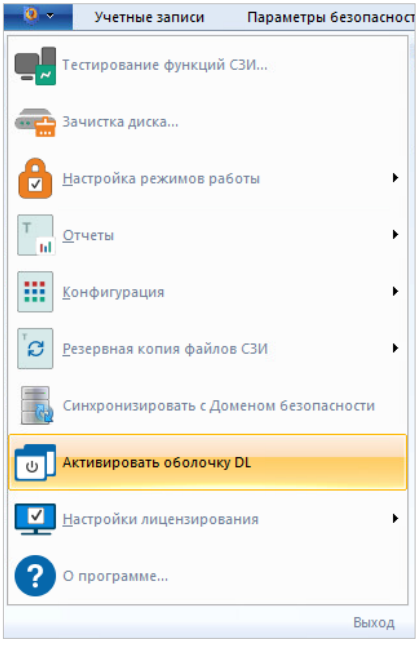


Рис. 144. Выбор установки оболочки Dallas Lock

Оболочка **Dallas Lock** будет применена для всех пользователей в ОС после завершения сеанса (выхода из системы) (рис. 145).

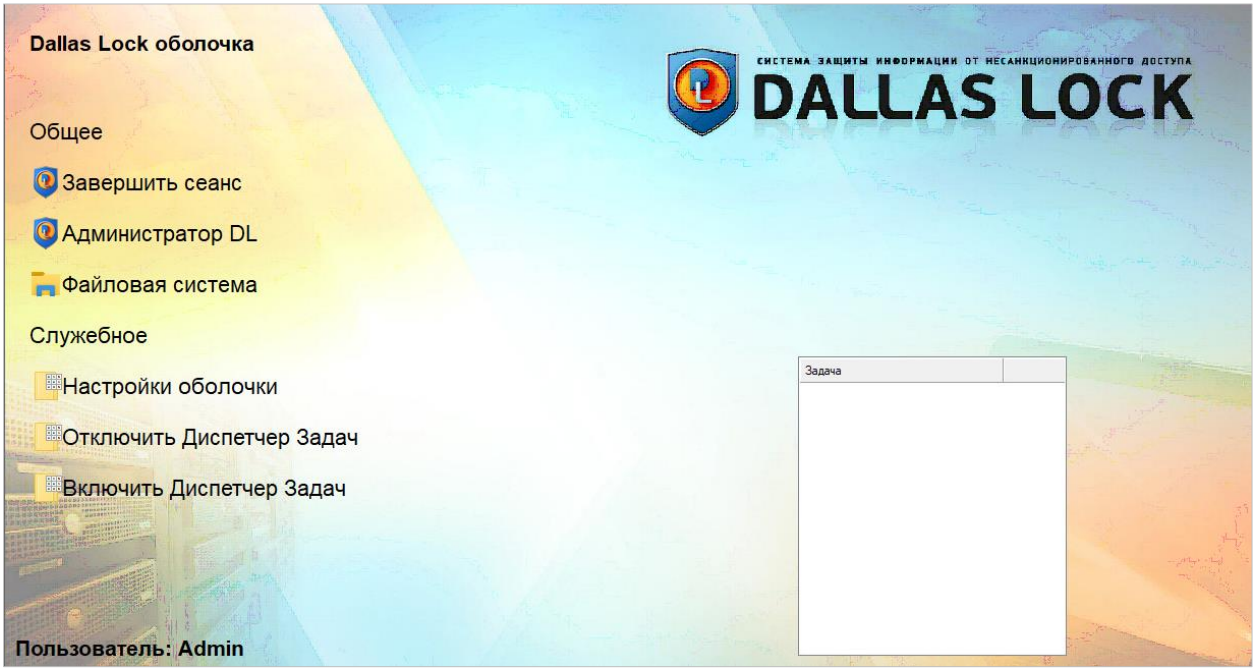


Рис. 145. Оболочка Dallas Lock

В правой части защищенного рабочего стола располагается список запущенных приложений, позволяющий пользователю переключаться между приложениями. Этот список является упрощенной версией диспетчера задач стандартной оболочки.

Основным механизмом ограничения оболочки **Dallas Lock** является блокировка меню **Пуск** и контекстного меню рабочего стола. Однако, пользователи, нажав комбинацию клавиш **Ctrl + Alt + Del**, могут запустить диспетчер задач и уже из него попытаться выполнить любое приложение (при наличии прав на запуск).

Чтобы исключить возможность запуска диспетчера задач и избежать лишних попыток пользователя перебирать приложения с правами на запуск, необходимо заблокировать диспетчер задач. Блокировка реализуется через групповые политики Windows. Настроить групповую политику для группы компьютеров можно через групповые политики AD, если используется домен AD, либо самостоятельно отредактировав локальную групповую политику локального компьютера. Оболочка **Dallas Lock** предоставляет возможность запустить редактор групповых политик и отключить диспетчер задач локально. Для этого в запущенной оболочке необходимо выбрать пункт **Отключить диспетчер задач**, после чего появится окно подтверждения действия (рис. 146).

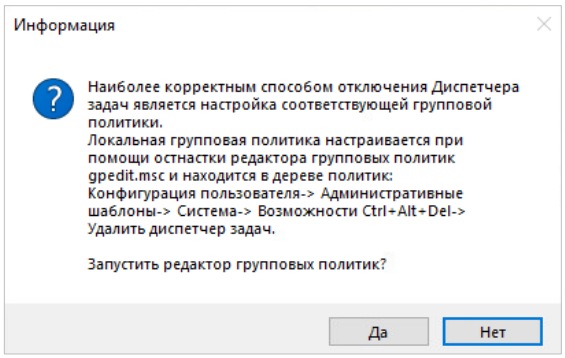


Рис. 146. Окно запуска редактора групповых политик

Следует учесть, что данная групповая политика применяется ко всем пользователям, работающим на данном компьютере.

Для применения нового значения необходимо завершить сеанс и снова войти в систему. Если политика настраивается через контроллер домена AD, то для ускорения применения политики на рабочих станциях перед выходом пользователя (с правами администратора) из системы требуется запустить утилиту gpupdate. После применения данной политики при попытке запуска диспетчера задач будет появляться сообщение «*Диспетчер задач отключен администратором*».

Для выключения оболочки **Dallas Lock** и включения графической оболочки Windows необходимо зайти в систему с правами администратора безопасности, и в списке дополнительных функций оболочки администратора, как и при включении, выбрать пункт **Активировать оболочку Explorer** и перезагрузить компьютер. Стандартная оболочка Windows станет доступной для всех пользователей.

5.5.2 Настройка оболочки

Все настройки оболочки **Dallas Lock** хранятся в файле «Zpsshell.ini» в системной папке «C:\Windows». Настройки позволяют определить внешний вид защищенного рабочего стола, список общих ярлыков для всех пользователей, а также список уникальных ярлыков для каждого пользователя (в том числе для доменных пользователей).

Изначально файл настроек содержит в себе пример настройки с установкой различных приложений для нескольких разных пользователей. Все настройки располагаются в различных секциях данного ini-файла и состоят из имени параметра и значения. Опираясь на примеры представленных настроек в данном файле, можно сформировать их для любого необходимого пользователя системы.

Среди общих настроек можно выбрать настройки фона оболочки, изменив его цвет или прописав путь к выбранному рисунку фона, а также изменить размер и расположение ярлыков и надписей. Следует помнить, что настройка параметров оболочки **Dallas Lock** доступна только пользователю с правами администратора и доступом к системной папке Windows. После изменения настроек для их применения необходимо завершение сеанса или перезагрузка.

6 ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА

6.1 Средства аудита

Важным средством обеспечения безопасности является механизм протоколирования. **СЗИ** должна фиксировать все события, касающиеся безопасности.

В процессе работы системы защиты **Dallas Lock 8.0** события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журналах. Ведение журналов в свою очередь регулируется параметрами аудита, задаваемыми пользователями с правами на управление аудитом. Система защиты позволяет осуществлять гибкую настройку аудита и выбирать, какие действия пользователя по отношению к каким ресурсам необходимо регистрировать. Можно протоколировать все действия, касающиеся администрирования системы защиты.

Просмотр и редактирование параметров аудита возможны в категориях **Политики аудита** и **Права пользователей** на одной из основных вкладок *Параметры безопасности* оболочки администратора.

6.1.1 Политики аудита

С помощью подсистемы аудита в **СЗИ** происходит регистрация событий и их группировка, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы.

Чтобы настроить параметры аудита, необходимо в основном меню оболочки администратора на вкладке *Параметры безопасности* выбрать категорию **Политики аудита** (рис. 147). В списке имеются следующие параметры:

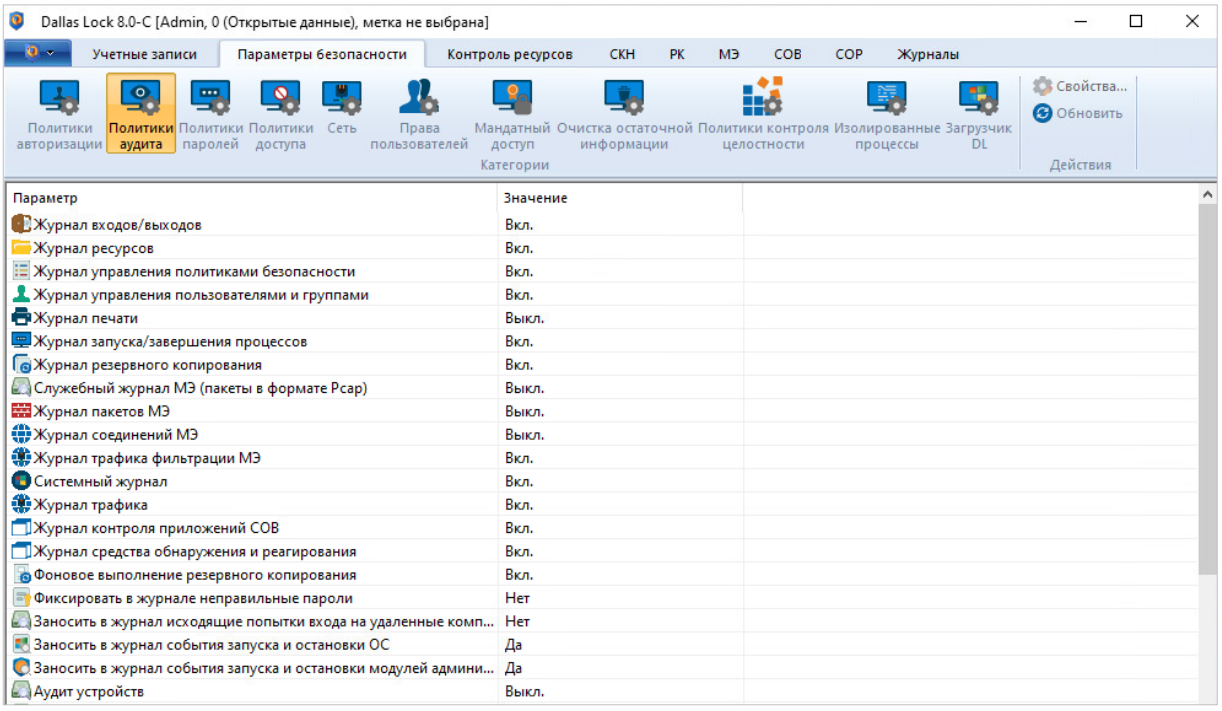


Рис. 147. Редактирование политик аудита

Доступны следующие параметры:

Таблица 9. Настраиваемые параметры безопасности подсистемы аудита

Журнал входов/выходов
Включение журнала позволяет протоколировать в нем события, связанные с входом, выходом, разблокировкой пользователей на ПК, включая как локальные, так и сетевые, в том числе терминальные входы и выходы. Параметр может принимать значение «*Вкл*» или «*Выкл*».

Журнал ресурсов
Включение журнала позволяет протоколировать в нем события по доступу к ресурсам ФС, программно-аппаратной среды и к устройствам (при включенном параметре **Аудит устройств** см. ниже). А также события очистки остаточной информации (при включении **Аудит событий зачистки**). Возможен аудит действий пользователей как с локальными ресурсами, так и с сетевыми. Сюда же заносятся события непосредственно по управлению доступом к ресурсам (в случае, когда на объект назначается любой дескриптор доступа, аудита, контроля целостности). Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал управления политиками безопасности
Включение журнала позволяет протоколировать в нем действия по настройке параметров системы защиты и по изменению прав пользователей. Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал управления пользователями и группами
Включение журнала позволяет вести в нем учет действий по созданию, удалению, редактированию учетных записей пользователей. Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал печати
Включение журнала позволяет протоколировать в нем события печати на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.). Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал запуска/завершения процессов
Включение журнала позволяет протоколировать в нем события запусков/завершения процессов в ОС. Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал резервного копирования
Включение журнала позволяет фиксировать в нем события по управлению заданиями резервного копирования, а также по запуску и завершению восстановления из резервных копий и удалению резервных копий.
Служебный журнал МЭ (пакеты в формате Pcap)
Включение данного журнала необходимо для создания файла со списком заблокированных пакетов в формате pcap (в случае возможных проблем детектирования пакетов) и может понадобиться при обращении в службу технической поддержки. Параметр может принимать значение «*Вкл*» или «*Выкл*».
Журнал пакетов МЭ
Включение журнала позволяет фиксировать все события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера. Параметр может принимать значение «*Вкл*» или «*Выкл*». Настройка правил осуществляется аналогично настройке правил **МЭ**, подраздел 15.2.5 Правила МЭ.
Журнал соединений МЭ
Включение журнала позволяет фиксировать сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами. Параметр может принимать значение «*Вкл*» или «*Выкл*». Настройка правил осуществляется аналогично настройке правил **МЭ**, подраздел 15.2.5 Правила МЭ.
Журнал трафика фильтрации МЭ
Включение журнала позволяет фиксировать проходящий сетевой трафик через контролируемые **МЭ** узлы сети. Параметр может принимать значение «*Вкл*» или «*Выкл*».

Системный журнал

Включение журнала позволяет фиксировать все важные события безопасности, генерируемые ОС и прикладным ПО.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Журнал трафика

Включение журнала позволяет фиксировать проходящий сетевой трафик через контролируемые СОВ узлы сети.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Журнал контроля приложений СОВ

Включение журнала позволяет фиксировать все события об активности приложений, их целостности и наборе загружаемых ими компонентов.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Журнал средства обнаружения и реагирования

Включение журнала позволяет фиксировать все события связанные с индикаторами компрометации и правилами автоматического реагирования **СОР** на их обнаружение.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Фоновое выполнение резервного копирования

Включение данного параметра (значение «*Вкл.*») позволяет понизить для задач резервного копирования приоритет выполнения потоков, обрабатывающих задачи резервного копирования.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Фиксировать в журнале неправильные пароли

Включение данного параметра позволяет фиксировать значения неверно введенных паролей в журнале входов (при условии, что журнал входов включен).

Параметр может принимать значение «*Да*» или «*Нет*».

> **!** При значении параметра *Да* возникает риск использования информации, содержащейся в столбце *Неверный пароль*, для скрытой компрометации паролей пользователей. Ошибки пользователей при вводе пароля неминуемо приведут к раскрытию части пароля, что может значительно облегчить для злоумышленника задачу его подбора.

Заносить в журнал исходящие попытки входа на удаленные компьютеры

Включение данного параметра позволяет регистрировать события исходящей попытки входа пользователя на удаленный компьютер через ЛВС в журнале входов (при условии, что журнал входов включен).

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Заносить в журнал события запуска и остановки ОС

Включение данного параметра позволяет регистрировать события, связанные с запуском/завершением работы ОС, события запуска/остановки ядра защиты **СЗИ**, в журнале управления политиками (при условии, что данный журнал включен).

Параметр может принимать значение «*Да*» или «*Нет*».

Заносить в журнал события запуска и остановки модулей администрирования DL

Включение данного параметра позволяет регистрировать события, связанные с запуском/завершением работы модуля администрирования **СЗИ** (**Dallas Lock**) в журнале управления политиками (при условии, что данный журнал включен).

Параметр может принимать значение «*Да*» или «*Нет*».

Аудит устройств

Включение данного параметра позволяет регистрировать события по доступу к подключаемым на данный ПК устройствам в Журнале ресурсов (при условии, что журнал ресурсов включен). Сами события настраиваются непосредственно в окне редактирования параметров дескриптора устройства (класса устройств).

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Аудит USB-накопителей

Включение данного параметра позволяет регистрировать попытки подключения определенных USB-устройств на данном ПК в Журнале ресурсов согласно выбранному значению:

- Незарегистрированных USB-накопителей.
- Зарегистрированных USB-накопителей.
- Всех USB-накопителей.

Для разрешения редактирования настроек политики необходимо включить параметр **Блокировать подключение незарегистрированных накопителей USB-Flash.**

Аудит событий зачистки

Включение данного параметра позволяет регистрировать события зачистки остаточной информации в следующих случаях:

- при включенных параметрах зачистки, раздел 8.2 Параметры очистки остаточной информации;
- при зачистке по запросу пользователя (пункт контекстного меню «Удалить и зачистить», раздел 8.3 Удаление файлов и зачистка остаточной информации по команде;
- при зачистке накопителя (функция Зачистка диска).

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Заносить в журналы ошибки ОС

Включение данного параметра позволяет вести учет ошибок доступа ОС Windows в журнале ресурсов (при условии, что журнал ресурсов включен). Так как **Dallas Lock 8.0** не подменяет механизмы контроля доступа к ресурсам ОС, а добавляет свои, то любое действие над ФС вначале попадает для проверки в драйвер защиты **СЗИ**, и, если этот драйвер разрешает данное действие, оно передается дальше ОС. ОС может отказать уже по своим причинам — эти отказы и протоколируются. В большинстве случаев аудит этих ошибок не требуется.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Аудит системных пользователей

Включение данного параметра позволяет вести учет действий системных пользователей (SYSTEM, LOCAL SERVICE, NETWORK SERVICE и пр.) в журнале ресурсов (при условии, что журнал ресурсов включен). В большинстве случаев, аудит этих пользователей не требуется.

Параметр может принимать значение «*Вкл*» или «*Выкл*».

Печатать/редактировать штамп

Включение и настройка параметров данной политики аудита позволяет на распечатываемых документах добавлять штамп, подраздел 7.2.3 Добавление штампа на распечатываемые документы.

Создавать теневые копии распечатываемых документов

Включение данного параметра (значение «*Да*») позволяет сохранять копии распечатываемых документов в отдельной папке по пути: «C:\DLLOCK80\Logs\PrintCopy». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства, подраздел 7.2.2 Теневые копии распечатываемых документов.

Управление хранилищем теневых копий отчуждаемой информации

Настройка данного параметра позволяет:

- задать размер хранилища теневых копий (по умолчанию – 150 Мбайт);
- задать время жизни теневой копии (по умолчанию 1 месяц);
- включить автоматическую перезапись при переполнении хранилища.



При заполнении хранилища теневых копий более чем на 85%, в Журнале управления политиками регистрируется событие с указанием текущей заполненности хранилища (в процентах).



При заполнении хранилища теневых копий более чем на 85%, регистрируется событие НСД с указанием заполненности хранилища (в процентах).

По умолчанию параметру задано значение «*Не используется*».

Выгрузка журналов
Настройка данного параметра в дополнительном окне позволяет: • экспортировать журналы **Dallas Lock 8.0** в журнал событий Windows; • экспортировать журналы **Dallas Lock 8.0** в SIEM систему с возможностью выбора из выпадающих списков формата выгрузки (Syslog, CEF или LEEF) и кодировки выгрузки (UTF-8 или CP1251). Для обоих типов экспорта возможно задать список экспортируемых журналов и определить период выгрузки журналов в диапазоне от 10 сек. до 24 часов.
Максимальное количество записей в журналах
Настройка данного параметра позволяет установить максимальное количество записей в определенном журнале. Параметр может принимать значение «*Не используется*» или «*100–20000*».
Периодическая архивация журналов
Включение данного параметра позволяет управлять периодами автоматической архивации журналов. После настройки данного параметра, все журналы по расписанию архивируются, все записи из них сохраняются в файл в системной папке «C:\DLLOCK80\Logs», записи журналов очищаются, и они начинают вестись заново. По умолчанию параметру задано значение «*Не используется*». Границы возможного временного интервала архивации варьируются от 1 часа до 1 года.

Для настройки аудита доступа к ресурсам недостаточно просто установить этому параметру значение «Включен» в окне редактирования параметров безопасности. Необходимо указать, какие именно операции по доступу, к каким именно ресурсам должны быть запротоколированы.

Аудит доступа к ресурсам нужно настраивать очень внимательно, так как в системе постоянно происходит множество событий, связанных с доступом к ресурсам ФС. К примеру, в процессе загрузки ОС происходит несколько тысяч таких событий. Если назначить аудит всех событий ФС, то журналы будут переполняться очень быстро, и в полученных журналах будет крайне сложно разобраться, а также будет иметь место замедление работы ПК. Поэтому рекомендуется назначать аудит только для необходимых ресурсов и событий.

6.1.2 Полномочия на просмотр и управление параметрами безопасности

Предоставить пользователю право на просмотр или управление параметрами аудита можно с помощью настройки параметров на вкладке **Параметры безопасности → Права пользователей** (рис. 148).

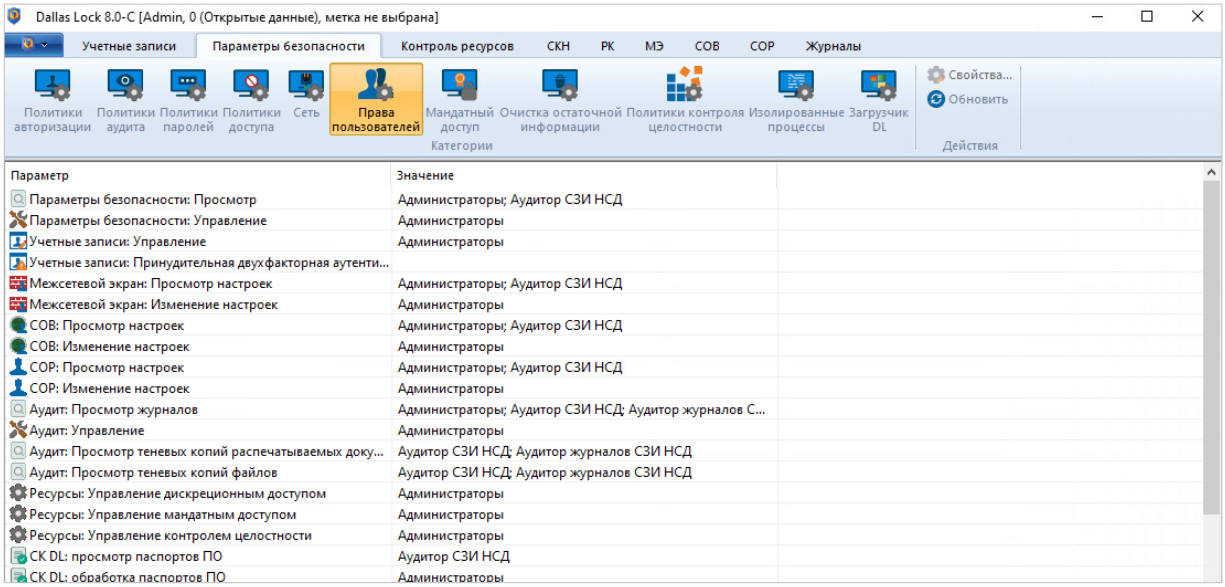


Рис. 148. Редактирование прав пользователей

Каждому пользователю, зарегистрированному в **СЗИ**, могут быть предоставлены следующие права аудита:

Таблица 10. Права пользователей на аудит

Право	Параметр безопасности («Параметры безопасности» → «Права пользователей»)
Право на просмотр теневых копий распечатываемых документов (копии создаются при условии, что включен параметр аудита «Создавать теневые копии распечатываемых документов», раздел 6.4 Теневое копирование	«Аудит: просмотр теневых копий распечатываемых документов»
Право на просмотр теневых копий файлов, раздел 6.4 Теневое копирование	«Аудит: Просмотр теневых копий файлов»
Право на просмотр только журналов в оболочке администратора СЗИ	«Аудит: Просмотр журналов»
Право на управление аудитом (назначение и редактирование назначенных параметров)	«Аудит: Управление»
Право на просмотр установленных параметров аудита (в том числе журналов)	«Параметры безопасности: Просмотр»

Для того, чтобы назначить право аудита пользователю, необходимо включить пользователя, учетную запись или группу пользователей в список для выбранного параметра. Для этого нужно выбрать параметр, нажать кнопку **Свойства** и добавить пользователей (или группы), воспользовавшись диалоговыми окнами **СЗИ** (рис. 149).

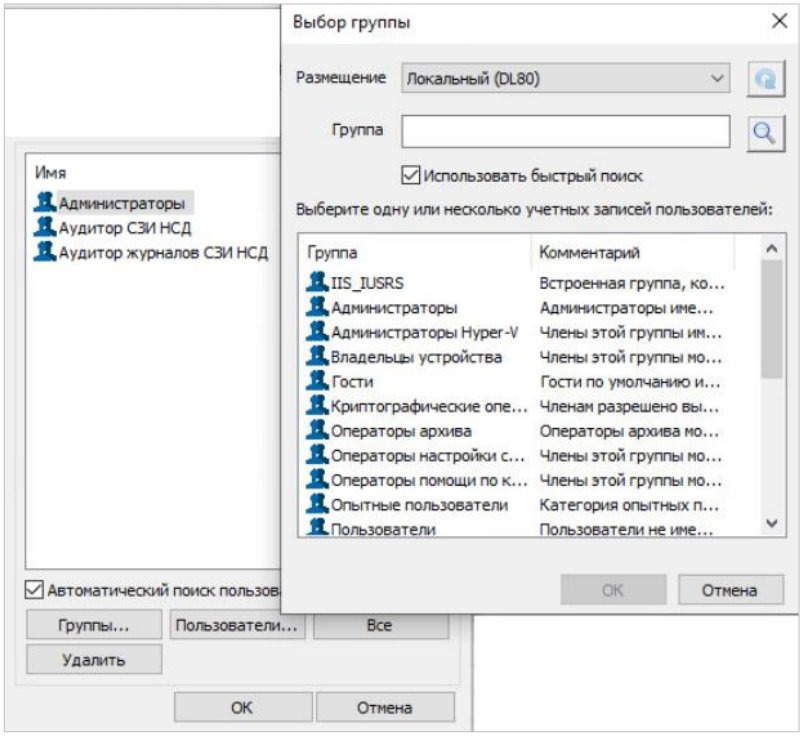


Рис. 149. Выбор пользователей для назначения просмотра параметров аудита

Для объектов у пользователей, не входящих в соответствующий список, нет возможности назначить аудит событий. При попытке просмотра назначенных параметров аудита пользователями, не входящими в список, установленный параметром для просмотра, выведется предупреждающее сообщение. Также будут заблокированы попытки просмотра теневых копий распечатываемых документов и теневых копий документов при копировании их на съемные и сетевые накопители.

В **Dallas Lock 8.0** по умолчанию реализовано создание двух групп пользователей с предустановленными правами аудита: группа *Аудитор СЗИ* и группа *Аудитор журналов СЗИ*. Члены этих групп автоматически получают права либо на просмотр установленных параметров аудита, в том числе журналов (*Аудитор СЗИ*), либо на просмотр только журналов **СЗИ** (*Аудитор журналов СЗИ*).

6.2 Аудит доступа

Аудит доступа к ресурсам в системе защиты настраивается как для глобальных, так и для локальных

объектов.

Аудит событий настраивается по принципу назначения дескриптора аудита для объекта. Для этого в дескрипторе объекта имеется закладка *Аудит доступа* со списком операций, которые могут быть запротоколированы в системе защиты.



Следует обратить внимание на то, что параметры настройки аудита не наследуются, а заменяются. То есть если, например, для папки «C:\Documents» назначить аудит успешного чтения, а в параметрах безопасности папки «C:\Documents\Secret» установить только аудит успехов записи, то для объектов из папки «C:\Documents\Secret» будет вестись аудит только успешной записи. Аудита успехов чтения для папки «C:\Documents\Secret» вестись не будет. Так как параметры аудита папки «C:\Documents\Secret» полностью перекрывают параметры аудита папки «C:\Documents». Благодаря такой особенности можно, например, снимать аудит с определенных объектов, находящихся в папке, для которой ведется аудит. Для этого достаточно у этого объекта в параметрах аудита выставить флаг *Аудит включен* и не ставить ни одного флага, отвечающего за события.

6.2.1 Аудит глобальных параметров

Список глобальные параметры ФС расположен на вкладке **Контроль ресурсов** → **Глобальные** оболочки администратора **Dallas Lock 8.0**.

Глобально параметры аудита можно задать:

Таблица 11. Глобальные дескрипторы

Назначение	Название параметра в Dallas Lock 8.0
на все ресурсы ФС	«Параметры ФС по умолчанию»
на жесткие диски, в том числе на устройства типа внешний жесткий диск USB	«Параметры фиксированных дисков по умолчанию»
на все сетевые ресурсы	«Параметры сети по умолчанию»
на файл-диски, которые были преобразованы	«Параметры преобразованных файл-дисков по умолчанию»
на все типы съемных накопителей, которые не были преобразованы, кроме CD-ROM дисков (по умолчанию)	«Параметры открытых съемных накопителей по умолчанию»
на все приводы компакт-дисков на данном компьютере	«Параметры CD-ROM дисков по умолчанию»
на все съемные USB-Flash накопители, которые не были преобразованы (по умолчанию)	«Параметры открытых USB-Flash накопителей по умолчанию»
на все Floppy-диски на данном компьютере, которые не были преобразованы (по умолчанию)	«Параметры открытых FDD-дисков по умолчанию»
на все типы съемных накопителей, которые были преобразованы	«Параметры преобразованных съемных накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все съемные USB-Flash накопители, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных USB-Flash накопителей по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
на все Floppy-диски на данном компьютере, которые были преобразованы в Dallas Lock 8.0	«Параметры преобразованных FDD-дисков по умолчанию» (только для Dallas Lock 8.0 с модулем СКН)
для всего реестра	«Параметры реестра по умолчанию»
для всех аппаратных идентификаторов	«Параметры аппаратных ключей по умолчанию»

Чтобы назначить события аудита для параметра, необходимо:

1. Выделить глобальный параметр и нажать **Свойства**. Откроется окно редактирования параметров — дескриптор объекта. Необходимо выбрать вкладку *Аудит доступа* (рис. 150).

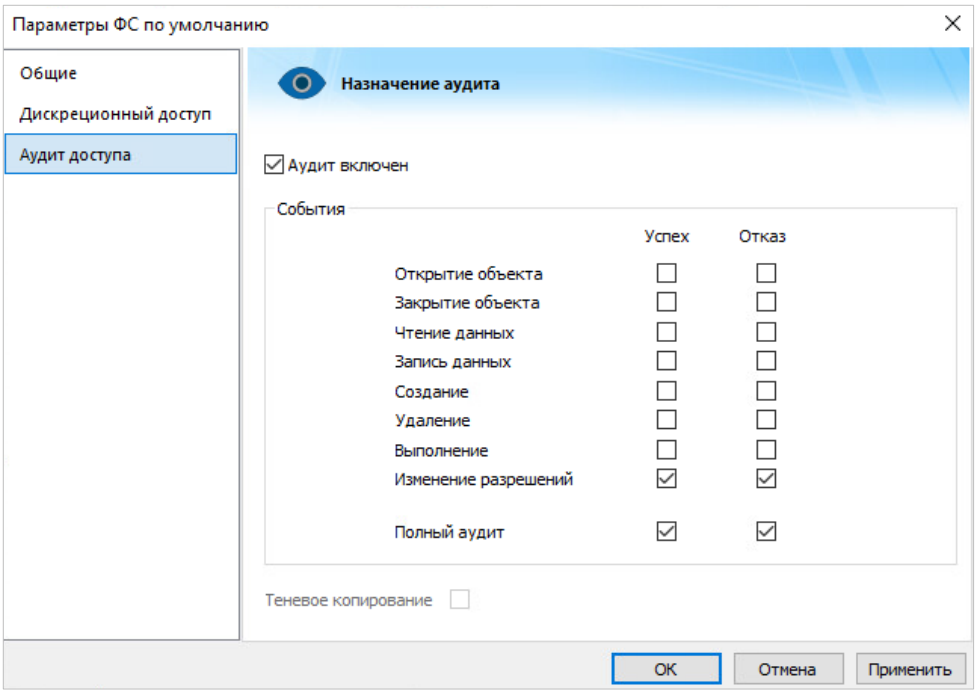


Рис. 150. Окно назначения аудита на ресурс ФС

2. Перед выбором событий необходимо включить аудит: отметить флагом поле *Аудит включен*.
3. В зависимости от того, успешное или неудачное событие нужно зарегистрировать, выставить флаг в полях *Успех* или *Отказ* для операции.

   Отмеченные события будут заноситься в журнал ресурсов. Если одновременно отметить и *Успех*, и *Отказ*, то в журнал, соответственно, будут заноситься и успешные события, и неуспешные.

   Отмеченное флагом поле *Полный аудит* позволяет автоматически расставить значения успеха или отказа во всех полях и вести аудит по всем позициям.

6.2.2 Аудит локальных объектов ФС и веток реестра

Чтобы установить событие аудита для конкретного объекта ФС или ветки реестра, необходимо выполнить следующие действия:

1. Открыть дескриптор безопасности объекта, используя оболочку администратора **Dallas Lock 8.0 (Контроль ресурсов → Все**, выбрать фильтр по типу контроля *Аудит* и нажать кнопку **Добавить (Глобальные)**, **Добавить (ФС)** или **Добавить (Реестр)**, или через контекстное меню объекта (пункт **Права доступа** для объекта ФС) (рис. 151).

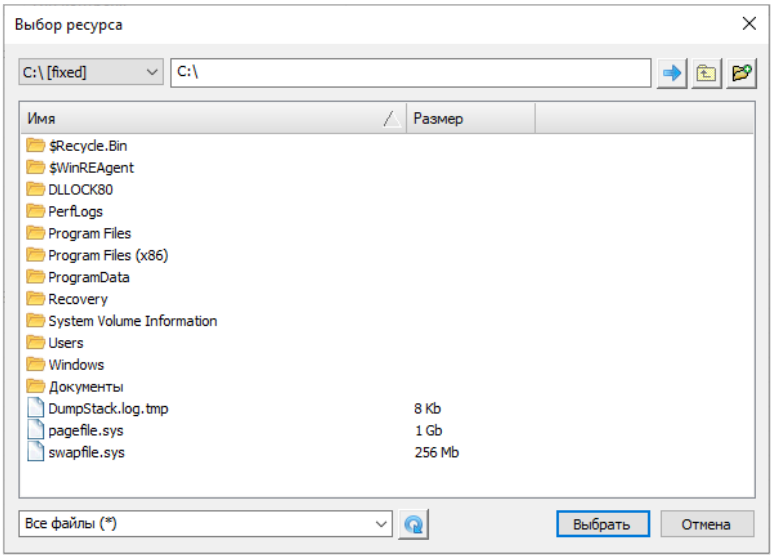


Рис. 151. Выбор ресурса для назначения аудита

2. В дескрипторе объекта открыть закладку *Аудит доступа*.

3. Включить аудит (отметить флагом поле *Аудит включен*), и отметить события *Успех* или *Отказ* по выбранным операциям.

Объекты, для которых назначен аудит любым из способов, автоматически появляются в списке объектов выбранного фильтра по типу контроля *Аудит* на вкладке **Контроль ресурсов**.

6.3 Журналы

В системе защиты **Dallas Lock 8.0** регистрация и запись событий ведется в различных типах журналов. Для удобства выделены 13 основных журналов.

1. Журнал входов.
2. Журнал управления учетными записями.
3. Журнал ресурсов.
4. Журнал печати.
5. Журнал управления политиками.
6. Журнал процессов.
7. Журнал резервного копирования.
8. Журнал пакетов МЭ.
9. Журнал соединений МЭ.
10. Системный журнал.
11. Журнал трафика.
12. Журнал контроля приложений.
13. Журнал средства обнаружения и реагирования.

Для просмотра содержимого определенного журнала необходимо в оболочке администратора на вкладке основного меню **Журналы** выбрать категорию, соответствующую одному из 13 типов журналов (рис. 152).

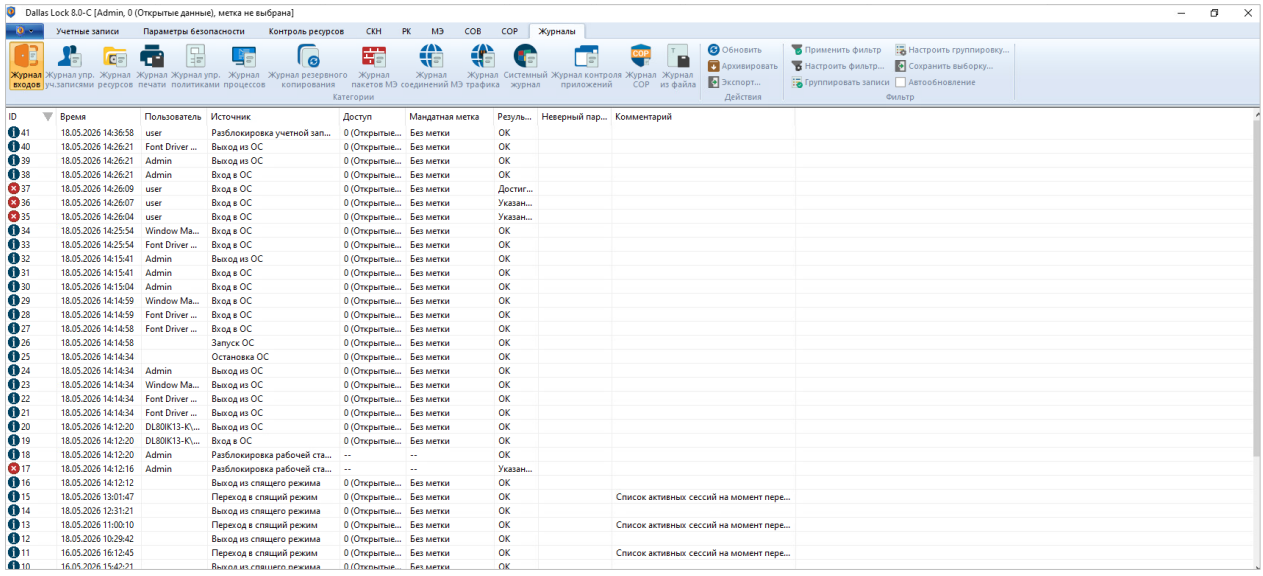


Рис. 152. Вкладка Журналы

В каждом журнале фиксируются дата, время, имя пользователя, операция, результат и прочие параметры. Возможно упорядочивание элементов списков журнала по необходимому значению, для этого нужно кликнуть на кнопку с названием столбца журнала.

Двойной щелчок мыши на любой записи любого журнала открывает окно, содержащее всю информацию, относящуюся к этой записи (рис. 153).

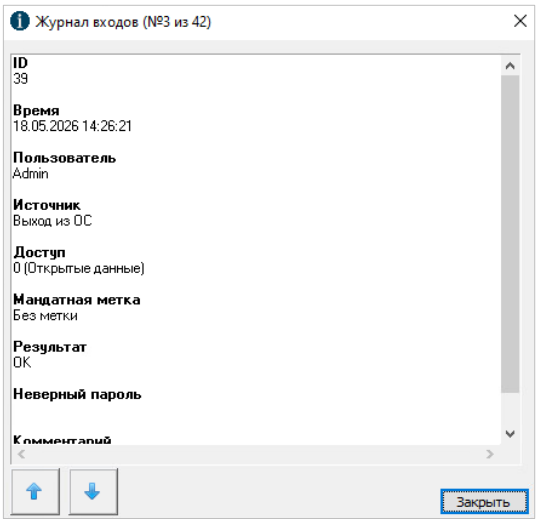


Рис. 153. Отдельная форма записи журнала событий

Нажимая на кнопки **вверх** и **вниз**, можно листать журнал, просматривая предыдущие или следующие записи.

Панель кнопок **Действия**, общая для всех журналов, позволяет произвести над открытым журналом действия по обновлению журнала (кнопка **Обновить**), по архивации всего журнала (кнопка **Архивировать**), по экспорту всего журнала или отфильтрованных записей в файл (кнопка **Экспорт**), по автоматическому обновлению журнала раз в 5 секунд (кнопка **Автообновление**). Также эти действия возможно выбрать из контекстного меню.

С помощью клавиши **Delete** можно очистить любой журнал. Для этого выполнить следующее:

1. Выделить выбранный журнал и нажать клавишу **Delete**.
2. Перед очисткой журнала пользователю задается вопрос о необходимости архивирования записей (Рис. 154).

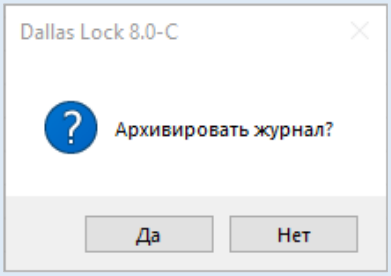


Рис. 154. Сообщение о архивировании журнала

3. При положительном ответе происходит архивирование и очистка журнала, при отрицательном обе операции будут отменены.

После выбора архивации журнала его записи сохраняются в файл в системной папке «C:\DLLOCK80\Logs», в окне журнала записи очищаются, и он начинает вестись заново. В том случае, когда журнал переполняется (максимальный размер — 20000 записей), он архивируется в файл со специальным расширением *.lg8 и помещается в папку «C:\DLLOCK80\Logs». При этом текущий журнал в оболочке администратора очищается и начинает вестись заново. В имени архивного файла с журналом записаны его тип, дата и время создания файла.

Каждый текущий журнал формируется в папке «C:\DLLOCK80\Jrn» и имеет фиксированный максимальный размер — 20000 записей.

Если необходимо удалить журнал окончательно, нужно зайти в папку «C:\DLLOCK80\Logs» и удалить соответствующий файл.

Категория **Журнал из файла** на вкладке *Журналы* позволяет открыть журнал из сохраненного файла, отфильтровать его значения и экспортировать в файл. Это могут быть журналы от **Dallas Lock 8.0** предыдущих версий.

Журналы в **Dallas Lock 8.0** имеют следующую структуру:

Журнал входов

В данном журнале фиксируются все входы (или попытки входов с указанием причины отказа) и выходы пользователей ПК, включая как локальные, так и сетевые, в том числе, терминальные входы и события разблокировки, а также события входа при активном модуле загрузчика DL (Включение ПК, вход с PIN-кодом, начало загрузки ОС). Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Пользователь*» фиксируется имя пользователя;
- в графе «*Источник*» фиксируется тип события: загрузка ПК, вход в ОС, выход из ОС;
- в графе «*Доступ*» указывается мандатный уровень, под которым осуществлен вход (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Мандатная метка*» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Результат*» фиксируется успех или отказ в доступе и причина отказа;
- в графе «*Неверный пароль*» фиксируются неверно введенные пароли при попытке загрузки ПК или входе в ОС;
- в графе «*Комментарий*» отображается дополнительная информация.



При сетевом входе в графе «*источник*» к типу события добавляется имя компьютера, с которого произведен вход, и его IP-адрес.

Журнал управления учетными записями

В данном журнале ведется учет всех действий по созданию, удалению или изменению прав пользователей и события смены пароля учетной записи. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время действий, производимых над правами пользователей;
- в графе «*Пользователь*» фиксируется имя пользователя, осуществившего вышеперечисленные операции администрирования;
- в графе «*Компьютер*» фиксируется имя компьютера, с которого производилось администрирование;
- в графе «*Имя*» фиксируется имя пользователя, изменение прав которого было произведено;
- в графе «*Результат*» отображается результат выполнения операции («*ОК*» — операция выполнена удачно или «*доступ запрещен*»);
- в графе «*Комментарий*» отображается дополнительная информация;
- в графе «*Операция*» отображается наименование произведенной операции (создать пользователя, удалить пользователя, сменить пароль, изменить параметры и др.).

Журнал ресурсов

Данный журнал позволяет проследить обращения к объектам ФС, реестру и устройствам, для которых назначен аудит, а также события по настройке дескрипторов объектов ФС и устройств. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Пользователь*» фиксируется имя пользователя, осуществившего действие;
- в графе «*Компьютер*» фиксируется имя компьютера, с которого осуществлялся доступ;
- в графе «*Объект доступа*» фиксируется путь к ресурсу или имя устройства;
- в графе «*Результат*» фиксируется успех или отказ в доступе и причина отказа;
- в графе «*Операция*» фиксируются все действия, которые производились с объектом;
- в графе «*Доступ*» указывается мандатный уровень, под которым осуществлен доступ к ресурсу (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Мандатная метка*» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Права*» фиксируются права, с которыми был осуществлен доступ к ресурсу ФС и ветке реестра:

Для папок и веток реестра	Для файлов и ключей параметров реестра
MAX — открытие на полный доступ	MAX — открытие на полный доступ

D	—	удаление папки	R	—	открытие на чтение
L	—	получить содержимое папки	W	—	открытие на запись
AF	—	добавление файла в папку	A	—	открытие на добавление данных в конец файла
AD	—	добавление подпапки	D	—	открытие с последующим удаление файла.
DF	—	удаление файла из папки	E	—	выполнение файла
RA	—	чтение атрибутов папки	RA	—	чтение атрибутов файла
WA	—	запись атрибутов папки	WA	—	запись атрибутов файла

- в графе «*Процесс*» фиксируется программа, из которой производилась операция по доступу;
- в графе «*Комментарий*» отображается дополнительная информация.

Журнал печати

В данный журнал заносятся все события, связанные с распечаткой документов на локальных или удаленных принтерах. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время начала печати;
- в графе «*Пользователь*» фиксируется имя пользователя, запустившего процесс печати;
- в графе «*Принтер*» фиксируется имя принтера, на котором производилась печать;
- в графе «*Порт*» фиксируется название порта, к которому подключено устройство;
- в графе «*Документ*» фиксируется название документа и программа, из которой производилась печать;
- в графе «*Результат*» фиксируется успех или отказ в печати;
- в графе «*Страниц*» фиксируется количество распечатанных страниц документа;
- в графе «*Копий*» отображается количество копий;
- в графе «*Процесс*» фиксируется процесс, который запущен программой печати;
- в графе «*Доступ*» фиксируется уровень мандатного доступа, под которым работает пользователь, производящий печать;
- в графе «*Мандатная метка*» — указывается назначенный уровень мандатного доступа для документа, отправленного на печать.

Записи в журнал печати заносятся при условии включенного аудита печати (вкладка «**Параметры безопасности**» → «**Политики аудита**»). Процесс печати сопровождается двумя записями: начала и окончания печати.

Журнал управления политиками

Данный журнал дает возможность просмотреть все действия, изменяющие настройку параметров системы защиты и прав пользователей. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Пользователь*» фиксируется имя пользователя, производящего изменения;
- в графе «*Компьютер*» фиксируется имя компьютера;
- в графе «*Параметр*» фиксируется название процесса по настройке параметров;
- в графе «*Комментарий*» отображается дополнительная информация;
- в графе «*Результат*» фиксируется результат редактирования.

Журнал процессов

В данный журнал заносятся события запуска и завершения процессов. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Процесс*» фиксируется путь к файлу процесса и его имя;
- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*PID родителя*» фиксируется номер идентификации процесса, от которого был создан текущий процесс;
- в графе «*Операция*» фиксируется тип события — запуск или завершение;
- в графе «*Доступ*» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Мандатная метка*» указывается информация о метке (только для Dallas Lock 8.0 редакции «С»);

- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен!*») результат;
- в графе «*Отправлено*» фиксируется количество отправленных байт;
- в графе «*Получено*» фиксируется количество принятых байт.

Журнал резервного копирования

В данный журнал заносятся события, связанные с резервным копированием. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Операция*» отображается наименование произведенной операции;
- в графе «*Имя*» отображается наименование задания;
- в графе «*Пользователь*» указывается пользователь, который принудительно запустил задание. Если задание запущено по расписанию — в поле указывается «Служба РК»;
- в графе «*Результат*» фиксируется успешность операции;
- в графе «*Комментарий*» отображается дополнительная информация.

Журнал пакетов МЭ

В данный журнал заносятся события, связанные с передачей пакетов данных в соответствии с заданными правилами в обоих направлениях через сетевые адаптеры компьютера. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Локальный адрес*» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Локальный порт*» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Внешний адрес*» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Внешнее имя*» фиксируется NETBIOS- или DNS-имя внешнего респондента при наличии такой информации в отправленных или принятых данных (принудительный запрос этой информации не производится);
- в графе «*Внешний порт*» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Направление*» фиксируется направление передачи данных (прием или отправка);
- в графе «*Протокол*» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Доступ*» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Процесс*» фиксируется путь к файлу процесса и его имя;
- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*Длина*» фиксируется отправленного или принятого пакета данных;
- в графе «*Правило*» фиксируется правило, которое было применено;
- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен!*») результат.

Журнал соединений МЭ

В данный журнал заносятся сведения об истории сетевых соединений, устанавливаемых процессами (приложениями) в соответствии с заданными правилами. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Локальный адрес*» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Локальный порт*» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Внешний адрес*» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Внешнее имя*» фиксируется NETBIOS- или DNS-имя внешнего респондента при наличии такой информации в отправленных или принятых данных (принудительный запрос этой информации не производится);

- в графе «*Внешний порт*» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*IP версия*» фиксируется версия используемого протокола IP;
- в графе «*Протокол*» фиксируется протокол отправленного или принятого пакета данных;
- в графе «*Информация*» фиксируется вся техническая информация, найденная и проанализированная в отправленном или принятом пакете данных;
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Доступ*» указывается мандатный уровень, под которым осуществлен доступ (только для Dallas Lock 8.0 редакции «С»);
- в графе «*Процесс*» фиксируется путь к файлу процесса и его имя;
- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*Событие*» фиксируется наименование события соединения;
- в графе «*Отправлено*» фиксируется количество отправленных байт;
- в графе «*Получено*» фиксируется количество принятых байт;
- в графе «*Правило*» фиксируется правило, которое было применено;
- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен!*») результат.

Журнал трафика

В данном журнале фиксируется проходящий сетевой трафик через контролируемые узлы сети. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен!*») результат;
- в графе «*Тип атаки*» фиксируется тип атаки события;
- в графе «*Адрес источника*» фиксируется логический или физический адрес внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Порт источника*» фиксируется логический порт внешнего сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Внешнее имя*» фиксируется имя компьютера, от которого запущена атака;
- в графе «*Адрес назначения*» фиксируется логический или физический адрес локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Порт назначения*» фиксируется логический порт локального сетевого интерфейса устройства, на котором происходил обмен информацией;
- в графе «*Протокол*» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Процесс*» фиксируется путь к файлу процесса и его имя;
- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*Комментарий*» отображается дополнительная информация;
- в графе «*Сообщение*» фиксируется описание атаки;
- в графе «*ID сигнатуры*» фиксируется уникальный идентификатор сигнатуры.

Системный журнал

В данном журнале фиксируются важные события безопасности, генерируемые ОС. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Уровень тревоги*» фиксируется уровень важности события;
- в графе «*Тип события*» фиксируется тип события;
- в графе «*Источник события*» фиксируется процесс, зарегистрировавший событие в журнале;
- в графе «*Код события*» фиксируется число, определяющее конкретный тип события;
- в графе «*Протокол*» фиксируется протокол отправленного или принятого пакета данных (самого верхнего уровня по модели OSI);
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Категория*» фиксируется категория события;
- в графе «*Процесс*» фиксируется программа, из которой производилась операция;

- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*ID сигнатуры*» фиксируется уникальный идентификатор сигнатуры;
- в графе «*Сигнатура*» фиксируется информация о сигнатуре;
- в графе «*Текст события*» фиксируется описание события;
- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен*!») результат.

Журнал контроля приложений

В данном журнале фиксируются события об активности приложений, их целостности и набора загружаемых ими компонентов. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Тип атаки*» фиксируется описание атаки;
- в графе «*Подробнее*» фиксируется сообщение, присвоенное правилу.
- в графе «*Процесс*» фиксируется путь к файлу процесса и его имя;
- в графе «*PID*» фиксируется уникальный идентификатор процесса;
- в графе «*PID родителя*» фиксируется номер идентификации процесса, от которого был создан текущий процесс;
- в графе «*Пользователь*» фиксируется пользователь, от имени которого был запущен процесс;
- в графе «*Правило*» фиксируется правило, которое было применено;
- в графе «*Результат*» фиксируется успешный (*OK*) или неуспешный («*Доступ запрещен!*») результат;
- в графе «*Комментарий*» фиксируется дополнительная информация.

Журнал СОР

В данном журнале фиксируются события работы средства обнаружения и реагирования. Журнал содержит следующие элементы списков:

- в графе «*Время*» фиксируется дата и время события;
- в графе «*Тип события*» фиксируется тип события;
- в графе «*Подробнее*» фиксируется сообщение, присвоенное событию.
- в графе «*Пользователь*» фиксируется пользователь;
- в графе «*Результат*» фиксируется успешный или неуспешный результат.

6.3.1 Фильтры журналов

Панель кнопок **Фильтр**, общая для всех журналов, используется для задания параметров отбора событий, отображаемых в текущем или экспортированном журнале.

Использование фильтров дает возможность отсеять ненужные данные в журнале так, что они становятся невидимы при просмотре. В то же время информация при использовании фильтров из журналов не удаляется.

Чтобы произвести настройки, необходимо нажать кнопку **Настроить фильтр** и выбрать необходимые параметры фильтра в открывшемся окне, нажать **OK** (рис. 155). После настройки необходимо нажать кнопку **Применить фильтр**, после чего записи журнала будут отсортированы. Повторное нажатие **Применить фильтр** вернет полное содержание журнала.

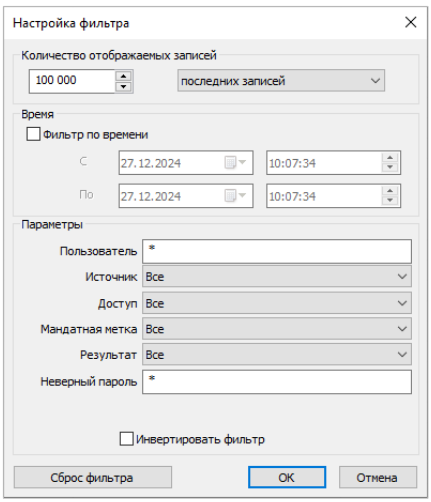


Рис. 155. Окно настройки фильтра журнала входов

Фильтр можно настроить по параметрам и (или) по времени. Для включения временного периода в фильтр необходимо отметить флагом поле *Фильтр по времени*.

Каждый фильтр имеет параметры настройки, которые соответствуют основным элементам списков выбранного журнала. Например, журнал входов можно отфильтровать по времени, в которое была осуществлена попытка входа на ПК, по логину пользователя, по результату процесса (удачный/не удачный), по источнику процесса (удаленный вход, терминальный вход, смена пароля и т. д.).

Отфильтрованные записи журнала можно сохранить, воспользовавшись кнопкой **Экспорт**, в выбранную папку в выбранном типе файла (TXT, CSV, HTML, XML). Экспортированные журналы служат для того, чтобы администратор мог рассмотреть записи в более удобном виде.

6.3.2 Группировка записей журнала

Для удобства просмотра записей в системе реализована группировка записей.

При включении действия **Группировать записи** полностью совпадающие записи (за исключением времени) группируются в одну запись. Если время самой ранней из них отличается от времени самой поздней, в колонке «*Время*» параметров журнала указывается диапазон. В этой же колонке в скобках указывается количество сгруппированных записей.

В отдельном окне характеристик такой записи в названии окна указывается, сколько записей объединено, перечисляются моменты времени с пометкой, какие записи выведены в журнал и другие общие параметры.

6.4 Теневое копирование

Функция теневого копирования обеспечивает копирование информации, которую пользователь записывает на съемные или сетевые накопители, в специальную папку на локальном жестком диске для последующего анализа.

Просмотр копий, созданных при теневом копировании, доступен для пользователей, наделенных данными полномочиями: **Аудит: Просмотр журналов** и **Аудит: Просмотр теневых копий файлов** на вкладке **Параметры безопасности → Права пользователей**.

Режим теневого копирования информации доступен для следующего типа съемных и сетевых накопителей:

- магнитные гибкие диски (FDD);
- оптические диски (CD, DVD);
- USB-Flash накопители и съемные дисковые накопители;
- сетевые диски и накопители;
- карты памяти (SD, MicroSD, MMC).

Чтобы задать теневое копирование, необходимо в дескрипторе объекта (класса объектов) перейти на закладку *Аудит доступа*, отметить флагом Включение аудита и поле *Теневое копирование* (рис. 156).

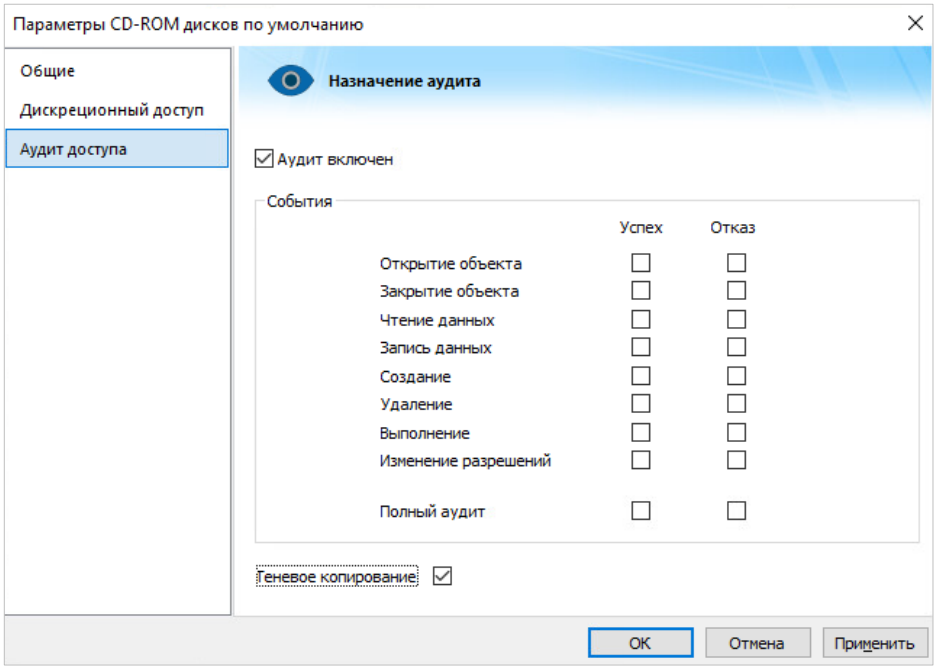


Рис. 156. Установка теневого копирования для устройств

Теневое копирование можно задать для классов накопителей и для конкретных экземпляров подключаемых накопителей:

- задать теневое копирование глобально и для определенного класса можно через оболочку администратора, выбрав необходимый параметр на вкладке **Контроль ресурсов** → **Глобальные**;
- задать теневое копирование для отдельно взятого накопителя можно, выбрав его в проводнике Windows, и с помощью пункта контекстного меню **Права доступа 8.0** открыть закладку аудита доступа или через оболочку администратора, добавив объект в список на вкладке **Контроль ресурсов** → **Аудит**.

В момент копирования информации на накопитель с включенным режимом теневого копирования копии файлов помещаются в специальную защищенную папку.

Просмотр теневых копий доступен через запись о теневом копировании в журнале ресурсов: в блоке **Действия** размещена кнопка **Теневая копия**, при нажатии открывающая файл в режиме редактирования (рис. 157).

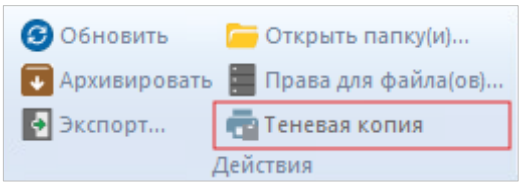


Рис. 157. Возможность просмотра теневой копии

Если теневое копирование было выполнено под определенным мандатным уровнем доступа, то просмотреть созданную теневую копию возможно только под таким же уровнем доступа или выше. Так же должны совпадать неиерархические мандатные метки.

7 ПОДСИСТЕМА ПЕЧАТИ

7.1 Разграничение доступа к печати

Для того, чтобы выполнить настройку разрешения или запрета печати с ПК, защищенного **Dallas Lock 8.0**, необходимо в оболочке администратора открыть вкладку **Параметры безопасности → Права пользователей**.

С помощью параметров **Печать разрешена** и **Печать запрещена** можно гибко настроить список учетных записей, которым разрешена или запрещена печать с данного компьютера. Добавить разрешенные или запрещенные учетные записи в список значений можно, выбрав параметр и нажав кнопку **Свойства** (рис. 158).

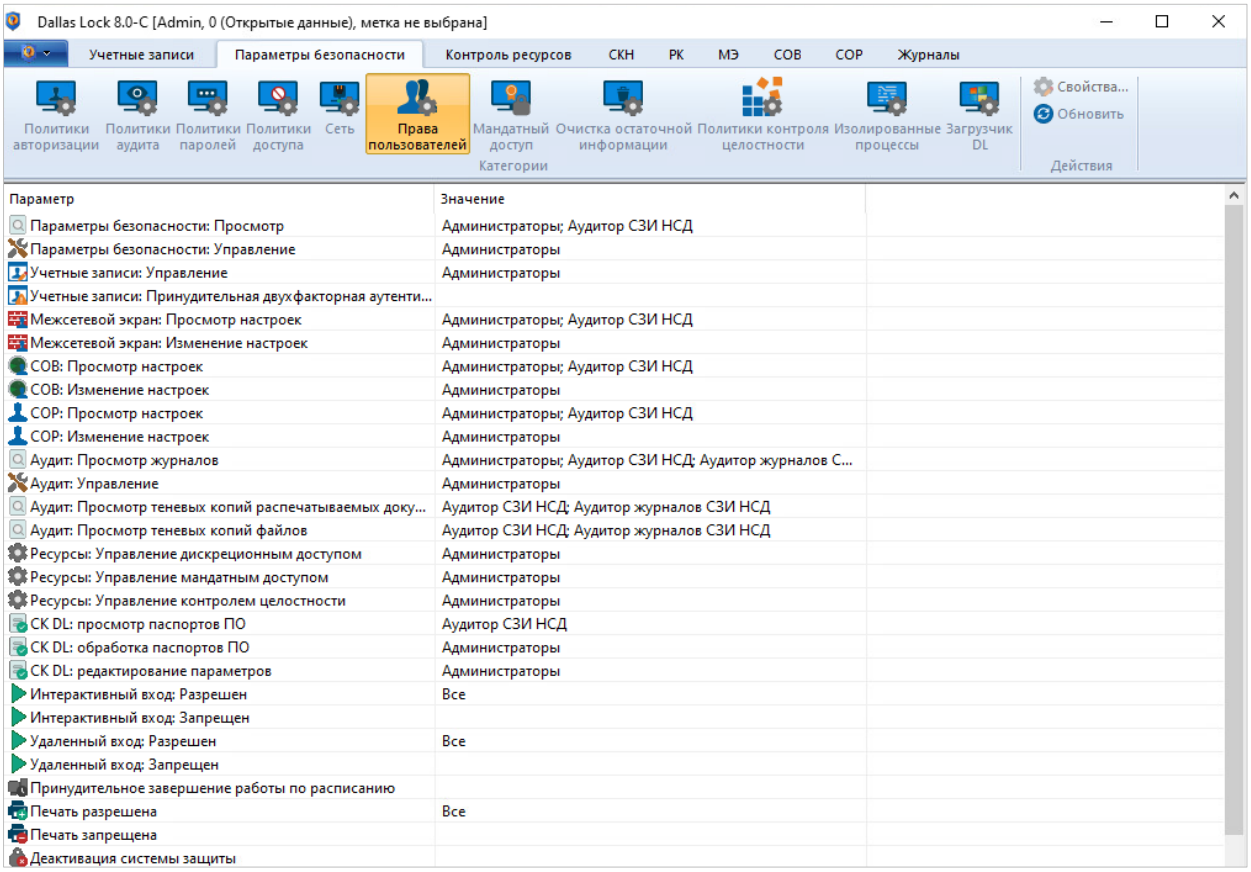


Рис. 158. Права пользователей на доступ к печати

При настройке следует учесть, что установленный параметр запрета имеет более высокий приоритет перед установленным параметром разрешения.

Правило разрешения и запрета следующее:

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

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

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

Пример

Требуется запретить печать определенным доменным пользователям определенного домена, а разрешить всем остальным пользователям только данного домена.

По умолчанию печать разрешена всем пользователям: параметр **Печать разрешена** имеет значение *Все*, параметр **Печать запрещена** имеет пустое значение. Чтобы запретить печать определенным доменным пользователям определенного домена, необходимо для параметра **Печать разрешена** установить значение «имя_домена*» (учетная запись по маске), а для параметра «Печать запрещена» установить значение «имя_домена\имя_пользователя» (индивидуальная учетная запись выбранного пользователя).

В итоге всем пользователям печать будет запрещена (так как группы «*Все*» уже не будет ни в одном из двух списков), пользователям выбранного домена печать будет разрешена, и индивидуальным выбранным пользователям данного домена печать будет запрещена.

7.1.1 Мандатное разграничение доступа к печати

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

В **Dallas Lock 8.0** редакции «С» имеется возможность выполнить настройку разграничения печати документов с защищенного ПК для пользователей, работающих под различными уровнями доступа, путем разрешения печати из-под определенных уровней.

Чтобы выбрать уровни доступа, необходимо в оболочке администратора открыть вкладку **Параметры безопасности** → **Мандатный доступ** и выбрать параметр **Печать из-под уровней доступа**. Появится окно, в котором необходимо отметить уровни, при работе под которыми для пользователей будет открыт доступ для печати документов с данного ПК (рис. 159).

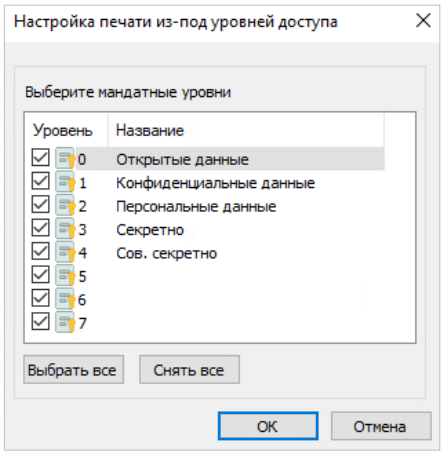


Рис. 159. Выбор мандатных уровней для доступа к печати

Пользователям, которые осуществили авторизацию под уровнем, не отмеченным к доступу печати, при попытке отправить файл на печать будет выдаваться отказ в доступе, процесс печати будет прекращен.

7.1.2 Разграничение доступа к принтерам

Средствами контроля доступа к устройствам в **СЗИ** можно настроить разграничение доступа определенных пользователей к определенным печатающим устройствам, глава 10 Контроль устройств.

В дереве устройств (**Контроль ресурсов** → **Устройства**) имеется возможность для выбранного значка печатающего устройства открыть дескриптор с параметрами безопасности, в котором возможны настройки доступа:

- Дискреционным принципом. Имеется два права доступа для выбранной учетной записи или группы по отношению к устройству: «*Разрешить*» и «*Запретить*».
- Мандатным принципом (только для Dallas Lock 8.0 редакции «С»). Имеется возможность установить уровень доступа и мандатную метку для доступа к устройству только пользователей с таким же уровнем.

Также возможна установка ведения аудита события доступа к выбранному устройству.

7.2 Аудит печати

Помимо разграничения доступа к печати документов в **СЗИ** имеется возможность вести аудит событий печати, настроить теневое копирование распечатываемых документов и добавление штампов на распечатываемые документы.

7.2.1 Журнал печати

Для того, чтобы протоколировать события печати с защищенного ПК на локальных и сетевых печатающих устройствах (принтерах, МФУ, плоттерах и пр.), необходимо включить журнал печати (вкладка **Параметры безопасности** → **Политики аудита**→ **Журнал печати** → значение «*Вкл.*»).

Если включен журнал печати, то подсистемам **СЗИ** необходимо контролировать права на выполнение печати для любого процесса, выполняющего печать. Для корректного расчета прав пользователя, запустившего процесс, определяется актуальный список групп, в которые данный пользователь входит. Соответственно, если пользователь доменный (AD) и нет связи с соответствующим контроллером домена (т. е. расчет актуального набора прав технически невозможен), то возможность печати для таких пользователей будет заблокирована **СЗИ**.

Печать пробной страницы является служебной информацией и не подлежит контролю и регистрации.

Если дополнительно включен параметр **Создавать теневые копии распечатываемых документов** (см. ниже), то в журнале печати для записи процесса распечатки документа доступна функция просмотра копии документа, созданной в системной папке (рис. 160).

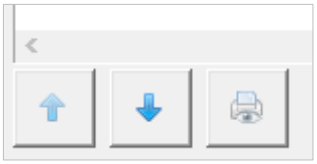


Рис. 160. Просмотр копии распечатываемого документа

Для корректной работы функции аудита печати необходимо сперва закрыть все открытые файлы, потом включить журнал печати. В противном случае для открытых ранее файлов события печати регистрироваться не будут.

7.2.2 Теневые копии распечатываемых документов

Для того, чтобы включить создание теневых копий, необходимо открыть вкладку **Параметры безопасности** → **Политики аудита**, выбрать параметр **Создавать теневые копии распечатываемых документов** и установить значение «*Да*».

Включение данного параметра позволяет сохранять копии распечатываемых документов в отдельной папке по пути: «C:\DLLOCK80\Logs\PrintCopy». В данной папке при каждой печати будут создаваться подпапки с файлами, названия которых состоят из времени печати и имени печатающего устройства. Просмотреть созданную таким образом копию документа можно, кликнув мышкой соответствующую запись в журнале печати, и в окне свойств записи нажав кнопку просмотра.

При просмотре теневой копии некоторые программы просмотра в процессе своей работы создают временные файлы в папках, не отмеченных, как разделяемые. Это может привести к соответствующим ограничениям при просмотре теневых копий в конфиденциальных сеансах доступа, так как нельзя создавать временные файлы в директориях с другой мандатной меткой или более низким уровнем доступа.

Для решения данной проблемы можно воспользоваться следующими вариантами:

1. Произвести настойку **СЗИ** таким образом, чтобы создание временных файлов выполнялось в разделяемых папках, подраздел 5.3.6 Механизм разделяемых папок.
2. Использовать программы просмотра, не создающие временные файлы, например, Paint.

С помощью параметра **Аудит: Просмотр теневых копий распечатываемых документов** на вкладке *Права пользователей* устанавливается доступ к данной папке, и, соответственно к возможности просмотра теневых копий.

При включенном параметре **Создавать теневые копии распечатываемых документов** вывод на печать файлов формата PDF будет осуществляться в виде пустых файлов. Это является особенностью защиты от копирования самого формата и не является ошибкой.

При включенном параметре **Создавать теневые копии распечатываемых документов** вывод на печать документов может происходить с задержкой, так как на печать отправляется именно созданная теневая копия (размер 1-страничного файла составляет ≈ 180 Мбайт).

При включенном параметре **Создавать теневые копии распечатываемых документов** печать с устройств, чьи драйвера не поддерживают возможность теневого копирования, заблокирована.

7.2.3 Добавление штампа на распечатываемые документы

Система защиты **Dallas Lock 8.0** позволяет на всех распечатываемых документах добавлять штамп независимо от программы, из которой производим печать.

Следует учесть, что при условии включенного аудита печати (вкладка **Параметры безопасности → Политики аудита)** в случае использования приложений Microsoft Edge, Internet Explorer 11, Microsoft.Photos при попытке печати штампа выполняется запрет печати, и выводится соответствующее предупреждение.

Для **Dallas Lock 8.0** редакции «С» имеется возможность разграничения нанесения штампа на распечатываемые документы при печати под определенными уровнями доступа. Для того, чтобы выбрать уровни доступа, необходимо в оболочке администратора открыть вкладку **Параметры безопасности → Мандатный доступ** и выбрать параметр **Добавлять штамп при печати под уровнями**. Появится окно, в котором необходимо отметить уровни.

Для настройки печати штампа на документах необходимо на вкладке основного меню *Параметры безопасности* открыть категорию **Политики аудита** и в списке параметров выбрать пункт **Печатать/редактировать штамп** (рис. 161).

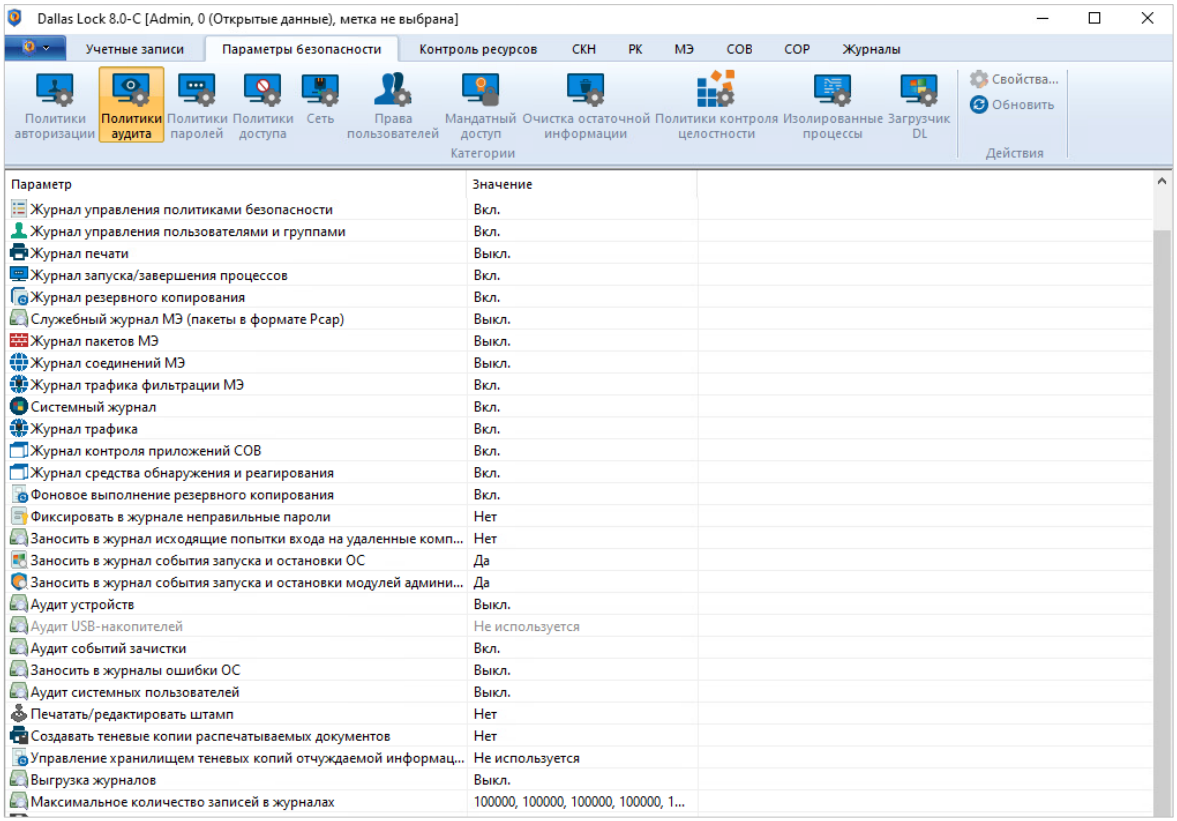


Рис. 161. Параметр печати/редактирования штампа

Откроется диалоговое окно включения и редактирования штампа на распечатываемые документы (рис. 162).

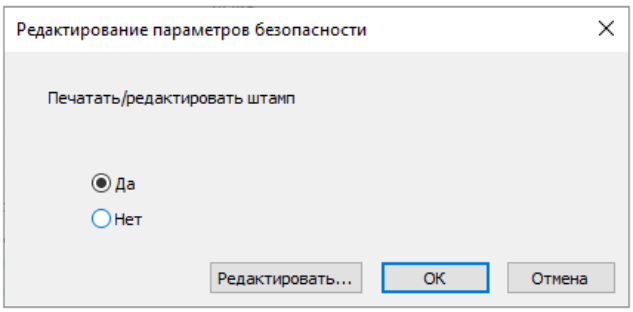


Рис. 162. Диалоговое окно включения и редактирования штампа

Для того, чтобы включить печать штампа, необходимо в диалоговом окне нажать кнопку **ОК**.

Для того, чтобы отредактировать штамп, необходимо нажать в диалоговом окне кнопку **Редактировать**.

Откроется окно **Редактор штампа** (рис. 163).

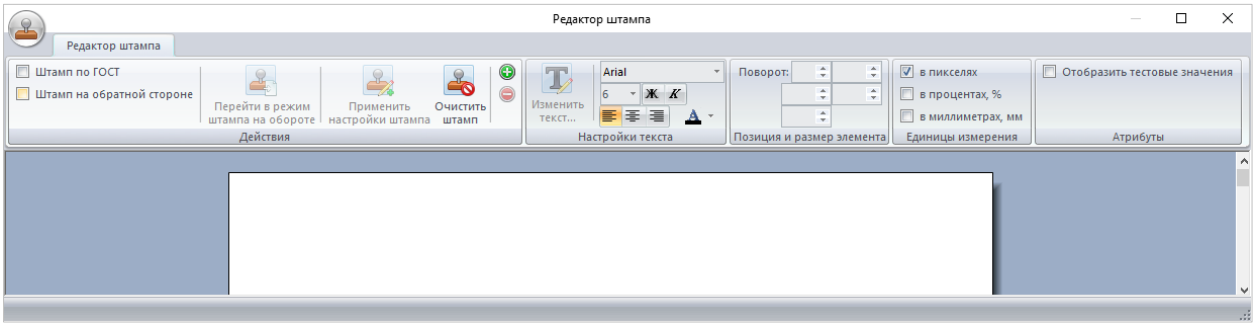


Рис. 163. Редактор штампа

Штампы в **Dallas Lock 8.0** могут быть двух типов:

- **Штамп по ГОСТ** — не редактируемый предопределенный вид штампа;
- **Штамп на обратной стороне** — пользователь может произвольно редактировать внешний вид штампа и его местоположение на листе.

При выборе печати штампа по ГОСТ на печатные документы будет наноситься штамп в соответствии с правилами учета секретных документов, при этом дополнительная настройка штампа невозможна: вид штампа предопределен.

При включенной печати штампа по ГОСТ выбрать число распечатываемых копий средствами ОС становится невозможным, но это меняется при появлении на экране формы параметров печати **Dallas Lock 8.0** распечатываемого документа.

В данном окне пользователю необходимо ввести:

- учетный номер документа (обязательное поле);
- код носителя (обязательное поле);
- общее количество экземпляров (по умолчанию — 1);
- номер текущего экземпляра (при выборе количества экземпляров более 1 определяется или автоматически и последовательно, или вручную);
- в поле *Использование* можно ввести комментарии для каждого распечатываемого экземпляра.

Штамп по ГОСТ на распечатанном документе имеет следующий формат: на первом листе документа в верхнем правом уголке добавляется уровень доступа и (или) мандатная метка и номер экземпляра, в нижнем левом уголке добавляется учетный номер. На последующих листках документа в нижнем левом уголке добавляется учетный номер.

В процессе распечатки документа на экране появляется сообщение: После того, как все страницы документа будут распечатаны, вставьте последнюю страницу в лоток подачи бумаги обратной стороной и нажмите кнопку **ОК**. Пользователю необходимо выполнить указанное действие.

В результате на обратной стороне последней страницы документа появится метка, содержащая учетный номер документа, код носителя, количество экземпляров, использование экземпляров, время распечатки и имя пользователя, который произвел распечатку. При этом имя пользователя берется из имени учетной записи пользователя.

Следует учесть, что при выборе типа печати штампа «по ГОСТ», печать каждого экземпляра осуществляется только после вызова функции печати данного файла. То есть за одно обращение к принтеру можно напечатать только одну копию документа. Если требуется N копий, то необходимо отправить документ на печать N раз.

При выборе печати штампа на обратной стороне становятся доступными для выбора другие поля окна настройки. Становится возможным отредактировать внешний вид и содержимое штампа (для редактирования доступны штампы на лицевой и обратной стороне документа). Доступны следующие настройки:

- **Настройки текста**. Здесь выбирается шрифт, размер, цвет шрифта и выравнивание текста в блоке штампа.
- **Позиция и размер элемента**. Здесь задается поворот штампа, ширина и высота штампа, а также координаты расположения штампа по осям X и Y.
- **Единицы измерения**. Указываются единицы измерения (%, пиксели, миллиметры).
- **Атрибуты** (отобразить текстовые значения). Вместо тегов в угловых скобках возможно задать текстовые значения.

В качестве имени пользователя для произвольного штампа можно использовать не имя учетной записи пользователя, а его описание, для чего выставить флаг в соответствующем поле.

Сам штамп представляет собой текст, который, после нажатия кнопки вводится в отведенном для набора поле (рис. 165).

В штамп можно вставить служебную информацию. Для этого необходимо дважды щелкнуть левой кнопкой мыши в поле ввода. В появившемся окне выбрать, какая именно информация должна быть напечатана (рис. 164).

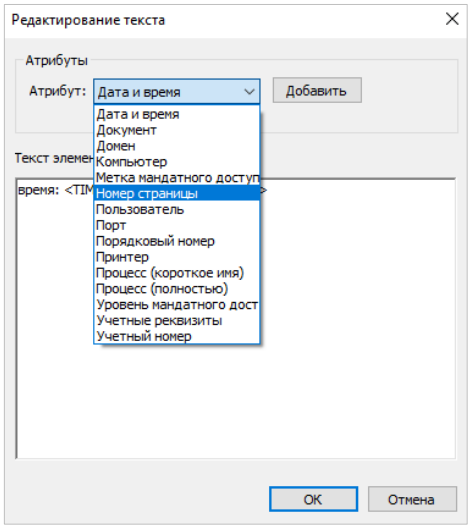


Рис. 164. Выбор данных для текста штампа из контекстного меню

В поле ввода в угловых скобках отображается выбранная для печати информация в виде тегов.

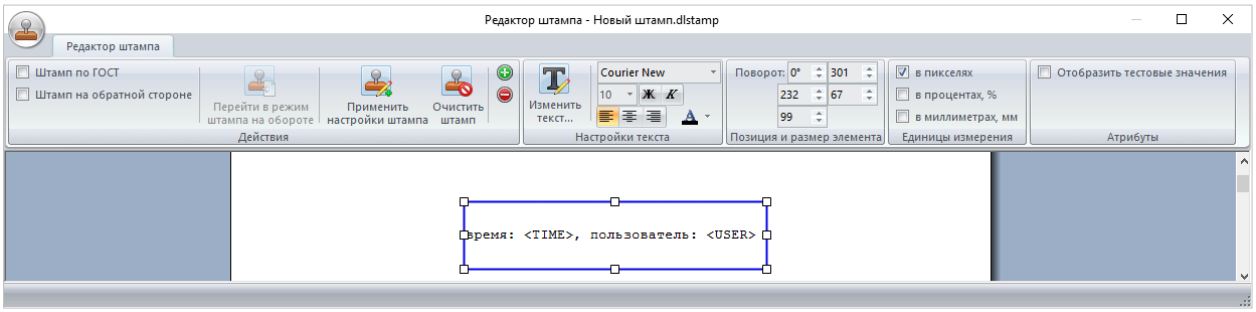


Рис. 165. Теги текста штампа в окне настройки

Если в штампе есть учетный номер документа (тег <REGISTRY NUMBER>), то перед распечаткой документа на экране появится окно, в котором пользователь должен ввести учетные реквизиты и нажать кнопку **ОК**. Вставка тега <SERIAL NUMBER> потребует ввести при печати порядковый номер документа в появившуюся форму.

При использовании произвольного типа штампа, на всех распечатываемых страницах, независимо от номера, будет добавляться одинаковый штамп.



Данное маркирование документов — это некий аналог «механического» штампа. Поэтому он добавляет штампы независимо от содержимого документов. В некоторых случаях, штамп может добавляться прямо поверх текста документа.

Что понимать под уровнем доступа документа, выводимого на печать?

Уровень доступа документа — это свойство объекта ФС, в частности файла. Но соответствия между конкретным файлом и распечатываемым документом может и не быть.

Например, запускается MS Word, в нем набирается какой-то текст и отправляется на печать. Как называется файл, который распечатывается? Никак. Файла нет, так как текст существует только в оперативной памяти компьютера, и когда закроется приложение MS Word, исчезнет и текст.

Другой пример. В MS Word открыт файл «C:\document1.docx», имеющий уровень доступа 0, далее, с помощью буфера обмена, ему добавлен в конец текст из файла «C:\document2.docx» имеющий уровень доступа 1. Исходный документ отправлен на печать. Как называется файл, который распечатывается, какой уровень доступа он имеет? Аналогично первому случаю — файла с таким содержимым нет, уровня доступа, соответственно, тоже нет.

Таким образом, под уровнем доступа распечатываемого документа понимается **текущий уровень доступа пользователя,** который распечатывает данный документ. И по этой же причине в журнале печати нет поля *имя файла*.

Маркирование документов под мандатными метками производится аналогичным образом.

8 ОЧИСТКА ОСТАТОЧНОЙ ИНФОРМАЦИИ

Большинство ОС при удалении файла не удаляют содержимое файла непосредственно, а всего лишь удаляют запись о файле из директории ФС. Так сделано для ускорения работы системы.

Реальное содержимое файла остается на запоминающем устройстве, и его можно достаточно легко просмотреть до тех пор, пока ОС заново не использует это пространство для хранения новых данных. Данная остаточная информация может легко привести к непреднамеренному распространению конфиденциальной и секретной информации.

СЗИ включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных.

Данная подсистема позволяет выполнять следующее:

- Затирать всю остаточную информацию при освобождении областей на дисках, т.е. при удалении файлов или при перемещении файлов, или при уменьшении размеров файлов. Затирание производится записью, маскирующей последовательности поверх освобождаемого пространства.
- Затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).
- Принудительно зачищать конкретную папку/файл, выбрав соответствующий пункт в контекстном меню данного файла.
- Проверять корректное завершение процесса очистки информации.
- Предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого без перезагрузки, что гарантирует освобождение используемых областей оперативной памяти, с помощью параметра «Запрет смены пользователя без перезагрузки».

8.1 Регистрация действий по очистке остаточной информации

Для того, чтобы фиксировать события зачистки остаточной информации (успешные и неуспешные), необходимо включить (значение «*Вкл.*») отвечающий за это параметр аудита: **Параметры безопасности** → **Политики аудита** → параметр **Аудит событий зачистки**.

При включенном данном параметре события очистки остаточной информации (см. ниже), будут заноситься в журнал ресурсов, который также должен быть включен (**Параметры безопасности** → **Политики аудита** → параметр **Журнал ресурсов**, значение «*Вкл.*»).

8.2 Параметры очистки остаточной информации

Для настройки процесса очистки остаточной информации в соответствии с требованиями, необходимо в оболочке администратора во вкладке основного меню *Параметры безопасности* выбрать категорию **Очистка остаточной информации** (рис. 166).

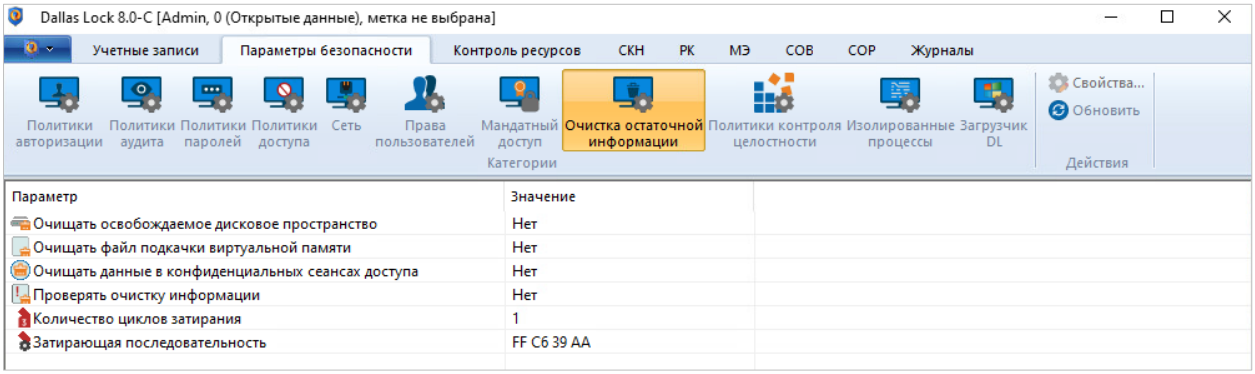


Рис. 166 Параметры очистки остаточной информации

Появится список параметров очистки остаточной информации. Изменить необходимый параметр можно, выделив его и нажав на панели действий кнопку **Свойства**.

8.2.1 Проверка очистки информации

Если параметр **Проверять очистку информации** включен, то после проведения очистки объектов ФС, дополнительно выполняется проверка того, что очистка действительно осуществлена. В том случае, если проверка выявила, что очистка не осуществлена или завершена с ошибкой, то в журнал ресурсов заносится соответствующее событие.

Проверка осуществляется при очистке остаточной информации, выполняемой по команде администратора, в автоматическом режиме, и при зачистке накопителя целиком (функция «Зачистка диска»).

8.2.2 Очистка освобождаемого дискового пространства

Включение параметра **Очищать освобождаемое дисковое пространство** (значение «*вкл.*») позволяет автоматически затирать всю остаточную информацию при освобождении областей на дисках, то есть при удалении файлов или при уменьшении размеров файлов. Затирание производится записью маскирующей последовательности поверх освобождаемого пространства заданным количеством циклов затирания (см. ниже). Включение данного параметра может заметно снизить скорость выполнения файловых операций, особенно при количестве циклов затирания больше единицы.

8.2.3 Очистка файла подкачки виртуальной памяти

Включение параметра **Очищать файл подкачки виртуальной памяти** (значение «*вкл.*») позволяет автоматически затирать всю остаточную информацию в файле подкачки Windows. Затирание производится записью маскирующей последовательности поверх файла подкачки. Очистка производится при завершении работы (закрытии файла подкачки) и, если очистка была прервана, при старте системы (открытии файла подкачки).

8.2.4 Очистка данных в конфиденциальных сеансах доступа

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

Включение параметра **Очищать данные в конфиденциальных сеансах доступа** (значение «*вкл.*») позволяет осуществлять автоматическую зачистку освобождаемого дискового пространства при удалении/перемещении/уменьшении размера объектов ФС при работе под мандатной меткой или уровнем доступа больше нуля. Данная политика функционирует при условии включенной политики **Очищать освобождаемое дисковое пространство**.

8.2.5 Количество циклов затирания, затирающая последовательность

Затирание производится записью маскирующей последовательности поверх освобождаемого пространства. Чем большее число циклов затирания выбрано, тем надежнее происходит удаление информации. При этом следует учесть, что чем больше циклов затирания будет выбрано, тем больше времени эта процедура будет занимать.

С помощью параметра **Количество циклов затирания** можно выбрать от одного до четырех циклов затирания.

Другим параметром **Затирающая последовательность** определяется метод затирания остаточной информации, путем установки числовых байтовых значений (от 0 до F) для каждого из четырех циклов затирания. Если эти значения не установлены или установлены не для каждого цикла, то по умолчанию для затирающей последовательности циклов используется последовательность, установленная в **Dallas Lock**.

Установленное количество циклов затирания и методы затирания используются при всех установленных видах очистки остаточной информации: по команде администратора, в автоматическом режиме, и при зачистке накопителя (функция Зачистка диска).

8.3 Удаление файлов и зачистка остаточной информации по команде

При необходимости удалить какие-либо данные без возможности их восстановления нужно воспользоваться контекстным меню данного объекта ФС и выбрать пункт **DL8.0: Удалить и зачистить** (рис. 167).

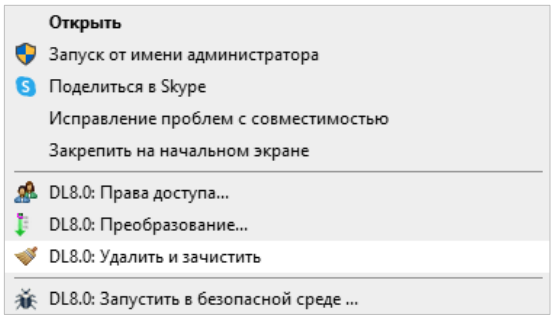


Рис. 167. Контекстное меню

Аналогичным образом реализуется удаление и зачистка файлов и папок, перемещенных в корзину (рис. 168).

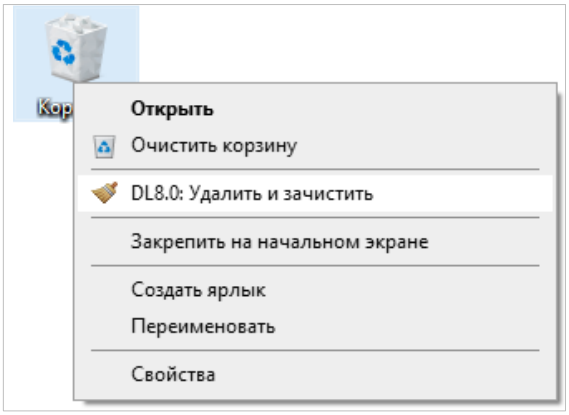


Рис. 168. Контекстное меню зачистки корзины

Появится окно с требованием подтвердить операцию (рис. 169).

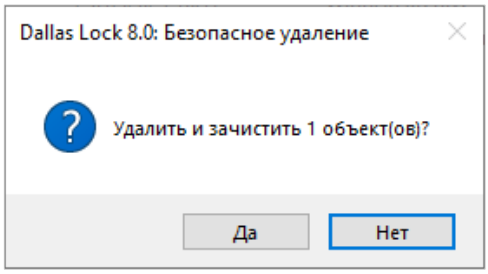


Рис. 169. Подтверждение удаления файла

Для того, чтобы выполнить зачистку логического диска, пользователь, от которого выполняется операция, должен иметь следующие права:

1. Низкоуровневая запись и чтение для данного диска.
2. Просмотр и редактирование политик.

При активации удаления происходит зачистка данного объекта путем перезаписи файла. Количество циклов затирания определяется соответствующей политикой, подраздел 8.2.5 Количество циклов затирания, затирающая последовательность. После перезаписи восстановить хоть сколько-нибудь значимый фрагмент файла становится практически невозможно. После успешного удаления объектов система выведет соответствующее подтверждение (рис. 170).

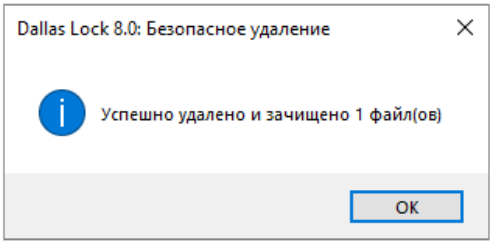


Рис. 170. Сообщение системы об успешном удалении

При нескольких одновременно выделенных объектах происходит их одновременное удаление и зачистку как группы. При этом появится окно подтверждения удаления с количеством зачищаемых объектов.

При автоматической зачистке файла, не содержащего информацию, запись в журнал не заносится.

8.4 Запрет смены пользователя без перезагрузки

В соответствии с требованиями политик безопасности организации возможно Включение запрета смены пользователя компьютером без его перезагрузки.

Чтобы установить данный запрет, необходимо включить параметр политик авторизации **Запретить смену пользователя без перезагрузки** (**Параметры безопасности → Политики авторизации**). Параметр может принимать значение «*Включен*» или «*Выключен*». Включение данной политики («*Вкл.*») не позволит осуществить смену пользователя без перезагрузки компьютера (рис. 171).

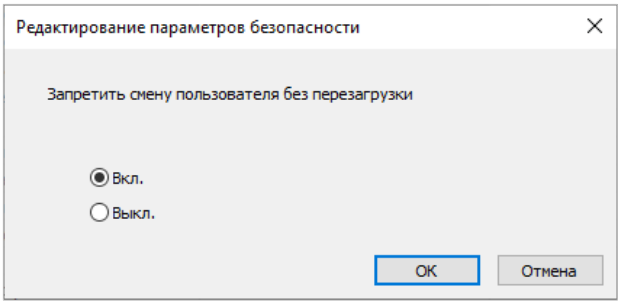


Рис. 171. Редактирование параметров безопасности

Если установлено значение «*Вкл*», то при выборе пункта *Завершение сеанса* в окне **Завершение работы Windows**, компьютер автоматически уйдет на перезагрузку (рис. 172).

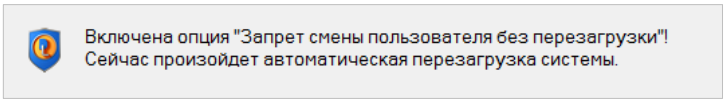


Рис. 172. Сообщение системы при автоматической перезагрузке

Данная политика позволяет предотвратить теоретическую возможность извлечения какой-либо информации из оперативной памяти ПК, оставшуюся там после завершения сеанса работы другого пользователя.

8.5 Зачистка диска

Система защиты **Dallas Lock 8.0** позволяет полностью зачищать остаточные данные всего диска или его разделов. Для этого служит функция **Зачистка диска**. Данная функция может применяться к разделам фиксированных и съемных жестких дисков и к USB-Flash накопителям. Системный раздел с установленной ОС для данной операции будет недоступен.

Функциональная возможность зачистки фиксированного диска требует наличия доступа к зачищаемому диску. В частности, если стороннее ПО (например, антивирусы или иные средства защиты информации) блокируют доступ к какому-либо файлу или папке на фиксированном диске, функция зачистки данного диска **Dallas Lock 8.0** может оказаться заблокированной.

Зачистка диска может быть полезна при снятии носителей с учета и необходимости полного удаления данных без возможности их восстановления по остаточной информации.

Полная зачистка диска выполняет в том числе зачистку boot-сектора. В связи с этим после проведения данной операции зачищенный диск подлежит форматированию.

Для вызова данной функции необходимо в оболочке администратора нажать кнопку основного меню и в списке дополнительных функций выбрать пункт **Зачистка диска** (рис. 173).

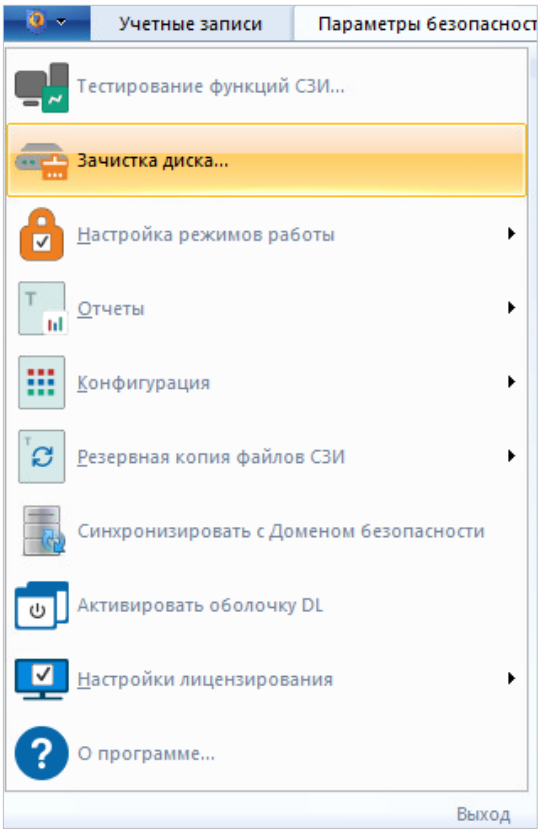


Рис. 173. Выбор функции «Зачистка диска»

Появится окно, в котором необходимо выбрать жесткие диск из списка обнаруженных в системе и нажать **Зачистить**.

Для того, чтобы выполнить зачистку логического диска, пользователь, от которого выполняется операция, должен иметь следующие права:

1. Низкоуровневая запись и чтение для данного диска.
2. Просмотр и редактирование политик.

Запустится процесс зачистки остаточных данных жесткого диска. Процесс будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса на экран будет выведено сообщение об успешном окончании операции.

9 ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ

Система защиты информации **Dallas Lock 8.0** включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность программно-аппаратной среды компьютера, целостность объектов ФС и реестра, а также восстанавливать файлы и ветки реестра в случае обнаружения нарушенной целостности.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Процедура контроля целостности осуществляется следующим образом: после назначения дескриптора целостности при следующей проверке проверяется, было ли уже вычислено эталонное значение контрольной суммы параметра. Если оно еще не было вычислено, оно вычисляется и сохраняется. Если же оно уже было вычислено, то оно сравнивается с вычисляемым текущим значением контрольной суммы контролируемого параметра. Если хотя бы для одного из проверяемых параметров текущее значение параметра не совпало с эталонным значением, результат проверки считается отрицательным, а целостность контролируемых объектов — нарушенной.

Для программно-аппаратного контроля целостности **СЗИ** использует подсистему WMI. Если стороннее ПО блокирует или встраивается в работу этой подсистемы, могут наблюдаться проблемы выполнения расчета программно-аппаратной целостности и, соответственно, проблемы авторизации пользователей. В частности, если требуется контролировать программно-аппаратную целостность системы, следует избегать установки Microsoft SQL сервера в конфигурации, при которой он будет запускаться от имени пользователя. Данный вариант приводит к взаимоблокировке подсистемы WMI и SQL-сервера. Это, в свою очередь, может сопутствовать проблемам авторизации пользователей в ОС.

В ряде подобных случаев для разрешения сценариев блокировки сессий на этапе авторизации может помочь использование функциональной возможности сессий-исключений. Достаточно понимать, что для сессий-исключений обращение к подсистеме WMI в рамках встроенных механизмов **СЗИ** не производится.

У каждой учетной записи пользователя есть свойство, отвечающее за то, что делать при выявлении нарушения целостности — либо блокировать загрузку (при условии, что в свойствах учетной записи включен параметр **Запретить работу при нарушенной целостности**), либо выдавать предупреждение и продолжать загрузку.

Проверка целостности по умолчанию осуществляется при загрузке компьютера, при доступе к объекту и при проверке по команде администратора. Дополнительно можно задать проверку целостности по расписанию и по времени.

Для расчета контрольных сумм по содержимому объектов используются алгоритмы: ГОСТ Р 34.11-94 (расчет хэш-функций), CRC32, MD5. Алгоритм выбирается администратором при назначении контроля целостности.

Для изменения значений параметров контроля целостности и для изменения списка контролируемых объектов: ФС, программно-аппаратной среды и веток реестра (добавление, удаление, редактирование), пользователь должен обладать правом **Параметры безопасности: управление**. В то же время для просмотра только значений установленных параметров и дескрипторов целостности пользователь должен обладать правом **Параметры безопасности: просмотр**.

СЗИ для возможности восстановления веток реестра при нарушении контроля целостности требуется доступ к соответствующим веткам от имени системного пользователя. Если доступ системному пользователю будет ограничен, функциональная возможность восстановления веток не будет работать корректно.

9.1 Настройка политик контроля целостности

Для настройки контроля целостности необходимо в оболочке администратора на вкладке *Параметры безопасности* выделить категорию **Политики контроля целостности**. В окне автоматически откроются параметры контроля целостности (рис. 174).

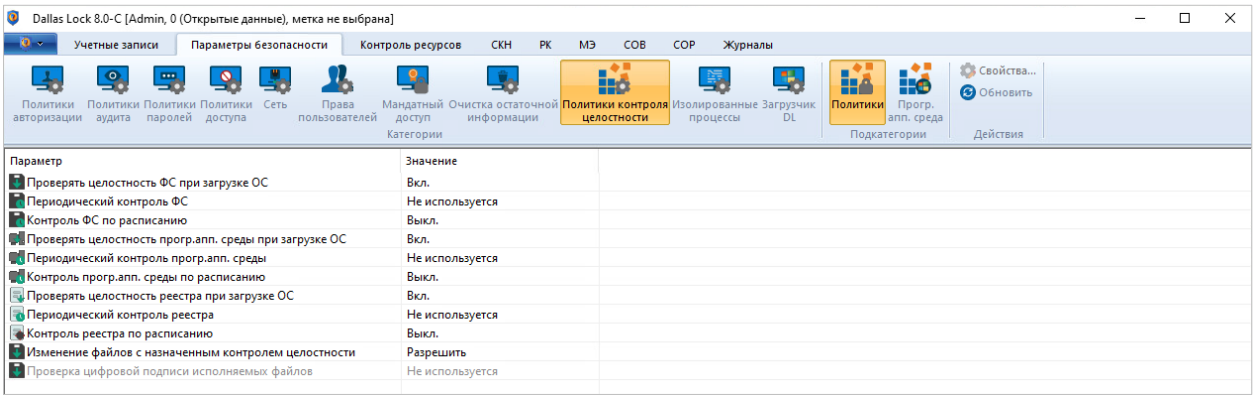


Рис. 174. Политики контроля целостности

С помощью данных параметров необходимо настроить периодичность проверки целостности отдельно для объектов ФС, отдельно для объектов программно-аппаратной среды и отдельно для реестра. По умолчанию проверка целостности установлена только при загрузке ОС.

Параметры проверки целостности при загрузке ОС могут быть установлены в значении «*включен*» или «*выключен*».

Параметры периодического контроля позволяют производить проверку целостности через указанный промежуток времени: от 1 минуты до 5 часов. Для отключения периода необходимо выбрать значение «*Не используется*».

Редактирование значений параметров контроля по расписанию позволяет настроить проверку целостности по гибкому расписанию (рис. 175).

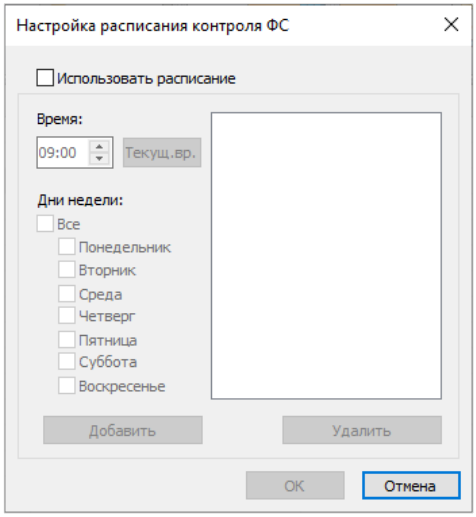


Рис. 175. Параметр «Контроль ФС по расписанию»

В окне настройки расписания необходимо включить контроль (поставить флаг в поле *Использовать расписание*) и составить расписание.

В случае обнаружения события нарушения целостности ФС в процессе периодического контроля ФС или контроля ФС по расписанию, действия СЗИ зависят от значения свойства текущего пользователя **Запретить работу при нарушенной целостности**. В случае, если это свойство включено, сеанс работы пользователя автоматически завершится. Если же это свойство выключено, то пользователю будет выведено предупреждение о нарушении целостности. Имена объектов ФС, целостность которых была нарушена, администратор системы защиты сможет посмотреть в журнале доступа к ресурсам.

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.

9.2 Контроль целостности объектов ФС и веток реестра

Моменты, когда осуществляется проверка целостности объектов ФС (файлов и папок) и веток реестра, определяются соответствующими политиками контроля целостности.

Также проверка целостности осуществляется по команде администратора (действие **Проверить** в оболочке администратора) и при доступе к объекту.

Назначить контроль целостности для файла можно двумя разными способами: используя оболочку администратора **СЗИ** или вызвав контекстное меню файла щелчком по его значку. Объекты ФС, на которые назначен контроль целостности любым из способов, автоматически появляются в списке объектов в окнах категорий **ФС** и **Реестр** при выбранном фильтре по типу контроля **Контроль целостности** на вкладке *Контроль ресурсов*.

При выборе категории **Все** на вкладке *Контроль ресурсов* также появляется список, содержащий параметры всех объектов: глобальных, локальных или сетевых, на которые назначены какие-либо права дискреционного доступа, аудит, а также контроль целостности.

9.2.1 Установка целостности

Для того, чтобы установить целостность для конкретного объекта ФС или ветки реестра, необходимо выполнить следующее:

1. Открыть дескриптор безопасности объекта, используя оболочку администратора **Dallas Lock 8.0** (перейти на вкладку *Контроль ресурсов*, выбрать тип ресурса **ФС** или **Реестр** и нажать кнопку **Добавить (ФС)** или **Добавить (Реестр)**) соответственно, или через контекстное меню объекта (пункт **Права доступа** для объекта ФС) (рис. 176).

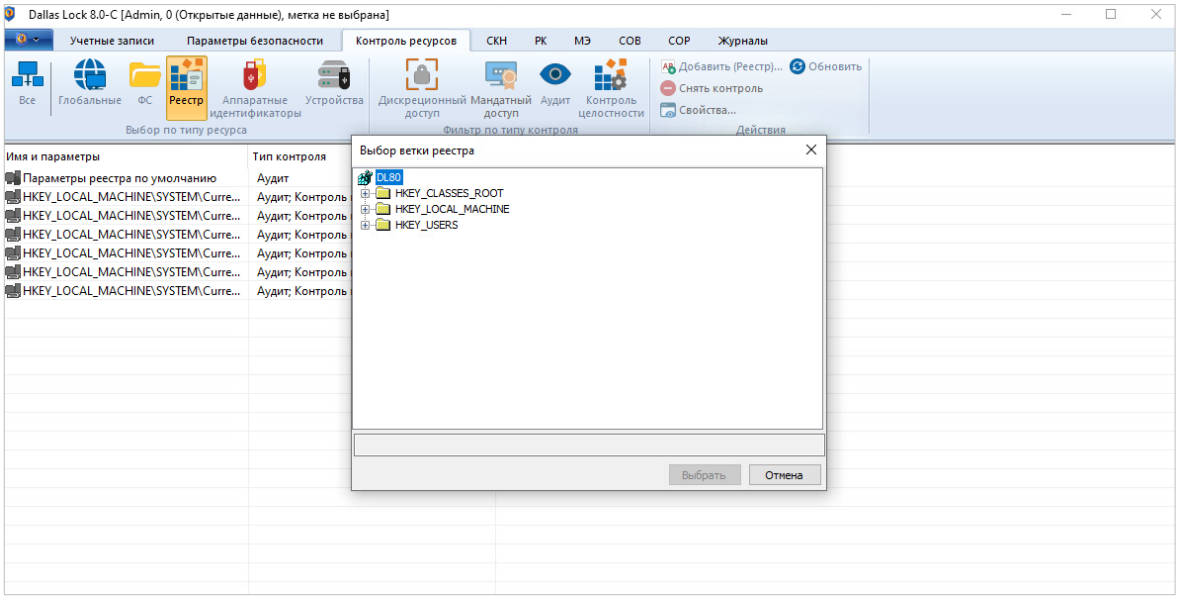


Рис. 176. Вызов дескриптора безопасности

2. В отобразившемся окне дескриптора безопасности объекта необходимо открыть закладку *Контроль целостности* (рис. 177).
3. Необходимо отметить флагом поле *Контроль целостности включен*, выбрать алгоритм расчета контрольной суммы (CRC32, Хэш ГОСТ Р 34.11-94, Хэш MD5) и нажать **Пересчитать**.
4. При необходимости нужно отметить следующие параметры для следующих объектов:
   - **Для файлов — Проверять контроль целостности при доступе** и Восстанавливать в случае нарушения целостности. При попытке доступа к файлу, у которого нарушена целостность, но отмечено поле *Проверять контроль целостности при доступе*, сеанс пользователя заблокируется (при условии, что в свойствах учетной записи включен параметр **Запретить работу при нарушенной целостности**). Правило распространяется

и для веток реестра.

- **Для папок** — **Проверять целостность при доступе** и **Включая вложенные папки**. Если поле *Включая вложенные папки* не отмечено, то контроль целостности будет распространяться только на содержимое корневой папки. Изменение содержимого вложенных папок к нарушению целостности не приведет. Если данное поле отмечено, то помимо корневой папки, на которую назначен контроль целостности, он будет распространяться и на содержимое внутренних (вложенных) папок. Правило распространяется и для веток реестра.
- **Для веток реестра** — **Включая вложенные ветки** и Восстанавливать в случае нарушения целостности.

5. Нажать **Применить** и **ОК**.

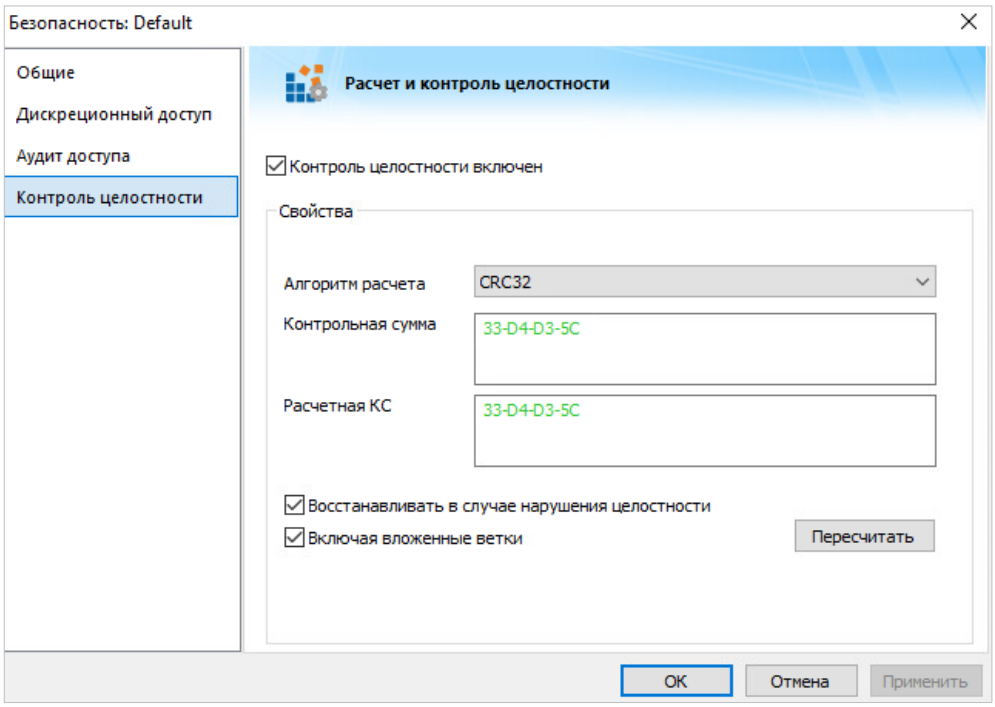


Рис. 177. Контроль целостности ресурса ФС

На вкладке *Параметры безопасности* в категории **Политики контроля целостности** необходимо установить значение параметра **Изменение файлов с назначенным контролем целостности** (рис. 178). Параметр может принимать одно из значений:

- «*Разрешить*» — при нарушении целостности **СЗИ** не блокирует доступ к объекту, для которого назначен контроль целостности;
- «*Запретить*» — при нарушении целостности **СЗИ** блокирует доступ к объекту, для которого назначен контроль целостности.

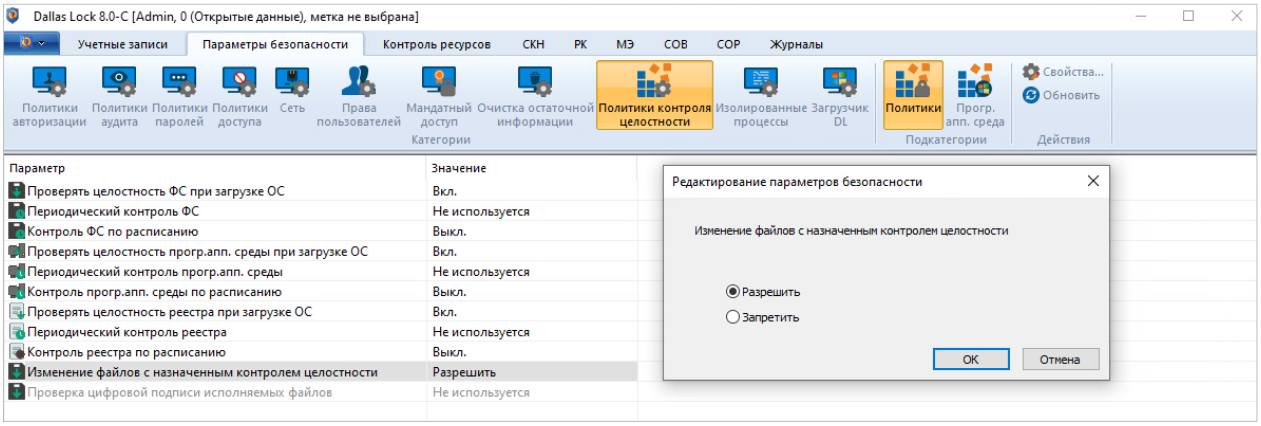


Рис. 178. Изменение файлов с назначенным контролем целостности

Для проверки цифровой подписи для исполняемых файлов перейти на вкладку *Параметры безопасности* в категории **Контроль целостности** и установить необходимое значение параметра **Проверка цифровой подписи исполняемых файлов** (рис. 179). Параметр может принимать значение «*Вкл*» или «*Выкл*». При «*Вкл*» необходимо указать расширения исполняемых файлов для проверки цифровой подписи.

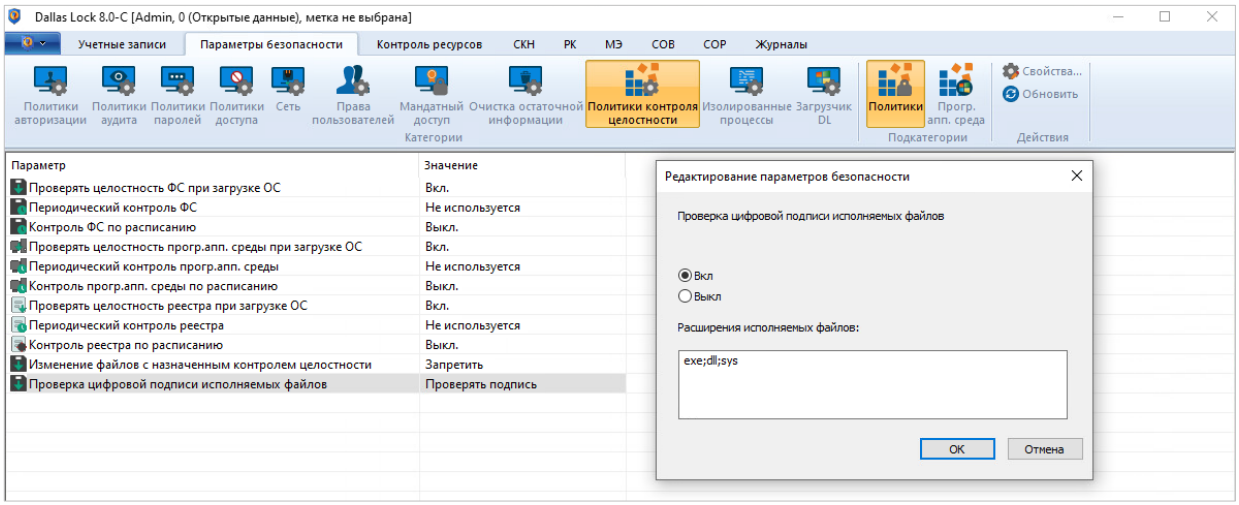


Рис. 179. Настройка проверки цифровой подписи исполняемых файлов

Если для объекта задан контроль целостности, то система защиты уже не позволит его удалить, изменить или переименовать. Попытки будут блокироваться. Такой объект будет доступен только для чтения и исполнения. Полный доступ к объекту, для которого установлен контроль целостности, имеет только суперадминистратор.

9.2.2 Проверка целостности

Если некоторый объект ФС или реестра, на который назначена целостность, будет изменен или поврежден, то при проверке (периодичность события проверки определяется установленными параметрами), контрольная сумма нарушится и ее запись в окне дескриптора безопасности будет выделена красным цветом (рис. 180).

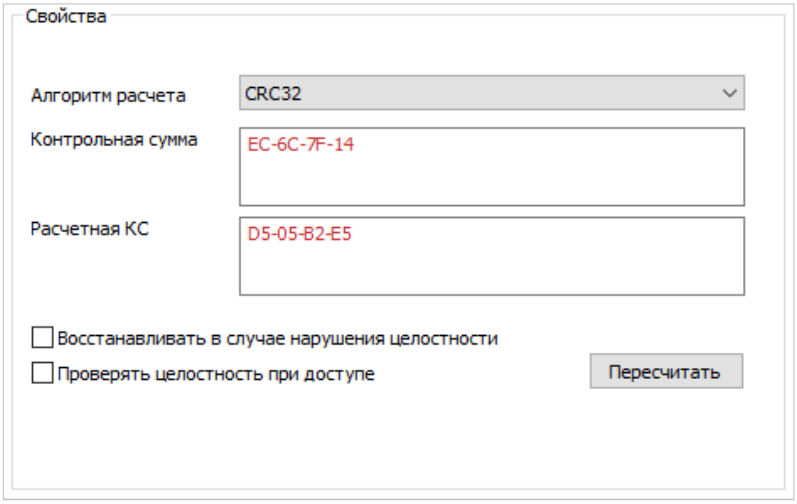


Рис. 180. Нарушение целостности файла

При нажатии на кнопку **Пересчитать** в окне дескриптора или на панели действий в оболочке администратора происходит пересчет контрольной суммы. Пересчет новой контрольной суммы позволяет снова установить целостность файла и проводить ее дальнейшее отслеживание.

События нарушения контроля целостности фиксируются в журнале ресурсов. При проверке целостности по команде администратора (действие **Проверить** в оболочке администратора) в списке объектов категории **Контроль целостности** значок объекта, у которого нарушена целостности будет выделен красным (рис. 181).

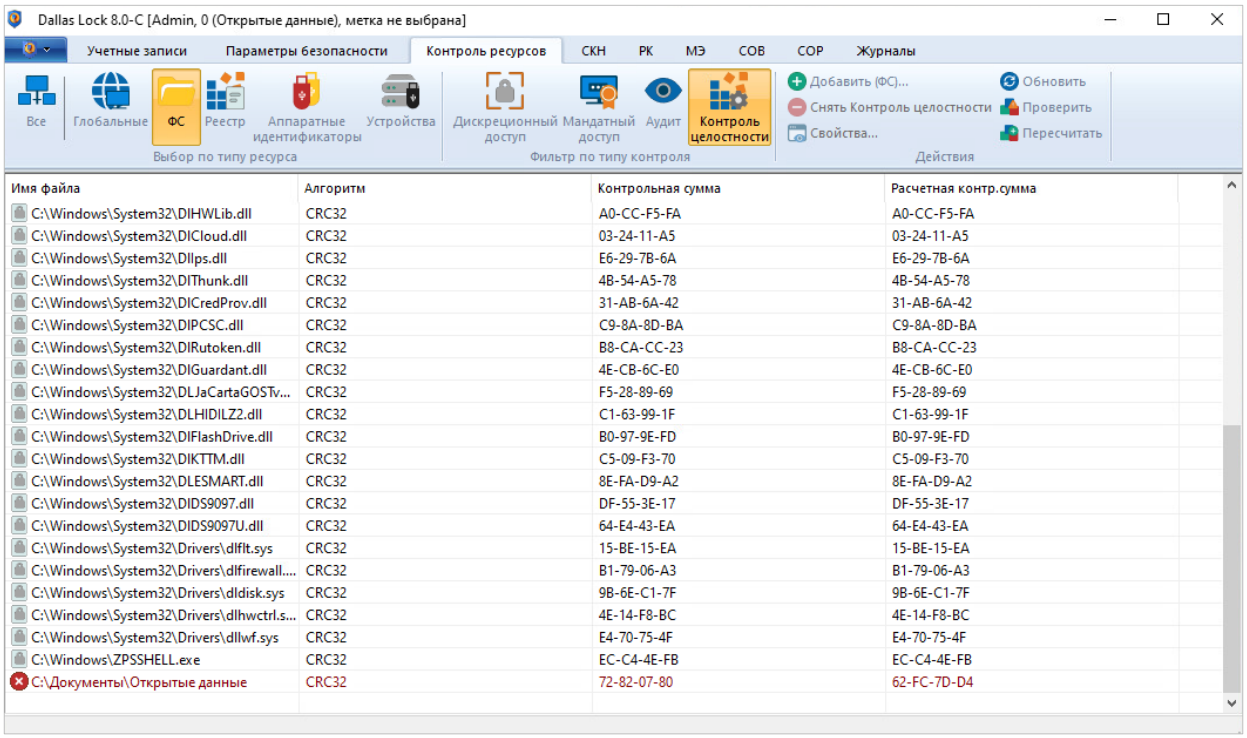


Рис. 181. Список контролируемых объектов

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

9.2.3 Восстановление файла или ветки реестра в случае нарушения целостности

Если для объекта (файла или ветки реестра) установлена целостность и отмечено свойство **Восстанавливать в случае нарушения целостности**, то в случае несанкционированного изменения объекта в результате проверки целостности он будет восстановлен до исходного состояния, для которого рассчитана контрольная сумма. Восстанавливается содержимое объекта и его атрибуты.

В списке объектов на вкладке **Контроль ресурсов** → **Контроль целостности** восстановленный объект будет выделен особым значком . Контрольные суммы восстановленного файла будут не измененными.

В журнал ресурсов будут занесены две записи о событиях: о нарушении целостности и о восстановлении объекта. Пользователю отобразится предупреждение.

9.3 Контроль целостности программно-аппаратной среды

С помощью политик контроля целостности на вкладке *Параметры безопасности* устанавливается периодичность и расписание контроля целостности для объектов программно-аппаратной среды.

Чтобы выбрать категории объектов программно-аппаратной среды, для которых требуется установить контроль целостности, необходимо открыть соответствующую категорию на вкладке **Параметры безопасности** → **Политики контроль целостности** (рис. 182).

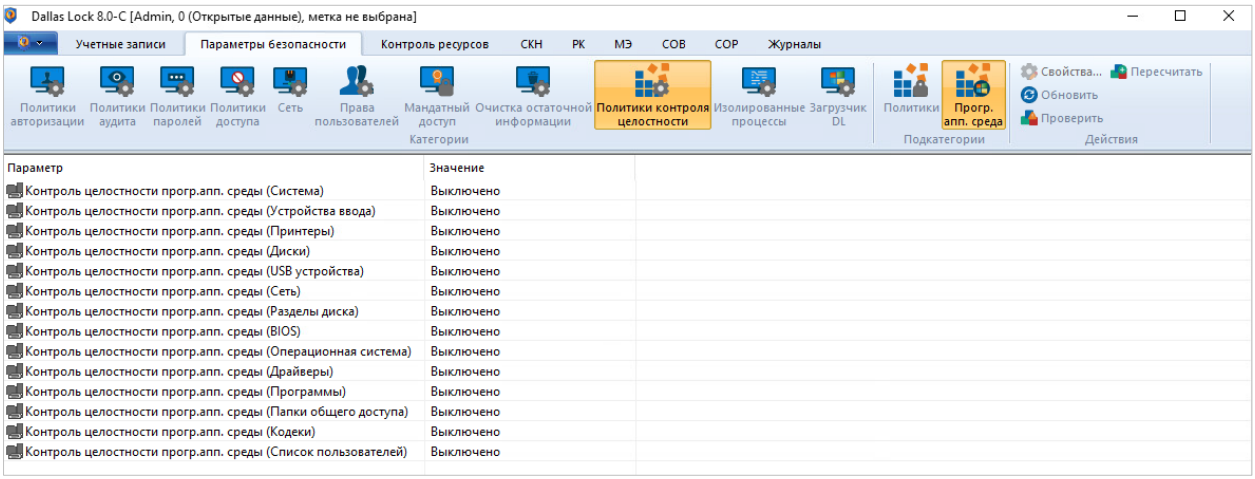


Рис. 182. Параметры программно-аппаратной среды

Для установки целостности параметров программно-аппаратной среды необходимо выделить параметр и нажать кнопку **Свойства**. В окне редактирования параметров выбрать алгоритм, который будет использоваться при подсчете контрольных сумм, либо отключить контроль целостности данного параметра (рис. 183).

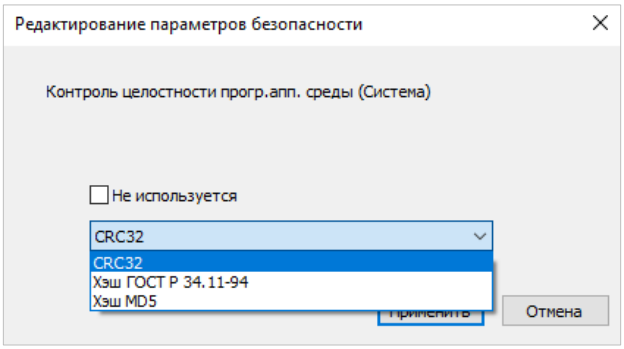


Рис. 183. Редактирование параметров безопасности

После нажатия кнопки **ОК** будет рассчитано значение контрольных сумм по алгоритму.

Для проверки значений целостности параметров следует нажать кнопку «Проверить». Система сверит установленные значения контрольных сумм параметров с текущими. В окне оболочки администратора у каждого параметра в списке появится значок, соответствующий значению целостности:

- — целостность не нарушена;
- — целостность нарушена;
- — целостность не установлена.

Чтобы установить новые значения целостности (пересчитать контрольные суммы параметров) следует нажать **Пересчитать**, система пересчитает значения контрольных сумм для параметров, у параметров появятся соответствующие значки.

Моменты, когда осуществляется контроль целостности программно-аппаратной среды, также, как и для объектов ФС, определяется политиками целостности: **Проверять целостность программно-аппаратной среды при загрузке ОС**, **Периодический контроль программно-аппаратной среды**, **Контроль программно-аппаратной среды по расписанию**. Также контроль целостности осуществляется по команде администратора (в оболочке администратора кнопка **Проверить**).

Расчет целостности программно-аппаратной среды по объективным причинам может занимать время. В связи с этим при включении контроля на какой-либо сегмент программно-аппаратной среды расчет эталонной контрольной суммы не производится. Он будет автоматически выполнен в момент первой проверки целостности. Таким образом, время на выполнение этой операции не отнимается у администратора без необходимости. Соответственно, если по каким-либо причинам есть потребность рассчитать эталонное состояние именно на текущий момент, следует сразу после назначения выполнить проверку целостности программно-аппаратной среды.

Dallas Lock 8.0 контролирует следующие объекты программно-аппаратной среды:

Параметр	Что контролируется
Система	Контролируются порты, мониторы, шины, звуковые устройства и другие системные устройства
Устройства ввода	Контролируются подключенные устройства ввода на данном ПК: клавиатуры, мыши
Принтеры	Контролируется список всех установленных на ПК принтеров, факсов, МФУ и др. печатающих устройств
Диски	Контролируются контроллеры гибких дисков, дисководы и дисковые устройства
USB-устройства	Контролируются изменения в USB-контроллере, подключения и отключения USB-портов
Сеть	Контролируются сетевые подключения и сетевые карты
Разделы диска	Контролируется добавление, изменение, удаление, форматирование и подключение новых дисков, но только для тех разделов, которым назначена буква
BIOS	Контролируются изменения параметров BIOS
Операционная система	Контролируются изменения свойств ОС данного ПК: изменение имени, IP-адреса и пр.
Драйверы	Контролируется установка и удаление драйверов
Программы	Контролируется установка или удаление программ на данном ПК
Папки общего доступа	Контролируется создание или удаление папок общего доступа на данном ПК
Кодеки	Контролируется установка или удаление кодеков на ПК
Список пользователей	Контролируется список пользователей, созданных в локальной ОС

10 КОНТРОЛЬ УСТРОЙСТВ

Основной задачей функции контроля доступа к устройствам в **Dallas Lock 8.0** является возможность разграничения доступа к подключаемым на ПК устройствам для определенных пользователей или групп пользователей и ведения аудита событий данного доступа.

Разграничение доступа и ведение аудита возможно, как для классов устройств, так и для конкретных экземпляров. К классу устройств на конкретном ПК может быть одновременно отнесено одно, несколько или ни одного устройств.

Чтобы произвести настройки доступа для контроля устройств, необходимо в оболочке администратора на вкладке основного меню *Контроль ресурсов* выбрать тип ресурса **Устройства** (рис. 184).

В основном окне отобразится дерево устройств, которое состоит из двух уровней иерархии: классов и индивидуальных устройств, которые входят в определенный класс. Если в класс входит несколько устройств, они отображаются последовательно.

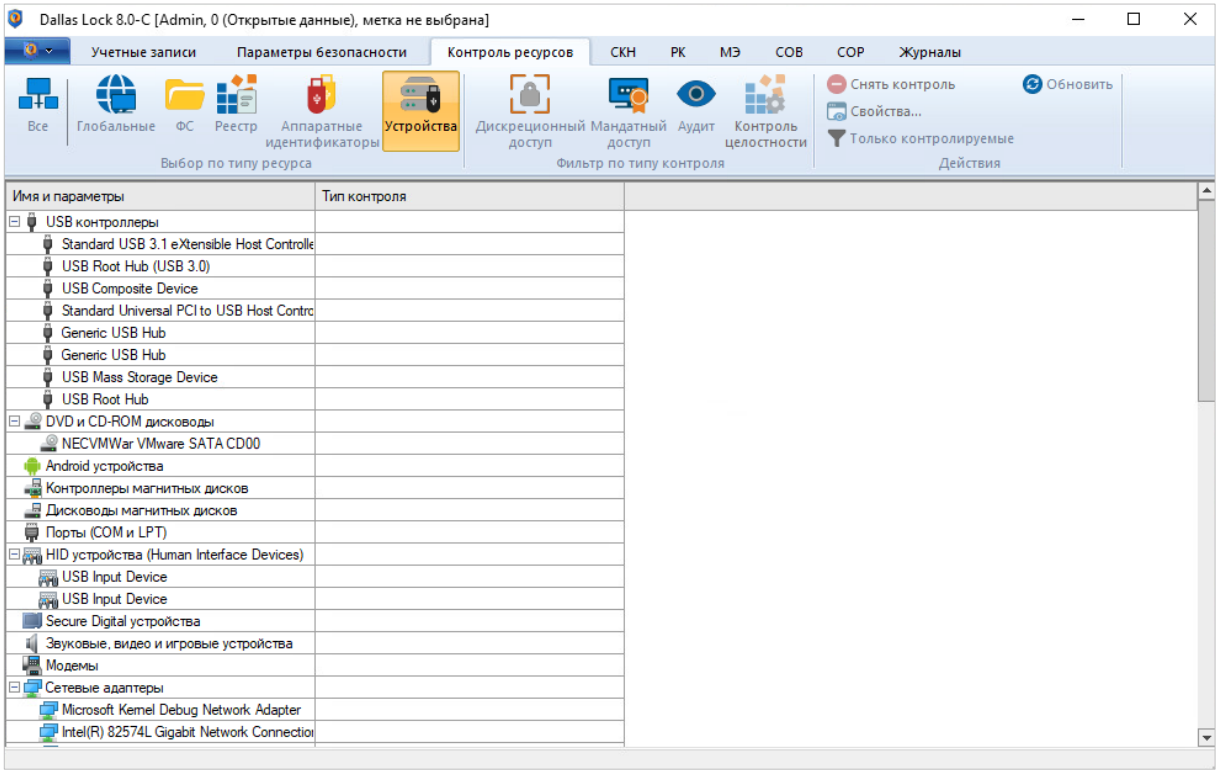


Рис. 184. Дерево классов и видов устройств

Список классов в **Dallas Lock 8.0** фиксирован и одинаков для всех защищенных ПК. Список устройств на каждом ПК свой индивидуальный, он берется из локальной ОС.

Также возможно блокировать перенаправляемые по RDP протоколу (Remote Desktop Protocol) устройства.

После назначения дискреционного доступа на **Перенаправленные по RDP устройства** администратору необходимо перезагрузить компьютер, чтобы назначенные права стали активными.

Часть устройств ПК относится к системным, без которых работа компьютера невозможна (процессор, оперативная память, видеоадаптеры, мосты системной платы и т. д.). Разграничивать доступ к таким устройствам не имеет смысла, так как запрет доступа к ним приведет к тому, что пользователь не сможет загрузить систему. Поэтому **Dallas Lock 8.0** такие устройства не контролирует.

При настройке работы с USB-устройствами их можно подключать как напрямую через USB-порт, так и через интерфейсные модули типа Anywhere USB.

Для идентификации сетевых принтеров приоритетным является использование протокола SNMP, который должен быть включен в настройках устройства. Если SNMP отключен, будет применен доступный метод идентификации принтера.

Для точной идентификации сетевого принтера необходимо проверить поддержку протокола WSD[12] и отключить его в настройках принтера, если это возможно. В случае невозможности отключения будет применен доступный метод идентификации принтера.

10.1 Полномочия на управление контролем устройств

Для того, чтобы иметь возможность управлять доступом к устройствам, пользователь должен иметь в **СЗИ** соответствующие права.

Для управления (назначения) дискреционным доступом к устройству учетная запись пользователя должна присутствовать в списке параметра **Ресурсы: Управление дискреционным доступом** (**Параметры безопасности** → **Права пользователей**).

Для управления (назначения) мандатным доступом к устройству учетная запись пользователя должна присутствовать в списке параметра **Ресурсы: Управление мандатным доступом** (**Параметры безопасности** → **Права пользователей**).

Если пользователю необходимо установить право только на просмотр уже установленных настроек доступа к устройствам, то его учетная запись должна присутствовать в списке параметра **Параметры безопасности: Просмотр**.

Пользователь, установивший **СЗИ**, суперадминистратор, обладает данными правами по умолчанию. В то же время, пользователь, учетная запись которого присутствует в списке **Параметры безопасности: Управление** может назначать других пользователей для управления доступом к устройствам.

Подробнее о предоставлении полномочий, раздел 3.6 Полномочия пользователей на администрирование системы защиты.

10.2 Разграничение доступа к устройствам

При настройке разграничения доступа к устройствам необходимо учесть следующие особенности:

В разных версиях ОС Windows в диспетчере устройств одно и то же физическое устройство может идентифицироваться по-разному. Это следует учитывать при определении прав доступа к устройству/классу устройств.

Сотовые телефоны в зависимости от комплектации самого устройства могут определяться как беспроводное устройство, как USB Flash накопитель, как набор портов, или даже как несколько устройств одновременно. В категорию **Беспроводные устройства** могут попадать устройства беспроводного доступа, такие как современные сотовые телефоны-модемы, в тоже время беспроводные адаптеры Wi-Fi обычно попадают в категорию **Сетевые адаптеры**. Это связано с особенностью реализации самих устройств и их драйверов, и может быть установлено наверняка опытным путем. В категорию "Переносные устройства (iOS и другие)" не попадают USB-Flash накопители.

Иногда некоторые устройства после их выключения могут потребовать перезагрузку компьютера для последующего включения. Это особенность конкретных устройств, которая будет проявляться и без **Dallas Lock 8.0** (если, например, вручную запретить устройство через диспетчер устройств). Важно помнить об этом, особенно при назначении мандатных уровней для доступа к устройствам — устройство может не включиться после входа пользователя под «разрешенным» уровнем, и для включения устройства будет требоваться перезагрузка ОС.

При разграничении доступа к устройствам, отличным от COM/LPT-портов, запрет доступа действует на всех пользователей и устройство полностью отключается в случае его запрета. Отключенное устройство будет недоступно, в том числе, для учетной записи пользователя, выполнившего установку СЗИ, суперадминистратора.

[12] WSD (Web Services for Devices) — это протокол автоматического обнаружения принтеров в сети, который не предоставляет MAC-адрес и может динамически менять IP-адрес.

!	Не рекомендуется глобально запрещать все USB-контроллеры, лучше выполнять блокировку на уровне конкретных контроллеров и устройств.
!	Запрещая использование некоторых устройств, например, USB-устройств ввода, можно лишиться возможности работать устройствами типа «мышь» и «клавиатура» и, соответственно, возможности отменить данную настройку на локально установленной **СЗИ** (тем не менее, по сети можно будет выполнить отмену такой настройки).
!	Важно помнить, особенно при настройке терминального сервера, что при назначении мандатного доступа к устройствам, устройства (кроме COM/LPT-портов) запрещаются, если в ОС зарегистрирована хотя бы одна сессия, которая является запрещенной для устройства. Например, если сетевой адаптер запрещен для работы в режиме «открытые данные», то пока на компьютере присутствует хотя бы одна сессия с открытыми данными, сетевой адаптер будет выключен. Вычисление эффективного состояния всех устройств в зависимости от настроек мандатного доступа и зарегистрированных в ОС сессий осуществляется в момент входа новой сессии и в момент завершения любой из сессий.

Для настройки прав доступа к классам устройств или устройствам необходимо выбрать соответствующий элемент в дереве устройств и нажать на кнопку «Свойства» на панели действий (или выбрать данное действие в контекстном меню объекта).

Откроется окно редактирования дескриптора устройства, которое состоит из закладок: *Дискреционный доступ*, *Мандатный доступ* и *Аудит доступа*. В зависимости от политик безопасности необходимо выполнить установку прав доступа. Значки устройств и классов в дереве объектов, для которых назначены какие-либо права, будут выделены определенным образом.

В дереве устройств помимо элементов, отображающих устройства данного ПК присутствуют дополнительные классы устройств. Это — классы съемных накопителей и преобразованных съемных накопители (только для Dallas Lock 8.0 с модулем СКН). Настройки доступа и аудита для объектов данных классов устанавливаются по общим правилам, а также соответствуют глобальным одноименным дескрипторам в списке вкладки «Контроль ресурсов» → «Глобальные», разделы 13.3.3 Доступ к преобразованным накопителям, 5.2.3 Дискреционный доступ для глобальных параметров и 6.2.1 Аудит для глобальных параметров.

10.2.1 Дискреционный доступ к устройствам

Дискреционный принцип разграничения доступа к устройствам состоит из двух возможностей: доступ всех пользователей к данному устройству разрешен и доступ запрещен (рис. 185). Для некоторых классов устройств разграничение дискреционного доступа на уровне пользователей не доступно, т.е. возможности выбора учетных записей нет, кроме записи «*Все*».

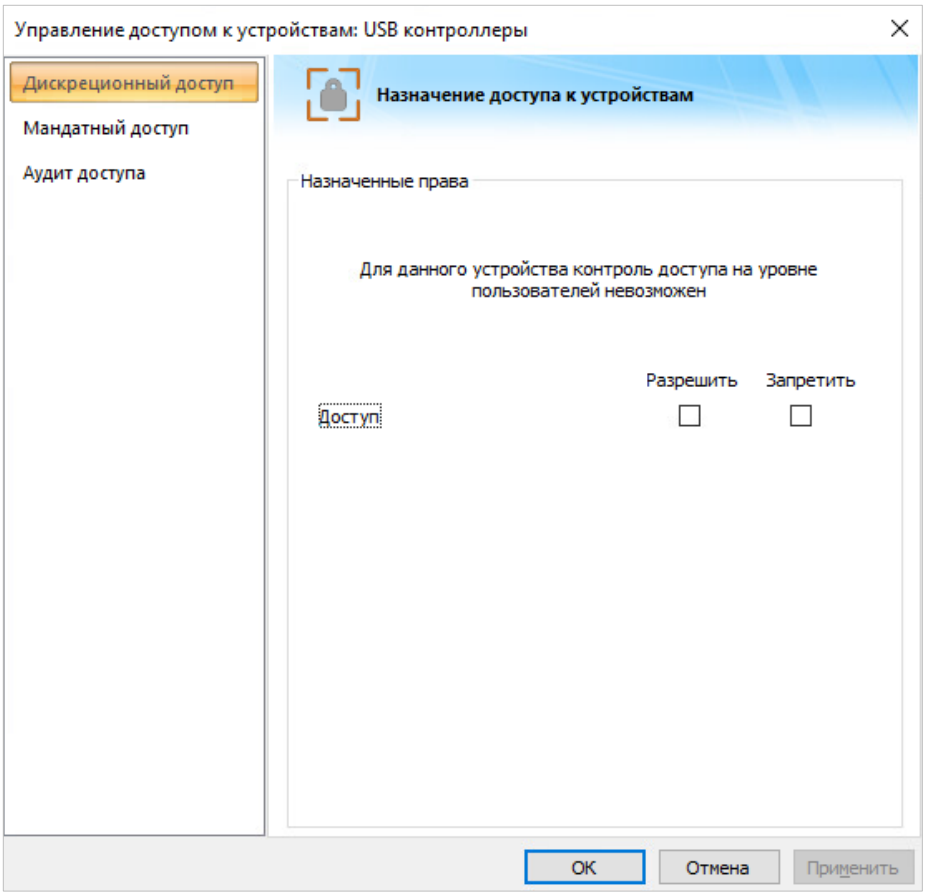


Рис. 185. Дескриптор дискреционного доступа к устройству

Принцип определения прав доступа пользователей к устройствам аналогичен Механизму определения прав доступа пользователя к ресурсам файловой системы:

1. Права, заданные для класса устройств, имеют более низкий приоритет, чем права, заданные для конкретного экземпляра.
2. Права, заданные для группы пользователей, имеют более низкий приоритет, чем права, заданные для пользователя (если доступно разграничение на уровне пользователей).
3. Если доступ к устройству не назначен ни классу, которому принадлежит устройство, ни самому устройству, то доступ разрешен.

10.2.2 Мандатный доступ к устройствам

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

Подробнее о принципе мандатного разграничения доступа раздел 5.3 Мандатный доступ. Установка мандатного доступа на устройство происходит путем определения уровней доступа и мандатных меток в дескрипторе объекта, для работы под которыми устройство должно быть доступно.

Для того, чтобы установить мандатный доступ на устройство, необходимо в окне дескриптора доступа объекта на закладке *Мандатный доступ* поставить флаг в поле *Мандатный доступ включен*, отметить мандатные уровни и добавить мандатные метки (рис. 186).

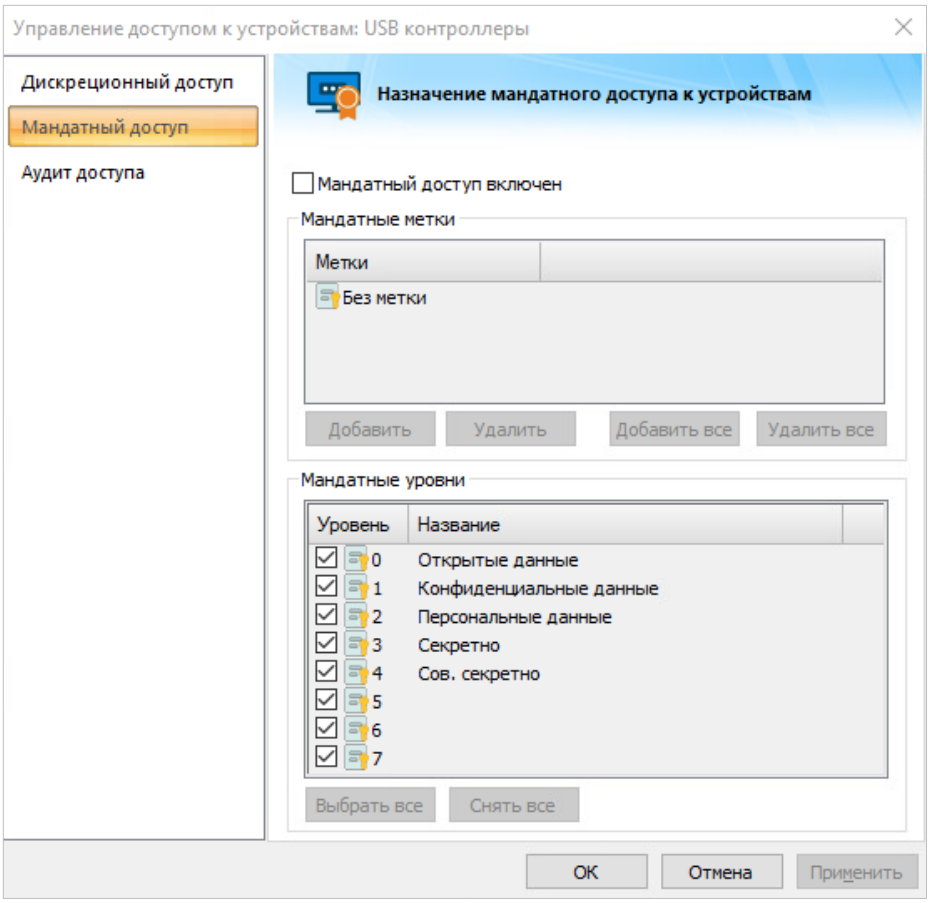


Рис. 186. Управление доступом к устройствам

Мандатный доступ можно назначить как для класса устройств, так и для отдельного экземпляра, при этом действует следующий принцип определения мандатного доступа:

- Если для устройства заданы некоторые мандатные уровни и мандатные метки, то доступ осуществляется в соответствии с ними.
- Если для устройства не заданы мандатные уровни и мандатные метки, то используются значения мандатного доступа класса устройств.
- Если и для класса устройств не назначены мандатные уровни и мандатные метки, то работать с устройством можно под всеми уровнями и метками.
- Сложения значений не происходит. Значения уровней устройства, если они заданы, «перекрывают» значения уровней класса. Например, если для класса значения состоят из уровней 0,1,2, а для устройства значения состоят из уровней 2,3, то действуют значения 2,3.

Мандатный доступ можно назначить к классам устройств, контролирующимся через контроль устройств (кроме съемных накопителей, преобразованных накопителей и перенаправляемые по RDP устройства).

10.3 Аудит доступа к устройствам

Для назначения аудита событий доступа к устройствам в первую очередь необходимо включить два глобальных параметра безопасности **Аудит устройств** и **Журнал ресурсов** на вкладке основного меню **Параметры безопасности** → **Политики аудита** (значение «*Вкл.*»).

В окне редактирования дескриптора выбранного устройства необходимо выбрать закладку *Аудит доступа*. Далее включить аудит устройства: поставить флаг в поле *Аудит включен* и выбрать из двух событий аудита: аудит успешных подключений устройства («Успех») или аудит неуспешных подключений («Отказ»).

Если для конкретного устройства не установлен аудит событий, то события аудита будут соответствовать значениям для класса, которому принадлежит данное устройство; если у класса устройств тоже не будут выбраны значения аудита, то аудит вестись не будет.

Аудит событий доступа к устройствам, а также аудит событий по настройке доступа ведется в журнале ресурсов, раздел 6.3 Журналы.

11 УДАЛЕННЫЙ ДОСТУП И СЕТЕВОЕ АДМИНИСТРИРОВАНИЕ

Если ЗАРМ входит в состав ЛВС, то информация, хранящаяся на этом компьютере, защищена от НСД по сети.

Возможны следующие ситуации:

1. Пользователь обращается к незащищенному **Dallas Lock 8.0** компьютеру с компьютера, который защищен **Dallas Lock 8.0**.
2. Пользователь обращается к защищенному **Dallas Lock 8.0** компьютеру с компьютера, на котором эта система не установлена (с незащищенного компьютера).
3. На компьютерах, с которого обращаются и к которому обращаются, установлена система защиты **Dallas Lock 8.0**.

Удаленный доступ защищенных компьютеров осуществляется независимо от редакций системы защиты **Dallas Lock 8.0** «К» или «С».

11.1 Удаленный доступ к незащищенному компьютеру с защищенного

Данный случай ничем не отличается от случая, когда доступ осуществляется с незащищенного СЗИ компьютера на незащищенный компьютер.

11.2 Удаленный доступ к защищенному компьютеру с незащищенного

По умолчанию в системе **Dallas Lock 8.0** на ЗАРМ предусмотрена зарегистрированная учетная запись пользователя *anonymous*.

Для того, чтобы был возможен доступ к защищенному **СЗИ** компьютеру по сети с незащищенного компьютера, учетная запись пользователя *anonymous* должна быть включена. Также нужно проследить, чтобы пользователю anonymous не был запрещен удаленный доступ. Все остальные права пользователя *anonymous* администратор определяет согласно проводимой политике безопасности.

Таким образом, со всех компьютеров, включенных в ЛВС, но не защищенных **СЗИ**, можно будет обратиться к ЗАРМ и получить доступ к его ресурсам в рамках прав, установленных для учетной записи *anonymous*.

При попытке обратиться к ЗАРМ на экране может возникнуть сообщение об ошибке (рис. 187).

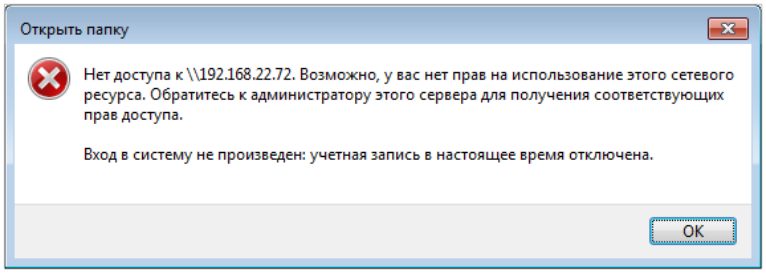


Рис. 187. Ошибка подключения к удаленному компьютеру

В этом случае следует внимательно проверить права, предоставленные учетной записи *anonymous*, в частности, право на удаленный доступ. Нужно внимательно просмотреть журнал входов, так как в нем можно увидеть причину отказа.

11.3 Удаленный доступ к защищенному компьютеру с защищенного

Для удаленного входа необходимо, чтобы у учетной записи, под которой входит пользователь, параметрами безопасности было предусмотрено соответствующее право: вкладка **Параметры безопасности** → категория **Права пользователей** → параметр **Удаленный вход: Разрешен**.

При удаленном входе с ЗАРМ на ЗАРМ, пользователь осуществляет вход под учетной записью с таким же именем, под которым он работает. Если на удаленном компьютере нет учетной записью с таким же именем, у пользователя есть возможность войти под учетной записью *anonymous*, которая предусмотрена в системе защиты по умолчанию.

Следует учитывать, что, если на ЗАРМ «Клиент» выполняется вход под пользователем «*user1*» и данный пользователь выполняет подключение сетевого диска через подключение к удаленной ЗАРМ «Сервер» под пользователем «*user2*», СЗИ на ЗАРМ «Сервер» будет фиксировать подключение именно пользователя «*user1*». Это обосновано тем, что работать с подключенным сетевым диском будет именно пользователь «*user1*».

В случае неудачного соединения, доступ к удаленному компьютеру осуществлен не будет, и система выдаст предупреждение.

На разных защищенных компьютерах в ЛВС одна учетная запись может быть зарегистрирована с разными правами. Когда происходит удаленный вход, права проверяются в соответствии с правами учетной записи удаленного компьютера.

Еще одним необходимым условием удаленного входа является следующее: если в свойствах учетной записи удаленного компьютера включен параметр **Запретить работу при нарушенной целостности**, то на удаленном компьютере целостность не должна быть нарушена.

Так же следует обратить внимание на то, что удаленный ввод аппаратного идентификатора не поддерживается.

11.4 Ключи защиты сетевого взаимодействия

Каждый защищенный **Dallas Lock 8.0** компьютер имеет ключ защиты сетевого взаимодействия. Данный параметр предназначен для усиления защиты сетевого взаимодействия между клиентом и модулем удаленного администрирования **Сетевой администратор**, раздел 11.5 Сетевое администрирование. Указанные виды сетевого взаимодействия возможны только при условии совпадения ключей защиты сетевого взаимодействия.

На всех защищенных компьютерах в ЛВС после установки **СЗИ** с файлом конфигурации по умолчанию зарегистрирован ключ защиты сетевого взаимодействия с пустым значением. Однако в системе реализована возможность изменения указанного ключа на компьютере. Для этого в оболочке администратора на вкладке *Параметры безопасности* в категории политик безопасности **Сеть** необходимо выбрать и открыть параметр **Ключ защиты сетевого взаимодействия** и заполнить требуемые поля (рис. 188).

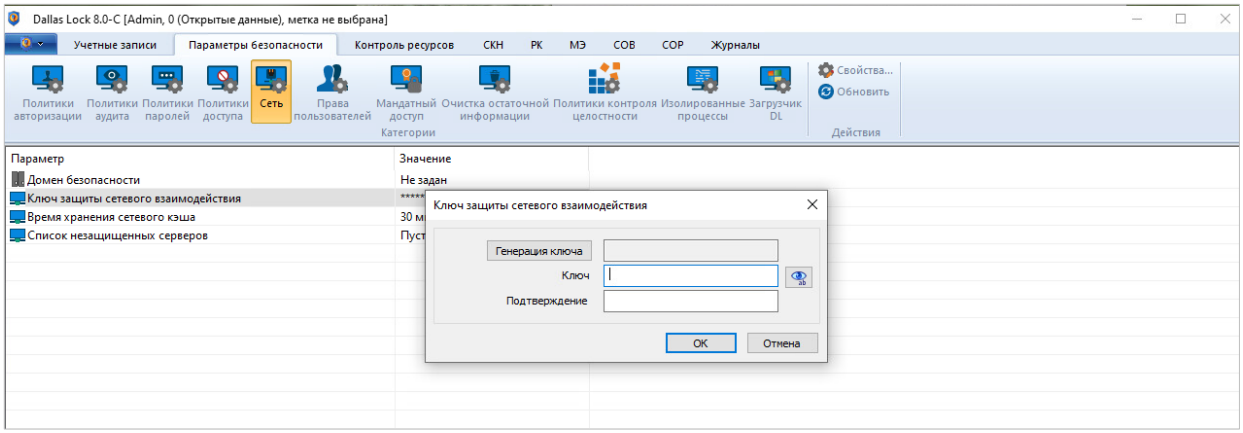


Рис. 188. Окно ввода нового ключа защиты сетевого взаимодействия

Рекомендуется вводить и изменять настройки ключей защиты сетевого взаимодействия только опытным специалистам, и только в тех случаях, когда это действительно необходимо. Так как неосторожная смена ключа доступа у одного ПК, может привести к тому, что удаленный доступ на него будет невозможен.

Для создания ключа защиты сетевого взаимодействия, отвечающего всем требованиям параметров безопасности, установленных системой защиты **Dallas Lock 8.0**, можно воспользоваться помощью генератора паролей системы защиты. Для этого следует нажать поле с надписью: *Генерация ключа*. Система автоматически создаст уникальный ключ, значение которого необходимо ввести в поля *Ключ* и *Подтверждение*.

Дополнительная кнопка  изменит скрытые символы на явные. Подтверждение в этом случае не потребуется и заблокируется.

Политики сложности паролей распространяются и на установку значений для ключа защиты сетевого взаимодействия. Поэтому, чтобы была возможность задать пустое значение ключа защиты сетевого взаимодействия, необходимо, чтобы параметр **Минимальная длина пароля** имел значение *Не используется*.

11.5 Сетевое администрирование

Система защиты **Dallas Lock 8.0** позволяет осуществлять сетевое (удаленное) администрирование параметров безопасности других компьютеров, на которых установлена система защиты. С помощью сетевого администрирования возможны те же действия, что и при локальном администрировании: создание, удаление, редактирование пользователей и групп; редактирование политик безопасности; просмотр, назначение, редактирование параметров доступа, контроля целостности, аудита объектов ФС; просмотр журналов и прочее.

Визуально процесс сетевого администрирования практически не отличается от процесса локального администрирования, так как запускается та же самая оболочка администратора, которая подключается не к локальному драйверу защиты, а к удаленному.

После установки системы защиты на компьютере в меню **Пуск** в группе программ **Dallas Lock 8.0** появляется значок модуля удаленного администрирования **Сетевой администратор** (рис. 189).

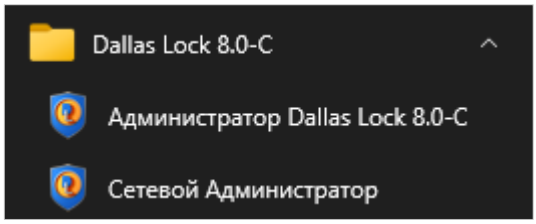


Рис. 189. Вызов удаленного администрирования СЗИ

Для осуществления сетевого администрирования на компьютерах, входящих в ЛВС, необходимо соблюдение следующих условий:

- На всех компьютерах, для которых предполагается сетевое администрирование, должна быть установлен **Dallas Lock 8.0**.
- Для межсетевого взаимодействия на целевых компьютерах, защищенных **Dallas Lock 8.0**, должен быть открыт TCP/IP порт 17490.
- На всех компьютерах, для которых предполагается сетевое администрирование, должны быть установлены одинаковые ключи защиты сетевого взаимодействия 11.4 Ключи защиты сетевого взаимодействия.

По умолчанию в системе защиты ключ защиты сетевого взаимодействия пустой, и если ни на одном из компьютеров он не изменялся, то специально для осуществления сетевого взаимодействия его вводить не следует.

- Пользователь, осуществляющий сетевое администрирование (удаленный администратор), должен быть зарегистрирован на всех компьютерах К1, К2, К3…Kn.
- Администратор должен обладать правом удаленного доступа на целевых компьютерах: вкладка **Параметры безопасности** → категория **Права пользователей** → параметр **Вход в ОС: удаленный** (в параметрах локально установленной **СЗИ**).
- На компьютерах К2, К3…Kn сетевому администратору должны быть предоставлены соответствующие полномочия на администрирование.
- Сетевое администрирование защищенных компьютеров осуществляется, независимо от редакций установленной системы защиты **Dallas Lock 8.0** «К» или «С».

При соблюдении этих условий с компьютера К1 можно осуществлять сетевое администрирование компьютеров К2, К3…Kn. Для этого необходимо запустить модуль **Сетевой администратор** и в появившемся окне ввести имя удаленного компьютера и авторизационные данные учетной записи пользователя (рис. 190). Если администрирование удаленного ПК осуществляется под учетной записью текущего пользователя, то авторизационные данные можно не вводить, но отметить флагом поле *Использовать текущего пользователя*.

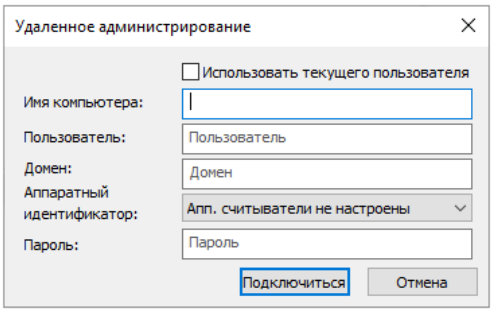


Рис. 190. Доступ к удаленному администрированию

Если имя и данные пользователя введены верно и все вышеперечисленные условия соблюдены, то на экране развернется оболочка администратора **Dallas Lock 8.0** с параметрами удаленного компьютера, и пользователь получит возможность осуществлять администрирование в рамках, предоставленных ему на том компьютере полномочий.

В случае неудачного соединения, доступ к удаленному компьютеру осуществлен не будет, и появится предупреждение. В этом случае следует внимательно проверить выполнение условий осуществления удаленного администрирования.

В окне отображения текущих сессий на клиенте в оболочки администратора можно наблюдать появление новой записи о текущей сессии и завершать активные сессии под учетной записью суперадминистратора с удаленного компьютера, (рис. 191).

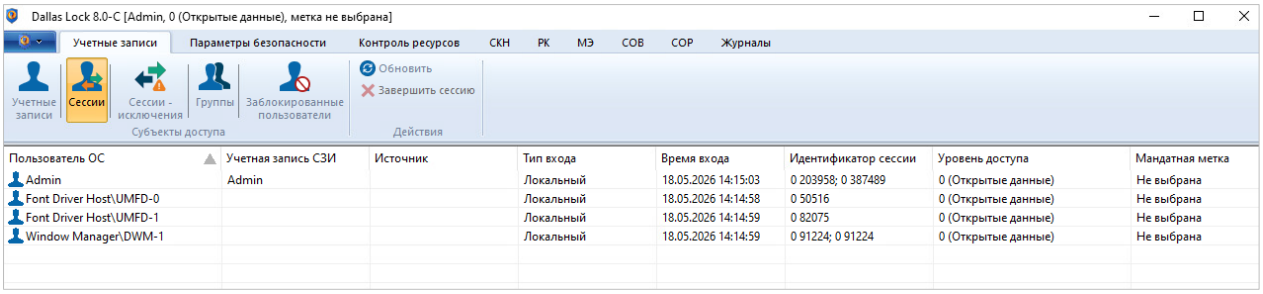


Рис. 191. Сессии пользователей при удаленном администрировании

В списке меню дополнительных функций оболочки администратора при удаленном администрировании компьютера появится функция принудительной перезагрузки удаленного компьютера (рис. 192).

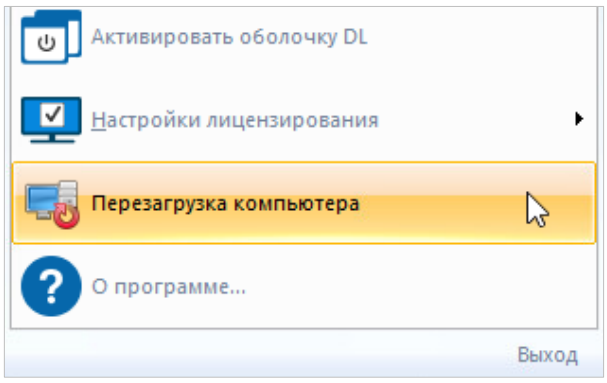


Рис. 192. Кнопка перезагрузки при удаленном администрировании

Однако функции **Тестирование функций СЗИ** и **Зачистка диска** станут недоступны.

12 ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ

12.1 Прозрачное преобразование дисков

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

В состав системы защиты **Dallas Lock 8.0-С** входит механизм прозрачного преобразования жесткого диска уровня загрузочной записи. Прозрачное преобразование позволяет осуществить преобразование информации, хранящейся на локальных, а также съемных жестких дисках.

При попытке работы с преобразованным жестким диском в обход системы защиты **Dallas Lock 8.0**, например, при извлечении жесткого диска из одного ПК и подключении его к другому, данные будут защищены.

Прозрачное преобразование становится доступным после включения модуля загрузчика DL. При включении загрузчика DL выбирается алгоритм преобразования жесткого диска. Выбор алгоритма преобразования зависит от политик информационной безопасности, принятых в организации. Подсистема позволяет настраивать и размер преобразуемой части жесткого диска.

Выполнять преобразование диска (полное или частичное), можно только убедившись, что сам модуль загрузчика DL корректно загружает ПК по PIN-коду.

После инициации процесса преобразования необходимо дождаться его завершения. Отслеживать статус возможно через оболочку администратора

Система защиты **Dallas Lock 8.0-С** не поддерживает использование функции прозрачного преобразования системной области на виртуальных машинах VMWare и Hyper-V с UEFI и дисками GPT.

Для преобразования дисков необходимо:

1. Включить модуль загрузчика DL 4.7 Загрузчик DL.
2. Перейти на вкладку *Список зон* (**Параметры безопасности** → **Загрузчик DL** → **Список зон**) и нажать действие **Добавить зону**[13].

Откроется окно создания зоны жесткого диска для прозрачного преобразования (рис. 193).

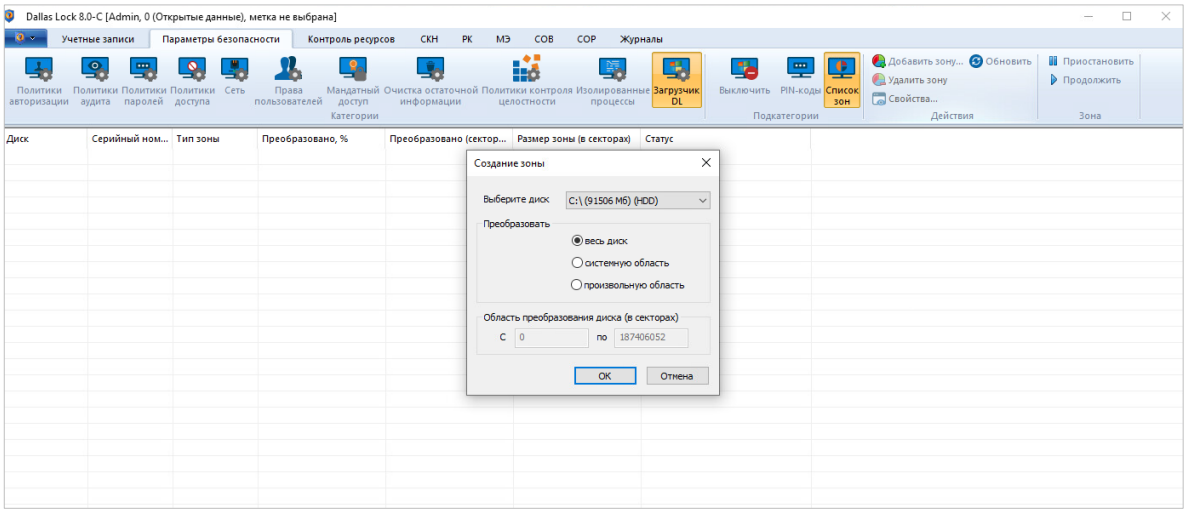


Рис. 193. Параметры создания зоны преобразования

3. В данном окне необходимо выбрать диск. Указать область выбранного диска, которую необходимо преобразовать:
   - весь диск;
   - системную область диска;
   - произвольную область (с указанием размера).

[13] Вызов данной функции также возможен из контекстного меню.

4. Нажать кнопку **OK** и подтвердить операцию. После чего сразу начнется процесс преобразования выбранной зоны жесткого диска.

В окне хода выполнения процесса преобразования его можно приостановить и продолжить, выбрав запись о процессе в списке основного окна и нажав кнопку на панели действий.

После преобразования на данной вкладке оболочки администратора в списке процессов появится запись о параметрах данного процесса преобразования.

Далее работа с данными жесткого диска, имеющего преобразованные области, на защищенном **Dallas Lock 8.0** компьютере никак не будет отличаться от работы с непреобразованными областями.

Чтобы удалить зону преобразования, т.е. произвести восстановление жесткого диска или его части, необходимо выделить его в списке и нажать кнопку **Удалить зону** на панели действий, далее подтвердить операцию. Запустится процесс обратного преобразования, который также можно приостановить и возобновить позже.

Выбор действия **Аварийное восстановление** клавишей **F2** при входе в загрузчике необходимо для обратного преобразования дисков до этапа загрузки ОС и доступно только с PIN-кодом администратора. Восстановление диска на данном этапе является необходимым для восстановления работоспособности компьютера при сбое системы защиты 21 Восстановление компьютера при сбое системы защиты.

12.2 Преобразование данных в файл-контейнер

Имеющиеся на защищенном ПК файлы или папки могут быть преобразованы в файл-контейнер с помощью системы защиты **Dallas Lock 8.0** с использованием ключевой информации (пароля и (или) аппаратного идентификатора). Преобразованные файлы или папки могут быть обратно преобразованы в исходные данные, при условии верного ввода ключевой информации.

Таким образом, содержимое файлов-контейнеров становится недоступным на ПК, не защищенном **Dallas Lock 8.0**, и также недоступным на ПК, защищенном **СЗИ**, но в случае введения неверной ключевой информации при обратном преобразовании.

Преобразованные данные хранятся в файле-контейнере, который может быть безопасно передан по незащищенным сетевым каналам, электронной почте или с помощью съемного накопителя.

Для восстановления этих данных необходим пароль и аппаратный идентификатор, используемый при преобразовании.

Следует отметить, что права на использование данной функции конкретному пользователю для конкретного файла определяются параметрами безопасности, установленными администратором безопасности. Если у пользователя данные права отсутствуют (установлен флаг *Запретить* в поле *Запись* в дескрипторе объекта для пользователя или группы), то попытка преобразования и зачистки исходных данных будет неуспешной, и появится предупреждающее сообщение.

12.2.1 Преобразование объектов ФС

Чтобы преобразовать объект ФС, необходимо выбрать в контекстном меню соответствующего файла или папки пункт **DL80: Преобразование** (рис. 194).

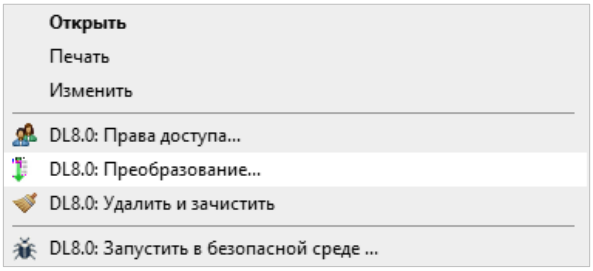


Рис. 194. Контекстное меню

На экране появится окно модуля преобразования объекта ФС, в котором необходимо указать данные и параметры. Окно модуля преобразования объекта ФС содержит следующие поля для заполнения:

Наименование поля	Описание
Результат преобразования	Имя и путь к будущему файлу-контейнеру (по умолчанию, оно формируется из имени преобразовываемого объекта с добавлением специального расширения, в текущей папке).

Наименование поля	Описание
	Имя будущего файла и путь к нему можно прописать вручную. Выбор другой папки можно осуществить с помощью кнопки **Обзор…**
Алгоритм преобразования	Операции по настройке алгоритма преобразования. По умолчанию используется встроенный в **Dallas Lock 8.0** алгоритм.
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей, подраздел 4.5.2 Настройка политик авторизации. Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные
Аппаратная идентификация	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка. Если аппаратный идентификатор не указывать, преобразование происходит только по паролю
Уровень доступа	Поле является информационным. При преобразовании объекта (только для Dallas Lock 8.0 редакции «С») ему присваивается мандатный уровень и мандатная метка текущего уровня доступа пользователя. При обратном преобразовании в этом же поле — уровень доступа, который назначен при прямом преобразовании. Для объектов, в **СЗИ** редакции «К» документы имеют уровень доступа «0»
Зачистить исходные файлы	Выбор операции по зачистке исходных данных после получения преобразованного файла-контейнера
Комментарий	Комментарий к файлу-контейнеру (он не преобразуется, является необязательным и доступен без пароля)

После заполнения всех необходимых параметров необходимо нажать **Преобразование**.

Преобразование может производиться без задания пароля, если будет использован аппаратный идентификатор. Значение пароля, который используется при преобразовании, должно соответствовать установленным политикам сложности паролей.

Процесс преобразования будет сопровождаться заполнением полосы индикатора прогресса. По окончании процесса будут выведены следующие сообщения: «Исходный файл удален!» (если операция по зачистке исходных файлов была включена) и сообщение об успешном преобразовании. Файл–контейнер с расширением *.dlcf появится в указанной папке (рис. 195).



Рис. 195. Ярлык преобразованного файла

Возможно одновременное преобразование сразу нескольких файлов. Для этого их нужно одновременно выделить (с помощью **Ctrl**) и, щелкнув правой кнопкой мыши, выбрать в контекстном меню пункт **DL8.0: Преобразование**. Будущий файл-контейнер будет содержать все выбранные файлы. При этом имя и путь к будущему файлу-контейнеру будет по умолчанию состоять из имени первого из выбранных файлов. Преобразование завершится сообщениями системы с указанием количества файлов.

При преобразовании и последующем обратном преобразовании папки, содержащей не только файлы, но и вложенные папки происходит следующее: если исходная папка содержит пустую подпапку (без файлов), то при преобразовании она удаляется. Соответственно и обратно — преобразованная структура вложенных папок будет отличаться от исходной.

12.2.2 Обратное преобразование объектов ФС

В окне модуля преобразования объекта всегда присутствует кнопка, которая может переключить окно в режим обратного преобразования. Выбрать и открыть файл-контейнер в данном окне можно с помощью кнопки проводника  или двойным нажатием значка преобразованного объекта.

Появится окно, подобное тому, что и при преобразовании, в котором нужно ввести параметры восстановления: папку для восстановления и пароль, а также выбрать предъявленный аппаратный идентификатор.

Отмеченное флагом поле *Зачистить исходные файлы* активирует операцию по удалению исходного файла-контейнера.

В этом же окне будет выведен комментарий к файлу-контейнеру, общее количество файлов и папок, содержащихся в нем, их общий размер, который определила **СЗИ**. Уровень доступа объекта будет тем, который присвоен объекту при преобразовании (только для Dallas Lock 8.0 редакции «С»).

После ввода параметров восстановления и нажатия кнопки «Обратное преобразование» будет произведено восстановление информации. По окончании появится сообщение о подтверждении удаления исходного файла-контейнера и сообщение об удачном завершении процесса (рис. 196).

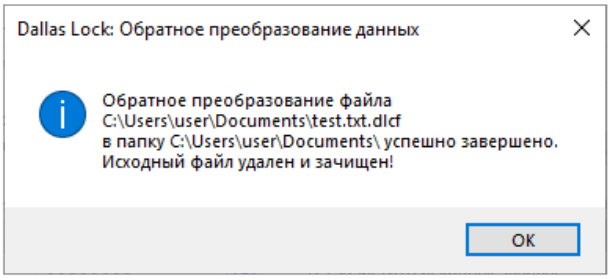


Рис. 196. Подтверждение успешного обратного преобразования файла

Преобразованные файлы-контейнеры, созданные в других версиях **Dallas Lock**, также можно обратно преобразовать в исходные данные, так как формат совместим. При этом необходимо учесть следующее:

Условие	Результат
Преобразованный архив в **Dallas Lock 8.0** редакции «С»	может быть обратно преобразован в **Dallas Lock 8.0** редакции «С», а также в **Dallas Lock 8.0** редакции «К» — но при условии у архива уровня доступа равным нулю («открытые данные») и без мандатной метки
Преобразованный архив в **Dallas Lock 8.0** редакции «К»	может быть обратно преобразован в **Dallas Lock 8.0** редакций «К» и «С»

12.3 Преобразованные файл-диски

Для безопасности хранения и обработки информации в **Dallas Lock 8.0** реализован механизм создания таких контейнеров информации, при работе с размещенными на которых объектами ФС параллельно работе и не заметно для пользователя выполняется преобразование информации. Данные контейнеры называются преобразованные файл-диски.

Особенностью данного механизма является то, что данные файл-диски могут подключаться (монтироваться и демонтироваться) в ОС Windows как логические диски и иметь свою букву диска и определенный объем. В то же время информация на таком диске будет преобразованной и подключение диска для работы с ним пользователем может быть произведено только на ПК, защищенном **Dallas Lock 8.0**, и только с указанием ключевой информации.

12.3.1 Создание преобразованного файл-диска

Создавать преобразованные файл-диски могут пользователи, обладающие следующим правом: разрешающее право **Изменение содержимого** для глобального дескриптора **Параметры преобразованных файл-дисков по умолчанию**.

Для того, чтобы создать преобразованный файл-диск, необходимо в меню значка блокировки ПК на панели задач  выбрать пункт меню **Создать преобразованный файл-диск** (рис. 197).

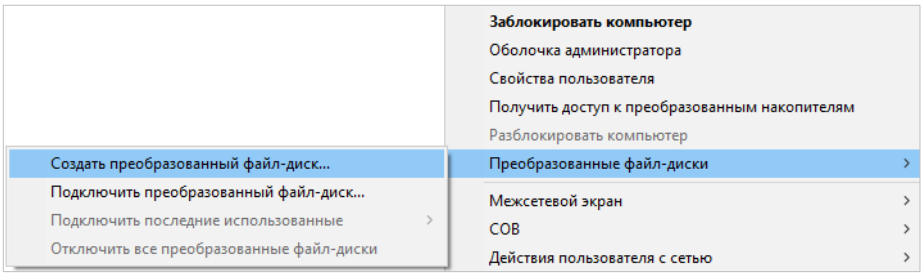


Рис. 197. Выбор пункта меню для создания преобразованного файл-диска

На экране появится окно свойств создаваемого файл-диска, в котором необходимо указать следующие параметры преобразования:

Наименование поля	Описание
Файл-диск	Путь, по которому будет сохранен создаваемый файл-диск и его имя
Название	Описание для создаваемого файл-диска (не обязательное поле)
Размер файл-диска	Необходимо указать оптимальный объем создаваемого файл-диска в МБ (учитывая наличие необходимого места на физическом диске ПК)
Буква диска	Необходимо определить букву логического диска для монтирования в ОС (букву диска можно выбрать и во время подключения файл-диска)
Подключить после создания	Отмеченное поле позволяет автоматически монтировать данный созданный файл-диск в качестве логического дичка в ОС и осуществлять на нем работу текущему пользователю
Алгоритм преобразования	Операции по выбору и настройке алгоритма преобразования, которым будет преобразовываться информация при работе в данном файл-диске. По умолчанию используется встроенный в Dallas Lock 8.0 алгоритм преобразования
Аппаратный идентификатор	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка (также необходимо предварительно зарегистрировать в **СЗИ** считыватели). Если аппаратный идентификатор не указывать, то преобразование будет происходить только по паролю
Пароль и подтверждение пароля	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей, подраздел 4.5.2 Настройка политик авторизации. Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные

После заполнения всех необходимых параметров необходимо нажать **Создать**.

После успешного создания пользователю будет выведено сообщение о том, что создан преобразованный файл-диск и, если было отмечено подключение, подключен как логический диск с указанной буквой диска.

Созданный таким образом файл будет иметь расширение *.dlpfd и иметь определенный значок (рис. 198).

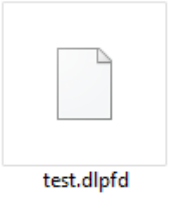


Рис. 198. Значок созданного преобразованного файл-диска

После создания изменить название, размер, алгоритм преобразования и свойства для объекта файл-диск уже невозможно.

12.3.2 Работа на преобразованном файл-диске

Для работы с преобразованным файл-диском необходимо подключить такой диск в ОС и зайти на логический диск, появившийся в проводнике Windows.

Если у пользователя есть разрешение на работу с преобразованными файл-дисками, то ему будет доступен пункт **Преобразованные файл-диски** в меню значка блокировки ПК на панели задач  . Для подключения файл-диска необходимо выбрать данный пункт меню или просто дважды кликнув кнопкой мыши на значке самого файл-диска. Включение также доступно из контекстного меню значка самого файл-диска.

В появившемся диалоговом окне при подключении файл-диска необходимо заполнить ключевую информацию:

- выбрать путь к файл-диску;
- указать букву, под которой он будет монтирован как логический диск в ОС;
- предъявить аппаратный идентификатор, если он был назначен;
- ввести пароль.

После нажатия кнопки **Подключить**, если введенные данные были корректны, файл-диск подключиться и отобразиться в проводнике как логический диск с присвоенной ему буквой диска.

Пользователь может работать с таким диском в штатном режиме, но в то же время вся информация на нем является преобразованной, преобразование же выполняется по установленному алгоритму в процессе самой работы. Пользователь может размещать, создавать, изменять файлы на преобразованном файл-диске, копировать их с него. Для пользователя подключенный файл-диск в своей работе ничем не отличается от любого другого диска.

В меню **Преобразованные файл-диски** значка блокировки на панели задач  также имеется пункт, позволяющий подключить последние использованные файл-диски — в выпадающем списке отображается список из 10 последних файл-дисков.

Чтобы отключить конкретный преобразованный файл-диск или все подключенные на данном ПК необходимо выбрать соответствующие пункты в меню **Преобразованные файл-диски**. Отключение также происходит после выключения или перезагрузки ПК.

Преобразованный файл-диск может быть перемещен на другой защищенный ПК. В этом случае такой диск должен успешно подключаться в ОС, при условии ввода корректной ключевой информации и установке используемого встроенного алгоритма преобразования. В то же время, дескриптор (права доступа и аудит), назначенный на преобразованный файл-диск, при его перемещении не сохранится.

12.3.3 Доступ к преобразованным файл-дискам

Кроме того, с помощью параметров безопасности можно определить, какие пользователи могут работать с преобразованными файл-дисками и с какими правами, а какие нет. Для этого используется настройка глобальных дескрипторов: **Параметры ФС по умолчанию**, **Параметры преобразованных файл-дисков по умолчанию** и настройка дескриптора объекта.

Настройка доступа и ведения аудита событий осуществляются в соответствии с описанием в разделах 5.2.3 Дискреционный доступ для глобальных параметров и 6.2.1 Аудит для глобальных параметров.

Если дескриптор **Параметры преобразованных файл-дисков по умолчанию** не настроен, то настройки такого дескриптора будут наследоваться от глобального дескриптора **Параметры по умолчанию**.

При настройке прав доступа необходимо учесть следующее:

- Для создания файл-дисков и работы с ним необходимо, чтобы пользователь имел разрешающее право **Изменение содержимого**.
- Для просмотра содержимого преобразованных файл-дисков необходимо, чтобы пользователь имел разрешающее право **Обзор папки**.
- Для запуска приложения необходимо, чтобы пользователь имел разрешающее право **Выполнение вложенных объектов**.

На расположенные в преобразованном файл-диске объекты ФС (файлы, папки) назначить дескриптор безопасности нельзя.

Операции по работе с преобразованными файл-дисками и настройкой прав доступа на управление преобразованными файл-дисками фиксируются в журналах аудита **СЗИ**.

13 СИСТЕМА КОНТРОЛЯ НАКОПИТЕЛЕЙ

В **Dallas Lock 8.0** в формате двух отдельных модулей реализована **СКН**, которые предназначены для контроля подключения съемных машинных носителей информации и контроля отчуждения (переноса) информации со съемных машинных носителей информации.

Модуль **СКН** уровня контроля подключения съемных машинных носителей информации в составе **Dallas Lock 8.0** позволяет разграничивать доступ пользователей информационной системы к съемным 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 **Dallas Lock 8.0** — совместное решение компаний **Конфидент** и **Актив-софт**, сертифицированное ФСТЭК России на соответствие требованиям к **СКН**[14].

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 съемные накопители не могут быть использованы. Дополнительно на каждый накопитель возможно установить пароль пользователя.

Единый центр управления 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.

13.1 Права доступа к съемным накопителям

Чтобы назначить права доступа к конкретному накопителю, необходимо подключить этот накопитель к соответствующему порту ПК (если это USB-Flash накопитель) или вставить его в привод CD-ROM (в случае компакт-диска). Далее необходимо найти объект, соответствующий накопителю, с помощью проводника Windows Explorer и в контекстном меню объекта выбрать пункт **DL8.0: Права доступа** или выбрать объект в дереве устройств на вкладке *Контроль устройств*. Дальнейшая настройка прав доступа ничем не отличается от настройки доступа к объектам ФС глава 5 Разграничение доступа к объектам ФС.

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



Реализована возможность назначения мандатных уровней на съемный накопитель для отдельных пользователей или групп пользователей.

При этом в список контролируемых объектов эти накопители занесутся без указания буквы диска, а в специальном формате, в который входит тип накопителя и его уникальный номер («Flash(XXXX-XXXX- XXXXXXXXXXXXXXXXXXX):\»).

Для USB-Flash накопителей номер высчитывается как: идентификатор производителя (VendorID), идентификатор продукта (ProductID) и серийный номер (Serial Number).



Для преобразованных съемных накопителей, раздел 13.3 Преобразование съемных накопителей, и дескрипторов объектов ФС на съемных накопителях, глава 5 Разграничение доступа к объектам ФС, уникальный номер накопителя дополнительно содержит серийный номер тома.

Для дискеты и компакт-диска уникальный номер накопителя содержит серийный номер тома («FDD(0000-0000- XXXXXXXX):\», «CD(0000-0000- XXXXXXXX):\»).

Поэтому, если при следующем подключении ОС назначит накопителю другую букву диска, права все равно будут контролироваться.

[14] Методический документ «Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты ИТ.СКН.Н4.ПЗ» (ФСТЭК России, 2014).

В окне категории **Съемные накопители** (**СКН → Съемные накопители**) контроля ресурсов формируется список всех установленных дескрипторов на съемные накопители, в том числе права доступа (дискреционный и мандатный доступ), назначенный аудит и установленный контроль целостности (рис. 199).

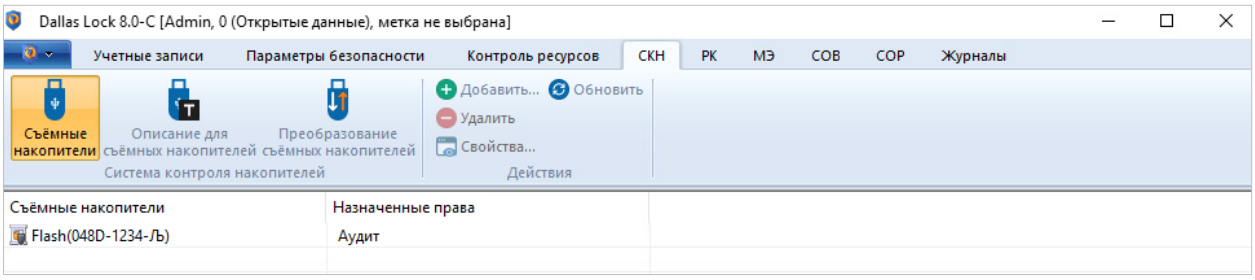


Рис. 199. Окно дескрипторов съемных накопителей

Действие **Добавить…**, доступное в категории «Съемные накопители», позволит открыть проводник для выбора ресурса именно на съемных накопителях, установленных в ОС.

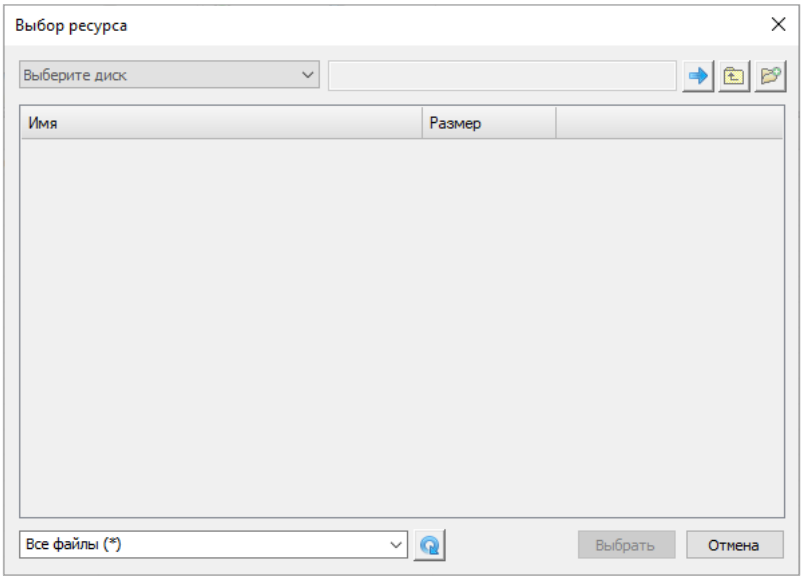


Рис. 200. Добавление съемного накопителя

После выбора необходимого накопителя появится окно **Безопасность** для настройки доступа к накопителю.

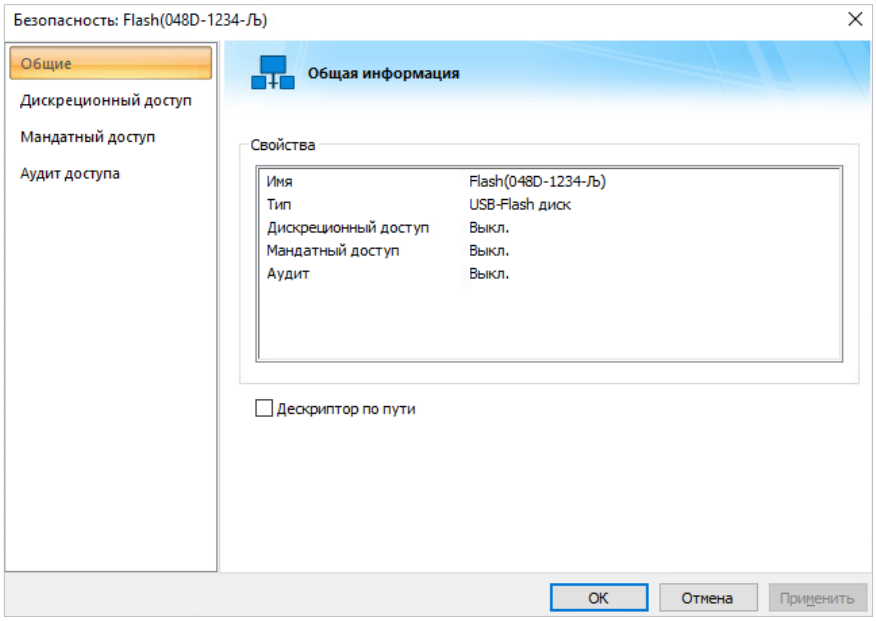


Рис. 201. Настройка безопасности для съемного накопителя

Существует возможность разграничить глобальный доступ к съемным накопителям или преобразованным съемным накопителям. Список глобальных параметров расположен на вкладке **Контроль ресурсов → Глобальные**.

Если определенному пользователю в глобальном параметре **Параметры открытых съемных дисков по умолчанию** запретить все действия, то этот пользователь не сможет работать ни с одним открытым съемным накопителем. Если в глобальном параметре **Параметры открытых съемных накопителей по умолчанию** запретить все действия для группы «*Все*», в этом случае с открытыми съемными накопителями не сможет работать ни один из пользователей (за исключением пользователя, установившего **СЗИ**, суперадминистратора).

Если же после этого необходимо разрешить пользователю работу с преобразованными съемными накопителями, нужно в глобальных параметрах **Параметры преобразованных съемных накопителей по умолчанию** разрешить пользователю все операции. В результате этот пользователь не сможет работать с открытыми съемными накопителями, но будет иметь полный доступ к преобразованным съемным накопителям.

13.2 Описание для съемных накопителей

Для упрощения контроля большого количества съемных накопителей в **Dallas Lock 8.0** имеется возможность задавать свое описание для отдельно взятого съемного накопителя. Описание съемного накопителя позволяет заменить установленным названием серийный номер для работы с накопителем в **СЗИ**.

Для того, чтобы назначить описание для съемного накопителя, необходимо предъявить накопитель на ПК, в оболочке администратора на вкладке **СКН** выделить категорию **Описание для съемных накопителей** и нажать **Добавить** на панели действий.

В появившемся окне выбрать накопитель из выпадающего списка и ввести описание для накопителя (рис. 202). В выпадающем списке будут отображаться только те накопители, для которых описание еще не назначено. Чтобы изменить уже установленное описание, необходимо выделить объект в списке основного окна и нажать **Свойства**, либо вызвать окно редактирования описания двойным кликом мыши по объекту.

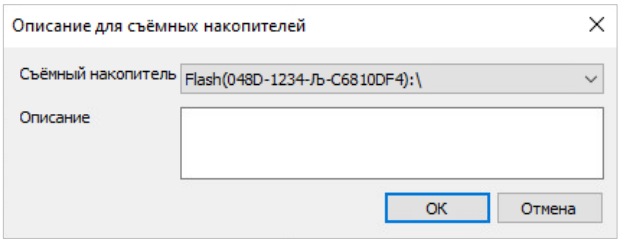


Рис. 202. Окно описания съемных накопителей

После этого при назначении прав доступа, контроля целостности или аудита для объектов ФС на данном накопителе в оболочке администратора в списках с дескрипторами накопитель будет отображаться под установленным описанием (рис. 203).

При просмотре устройств на вкладке *Контроль ресурсов* текст наименования добавленного съемного накопителя изменится на его описание.

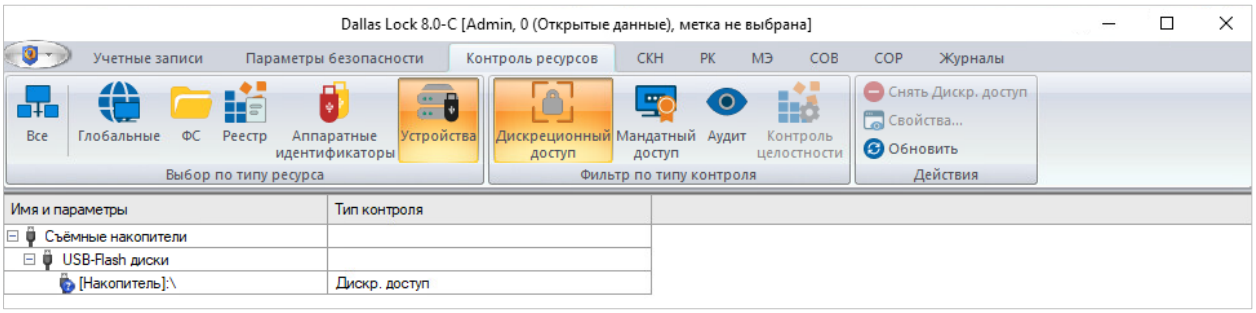


Рис. 203. Отображение съемных накопителей

13.3 Преобразование съемных накопителей

В системе защиты **Dallas Lock 8.0** реализована возможность преобразования съемных накопителей. Преобразование съемных накопителей может быть использовано, например, при передаче секретных документов между автономными рабочими станциями.

Данная функция представляет собой создание с помощью ключа преобразования такого

накопителя, с информацией на котором работа возможна строго на рабочих станциях, защищенных **Dallas Lock 8.0**, при условии наличия и совпадения ключа преобразования.

Понятие «преобразование съемных накопителей» подразумевает, что данный накопитель при подключении его к ПК будет отмечен в **СЗИ** таким образом, что вся информация на нем при ее обработке (создании и изменении файлов) будет автоматически преобразована.

Преобразование съемных накопителей доступно только для тех устройств, которые распознаются ОС как сменный/съемный (removable) (USB-Flash накопители, карты памяти, Floppy-диски и прочие). Жесткие диски, подключаемые через устройство Mobile Rack или USB-порт, физически являются съемными, но логически для ОС являются фиксированными. На такие диски данная функция не распространяется.

В отличие от функции прозрачного преобразования фиксированных дисков, раздел 12.1 Прозрачное преобразование дисков, в которой возможен выбор областей и размера преобразовываемой области диска, преобразование съемных накопителей происходит только полностью.

Преобразование съемных накопителей осуществляется через оболочку администратора: вкладка *СКН* → категория **Преобразование съемных накопителей** (рис. 204).

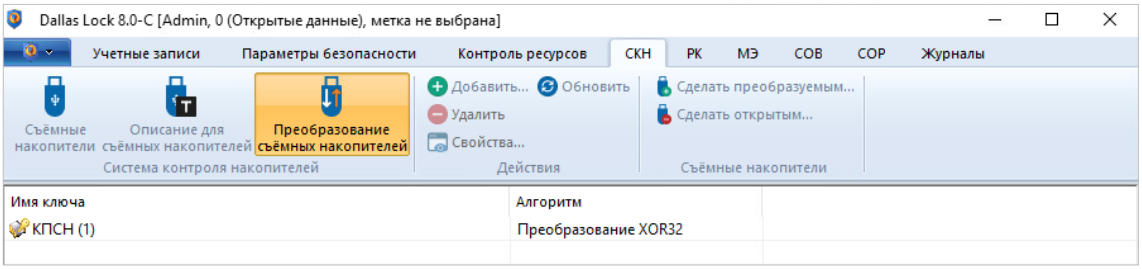


Рис. 204. Преобразование съемных накопителей

Создавать ключи преобразования, выполнять преобразование съемных накопителей могут только пользователи с правом **Параметры безопасности: Управление**, подраздел 3.6.3 Полномочия на управление параметрами безопасности.

13.3.1 Создание ключей преобразования

Для создания преобразованных съемных накопителей необходимо наличие ключа преобразования. Чтобы создать ключ преобразования, необходимо нажать **Добавить** на панели действий. Появится окно ввода параметров ключа преобразования:

Наименование поля	Описание
Имя ключа	Имя ключа предлагается по умолчанию «КПСН» — ключ преобразования съемных накопителей. Его можно изменить. Имя ключа должно быть уникальным, создание двух ключей с одинаковыми именами невозможно
Ключ отключен	Определяет активность ключа преобразования
Доступ к накопителю по паролю	Определяет необходимость предоставления пароля для доступа к накопителю. Функциональная возможность доступна в случае приобретения лицензии на модуль «Средство контроля подключения съемных машинных носителей информации»
Алгоритм	Алгоритм преобразования
Идентификатор	Для назначения аппаратного идентификатора необходимо идентификатор предъявить и выбрать из списка (предварительно зарегистрировав в СЗИ считыватели идентификатора, как и для любого другого действия с идентификаторами, раздел 4.3.2 Настройка считывателей аппаратных идентификаторов. Если аппаратный идентификатор не указывать, то преобразование происходит только по паролю
Пароль ключа и подтверждение	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей 4.5.3 Настройка политик паролей. Дополнительно можно воспользоваться кнопкой, меняющей скрытые символы на явные

После заполнения полей необходимо нажать **ОК**. Созданный ключ преобразования появится в списке.

С помощью кнопок на панели **Действия с ключами преобразования** можно удалить, изменить параметры выбранного ключа и обновить весь список.

Операции по управлению списком ключей преобразования съемных накопителей фиксируются в журнале управления политиками.

13.3.2 Процесс преобразования накопителя

> В процессе преобразования накопителя вся информация, расположенная на нем, будет утрачена, так как накопитель будет отформатирован.

Для преобразования съемного накопителя необходимо:

1. Вставить накопитель в разъем.
2. Выбрать на панели действий со съемными накопителями **Сделать преобразуемым**. Откроется окно параметров для преобразования (рис. 205).

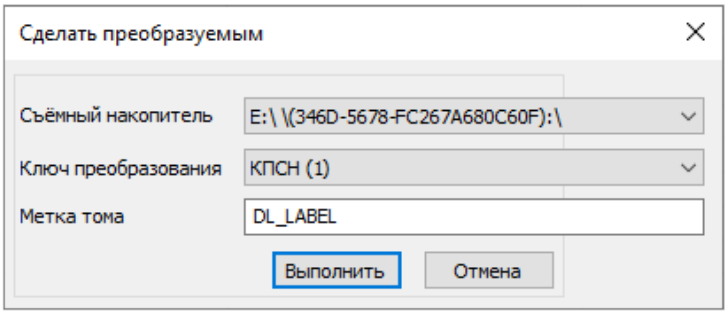


Рис. 205. Параметры для преобразования информации на выбранном диске

3. В появившемся окне параметров преобразования:
   - выбрать букву диска *съемного накопителя*, определенную ОС (если буква не определена, нужно перезапустить окно);
   - выбрать *ключ преобразования* из списка созданных;
   - ввести *метку тома* — произвольное имя будущего преобразованного накопителя.
4. Нажать **Выполнить**. Далее запускается процесс форматирования диска, по окончании которого появится сообщение об успешности включения режима преобразования для диска E (рис. 206).

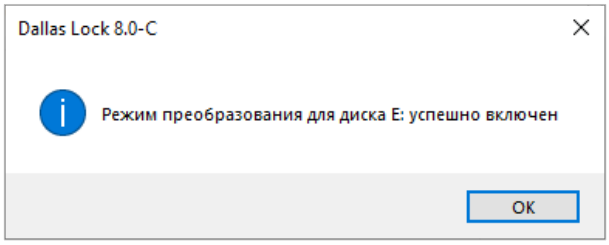


Рис. 206. Сообщение об успешном преобразовании накопителя

Операции по преобразованию съемных накопителей фиксируются в журнале управления политиками.

> Преобразование уже использованного в качестве аппаратного идентификатора для ключа преобразования USB-Flash накопителя не допускается.

13.3.3 Доступ к преобразованным накопителям

После того, как съемный накопитель преобразован, работать с ним можно только на тех компьютерах, которые защищены **Dallas Lock 8.0**, и на которых установлен ключ преобразования, аналогичный тому, которым преобразование было выполнено (должен совпадать пароль ключа, предъявленный идентификатор и алгоритм преобразования). При невыполнении этих условий доступ к накопителю будет заблокирован, и появится сообщение о том, что работа с данным накопителем возможна только после его форматирования в ОС (рис. 207).

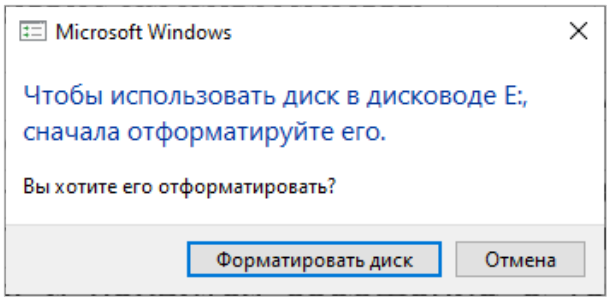


Рис. 207. Блокировка съемного носителя

Для настройки доступа к съемному накопителю по паролю, нужно поставить флаг в соответствующем поле при создании ключей преобразования.

Чтобы получить доступ к преобразованному съемному накопителю с установленным паролем, необходимо подключить данный накопитель к компьютеру. После подключения на экране появляется всплывающее уведомление (рис. 208) и окно для ввода пароля ключа преобразования (рис. 209).

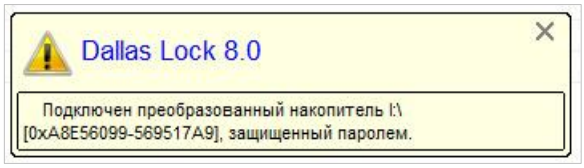


Рис. 208. Получение доступа к преобразованным съемным носителям

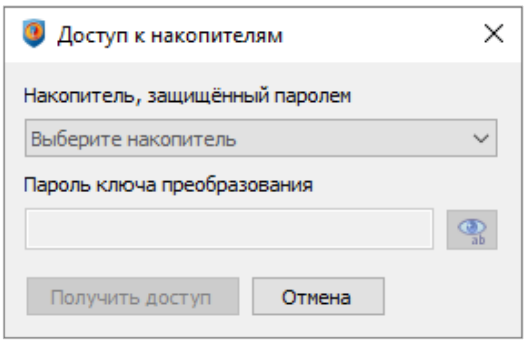


Рис. 209. Пароль ключа преобразования для доступа к преобразованным съемным накопителям

Для открытия окна **Доступ к накопителям** нужно нажать правой кнопкой мыши на панели задач на значок  и из появившегося списка выбрать пункт **Получить доступ к преобразованным накопителям** (рис. 210).

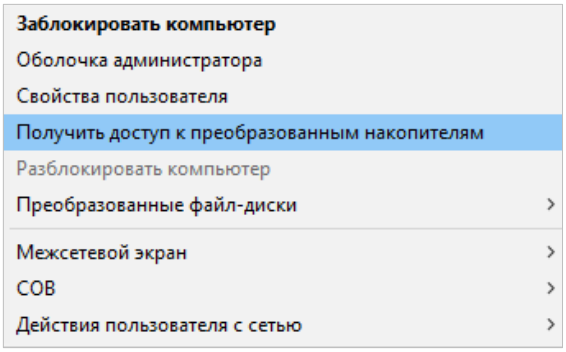


Рис. 210. Получение доступа к преобразованным съемным носителям

В результате на экране должно отобразиться окно, в котором можно выбрать накопитель, к которому необходимо получить доступ, и ввести пароль ключа преобразования для него (рис. 211).

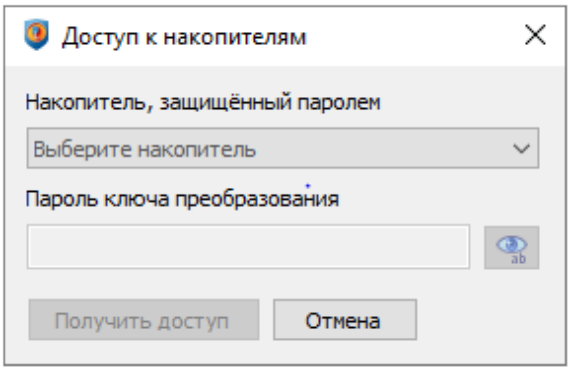


Рис. 211. Получение доступа к преобразованным съемным носителям

При попытке открытия преобразованного съемного накопителя из проводника, возникает сообщение об отказе доступа (рис. 212).

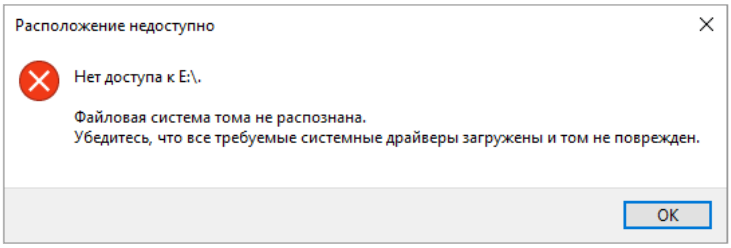


Рис. 212. Отказ доступа

При вводе неверного пароля на экране появляется сообщение об ошибке (рис. 213).

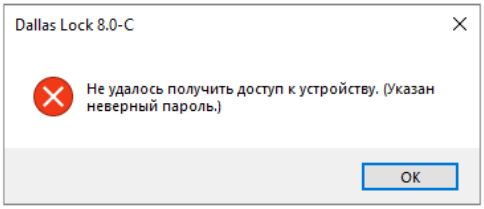


Рис. 213. Попытка доступа к устройству с неверным паролем

При превышении допустимого количества неуспешных попыток аутентификации доступ к защищаемому устройству для данного пользователя блокируется. На экране появляется соответствующее сообщение (рис. 214), в **Журнале входов** регистрируются соответствующие события.

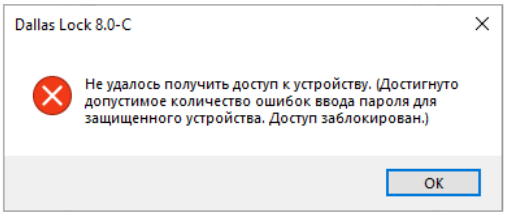


Рис. 214. Блокировка доступа к устройству

Восстановление информации после блокировки доступа к преобразованному съемному накопителю осуществляется администратором **СЗИ**.

Количество попыток ввода пароля для получения доступа к преобразованному накопителю попадает под действие парольной политики **СЗИ**. Управление политикой осуществляется путем изменения параметра **Максимальное количество ошибок ввода пароля** категории **Политики авторизации** вкладки *Параметры безопасности*.

Для снятия блокировки доступа к защищенным накопителям для пользователя, администратору необходимо выполнить следующую последовательность действий: открыть в панели администрирования **Учетные записи** → **Заблокированные пользователи** → выделить соответствующее поле в таблице → на панели **Действия** нажать кнопку **Разблокировать** (рис. 215).

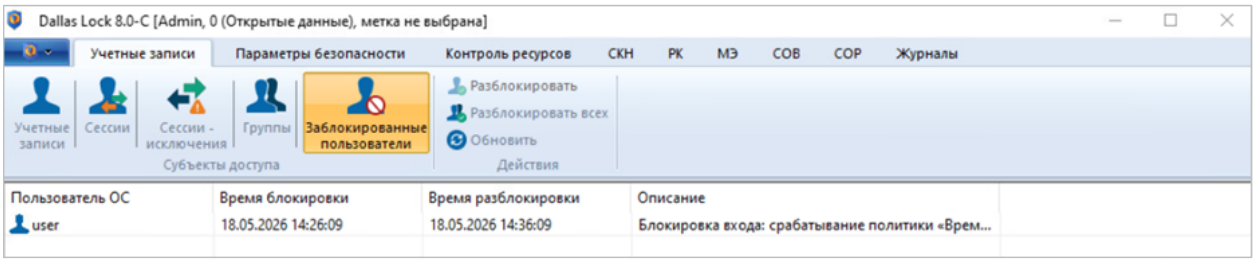


Рис. 215. Разблокировка доступа к защищенному устройству

При указании верного пароля для устройства пользователю предоставляется доступ. На экране появляется соответствующее сообщение (рис. 216).

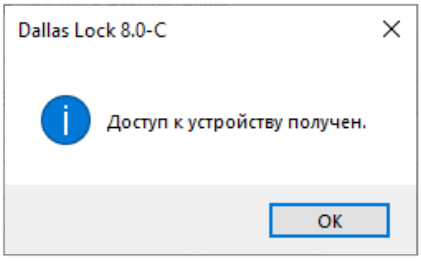


Рис. 216. Доступ к устройству

Кроме того, с помощью параметров безопасности можно определить, какие пользователи могут работать с преобразованными накопителями и с какими правами, а какие нет. Для этого используется настройка глобальных дескрипторов и настройка дескриптора данного накопителя.

Настройку глобальных дескрипторов дискреционного доступа и аудита для преобразованных съемных накопителей можно выполнить в оболочке администратора на вкладке *Контроль ресурсов* → **Глобальные**. В списке имеются следующие параметры для настройки преобразованных накопителей:

- Параметры преобразованных съемных накопителей по умолчанию.
- Параметры преобразованных FDD-дисков по умолчанию.
- Параметры преобразованных USB-Flash накопителей по умолчанию.
- Параметры преобразованных файл-дисков по умолчанию.

Настройка доступа и ведения аудита событий осуществляются в соответствии с описанием в разделах 5.2.3 Дискреционный доступ для глобальных параметров и 6.2.1 Аудит для глобальных параметров.

Настроить параметры доступа и аудита для индивидуального устройства можно через окно дескриптора, вызвав его из контекстного меню объекта в проводнике Windows. Объекты, для которых назначен дескриптор любым из способов, автоматически появляются в списке объектов выбранной категории **Дискреционный доступ** и **Аудит** на вкладке *Контроль ресурсов*.

Также можно настроить доступ к преобразованному накопителю на вкладке *Контроль ресурсов* → **Устройства**, выбрав класс устройств или само устройство в дереве объектов, раздел 10.2 Разграничение доступа к устройствам.

В окне свойств доступа устройства или класса устройств также можно назначить теневое копирование информации с преобразованного накопителя, раздел 6.4 Теневое копирование.

Создавать преобразованные файл-диски могут пользователи, обладающие следующим правом: разрешающее право **Изменение содержимого** для глобального дескриптора **Параметры преобразованных файл-дисков по умолчанию**.

13.3.4 Обратное преобразование

Процесс обратного преобразования представляет собой форматирование выбранного съемного накопителя и затирание всей остаточной информации. После этого накопитель будет доступен для работы на любом ПК без ограничений и требований форматирования.

Чтобы запустить данный процесс, необходимо выбрать действие **Сделать открытым**. В появившемся окне параметров выбрать букву диска накопителя из списка и ввести в поле «Метка тома» наименование, которое будет у носителя после форматирования.

14 РЕЗЕРВНОЕ КОПИРОВАНИЕ

14.1 Назначение и общие принципы работы

Модуль резервного копирования позволяет восстанавливать безвозвратно модифицированные или удаленные файлы и каталоги (с поддержкой вложенных файлов). Управление резервным копированием может осуществляться локально с помощью оболочки администратора.

Данный модуль доступен при наличии лицензии, в состав которой включен модуль **Резервное копирование.**

В ходе настройки механизмов резервного копирования создаются задания на резервное копирование, которые определяют периодичность создания резервных копий объектов ФС, их количество, длительность и место хранения. Созданные задания на резервное копирование выполняются в фоновом режиме.

Одновременно может выполняться не более 5 заданий (без возможности редактирования), запуск 6-го возможен только принудительно администратором.

Резервные копии объектов ФС создаются в виде zip-архивов, наименования которых автоматически задается по следующей схеме: «*Имя клиента*_*Имя задания*_ДД.ММ.ГГГГ_ЧЧ.ММ.СС».

14.2 Эксплуатация

Полномочия на управление резервным копированием устанавливаются в разделе **Права пользователей** на вкладке *Параметры безопасности* следующими параметрами:

- **Резервное копирование: Просмотр**;
- **Резервное копирование: Управление**.

В случае, если резервные копии хранятся на сетевом хранилище, учетной записи пользователя, которая будет использоваться для запуска заданий по резервному копированию, должен быть обеспечен доступ к этому хранилищу.

Управление заданиями на резервное копирование осуществляется в оболочке администратора на вкладке «РК».

Функции создания, копирования, удаления, активации и деактивации заданий недоступны в случае, если клиентский компьютер введен в домен безопасности.

Для осуществления резервного копирования должен быть открыт TCP/IP порт 17903.

Для создания нового задания на резервное копирование необходимо:

1. Нажать кнопку **Создать** в панели действий категории **Задания** либо в контекстном меню, вызываемом щелчком правой кнопки мыши в рабочей области (рис. 217).

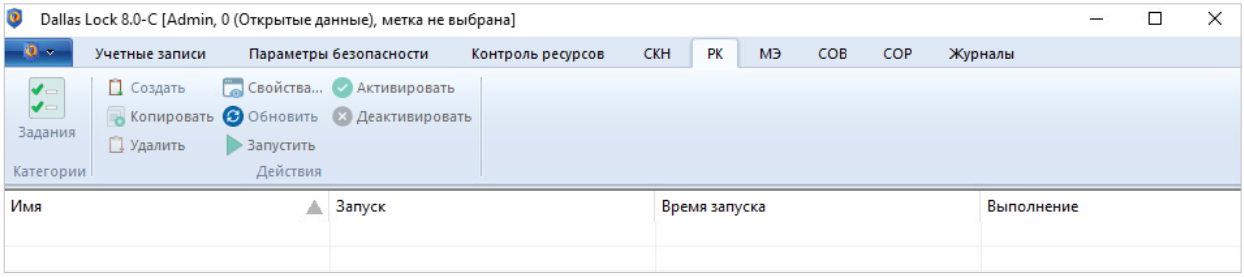


Рис. 217. Создание задания на резервное копирование

2. В появившемся окне мастера создания заданий на вкладке *Параметры* задать параметры резервного копирования (рис. 218).

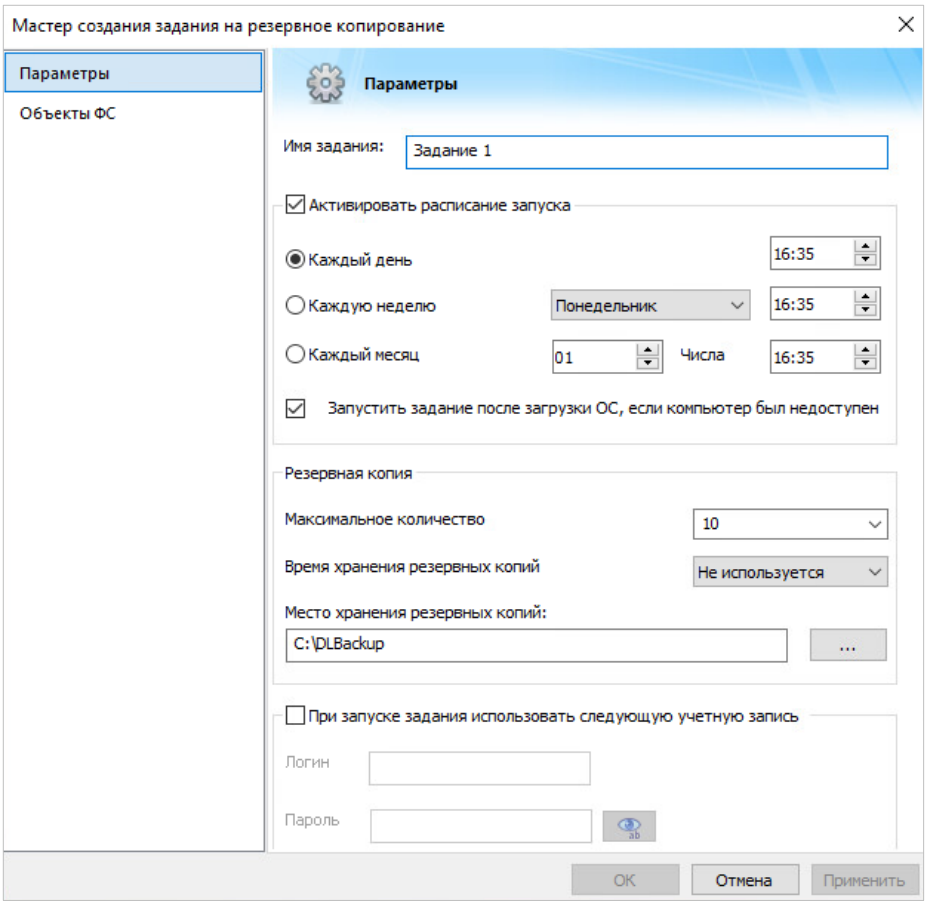


Рис. 218. Мастер создания задания на резервное копирование

В поле *Имя задания* вводится наименование, которое будет отображаться в списке заданий.

Для настройки периодичности резервного копирования необходимо установить флаг в поле *Активировать расписание запуска*. Далее необходимо выбрать периодичность и указать время проведения резервного копирования в соответствующем поле (вручную с клавиатуры, либо используя стрелочки).

При необходимости установить флаг в поле *Запустить задание после загрузки ОС, если компьютер будет недоступен*.

Настройка параметров резервной копии:

- *Максимальное количество* — значение данного параметра определяет максимальное количество сохраняемых резервных копий объекта ФС. При превышении заданного значения происходит удаление старых копий и создаются новые.
- *Время хранения резервных копий* — данный параметр устанавливает максимальный срок хранения копий. По истечению заданного времени с момента создания копии, данная копия удаляется.
- *Место хранения резервной копии* — данный параметр предоставляет возможность выбора директории, которая послужит хранилищем для создаваемой резервной копии. По умолчанию задан путь «C:\DLBackup».

Задания по резервному копированию по умолчанию выполняются из-под системной учетной записи. Чтобы это изменить, необходимо установить флаг в поле *При запуске задания использовать следующую учетную запись* и ввести данные учетной записи, из-под которой необходимо выполнять задания.

Учетная запись пользователя должна быть зарегистрирована на клиенте, на котором будет выполняться данное задание. В противном случае произойдет ошибка архивирования.

Для учетной записи, которая используется для запуска заданий, должен быть обеспечен доступ к сетевому хранилищу.

После нажатия кнопок **Применить** или **Ок** будет выполнена проверка используемой учетной записи и возможность доступа к указанному месту хранения резервных копий. Если после проверки указанная учетная запись не имеет доступа к указанному месту хранения, будет выведено предупреждение: «*Учетная запись не имеет доступа к указанному месту хранения резервных копий. В случае отсутствия доступа резервная копия не будет сохранена. Вы хотите продолжить?*»

3. Перейти на вкладку *Объекты ФС* и добавить объекты ФС, для которых необходимо создавать резервные копии, указав к ним путь в окне выбора ресурса (рис. 219).

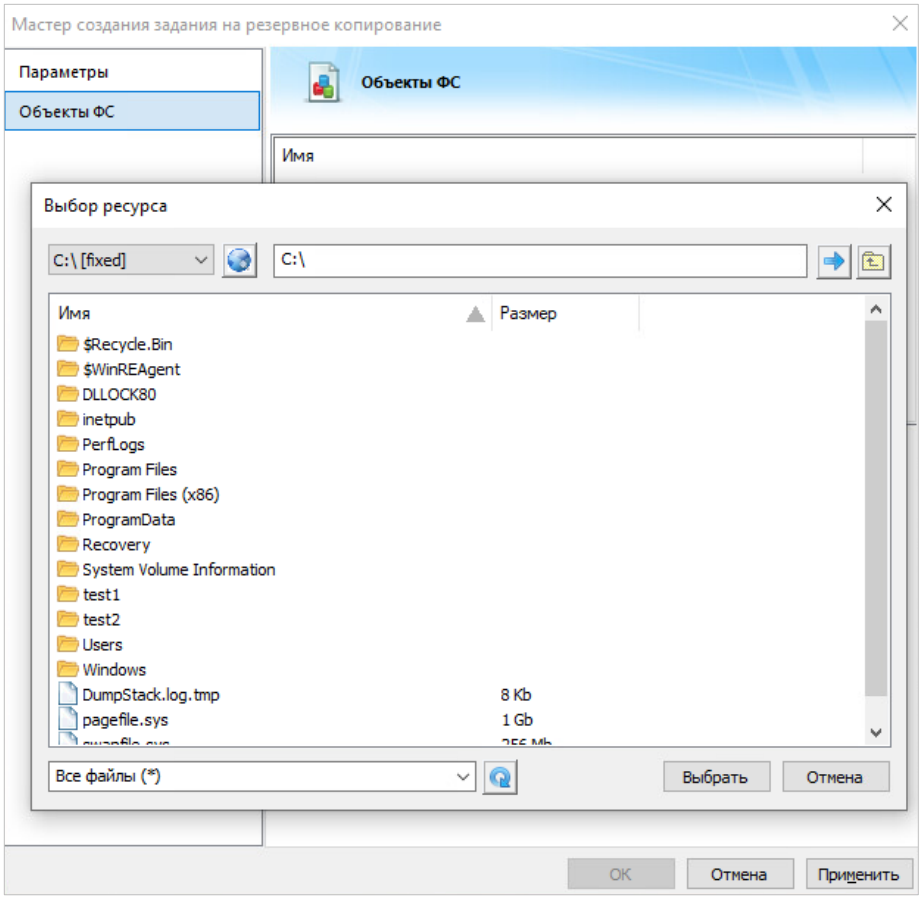


Рис. 219. Выбор объекта ФС для резервного копирования

Для резервного копирования невозможно выбрать файловый объект, которому назначен дескриптор.

Установить флаг в поле *Создать резервную копию, если часть объектов ФС не найдена* — в таком случае, резервная копия будет создаваться для всех обнаруженных объектов ФС, которые определены для резервного копирования. Если часть объектов окажется недоступна, в графе *Выполнение* в рабочей области будет отображен статус процесса *Архивирование выполнено частично*.

В случае, если не обнаруживается ни одного из выбранных объектов ФС, процедура завершится ошибкой, а в графе *Выполнение* будет отображен статус процесса *Ошибка архивирования*.

Для резервного копирования сетевого ресурса необходимо установить флаг в поле *При доступе к сетевым ресурсам использовать следующую учетную запись* и ввести данные учетной записи для доступа к этому сетевому ресурсу.

Для создания копии выбранного задания необходимо нажать кнопку **Копировать**, откроется окно **Мастер создания задания** с уже установленными параметрами для копирования задания, в поле *Имя задания* имя автоматически меняется на *Имя копируемого задания-копия*. В окно можно внести изменения и нажать **ОК** после чего будет создано новое задание.

Чтобы удалить задание, необходимо нажать кнопку **Удалить** в панели **Действия** либо в контекстном меню задания. При этом будут удалены все резервные копии, созданные этим заданием, о чем предупредит соответствующее диалоговое окно (рис. 220).

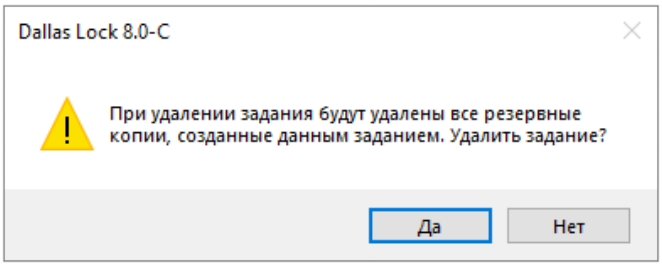


Рис. 220. Окно подтверждения удаления задания

Для просмотра параметров задания необходимо нажать на кнопку **Свойства…** в панели **Действия**, откроется окно **Свойство задания**, в котором можно изменить параметры выбранного задания и нажать кнопку **Применить** для сохранения измененных параметров.

Для просмотра созданных резервных копий и восстановления объектов ФС необходимо открыть свойства здания и в открывшемся окне перейти на вкладку *Резервные копии* (рис. 221). Для восстановления объектов ФС необходимо выбрать соответствующую резервную копию и нажать кнопку **Восстановить**.

Во время выполнения задания восстановление данных из резервной копии невозможно. В этом случае появится соответствующее информационное сообщение.

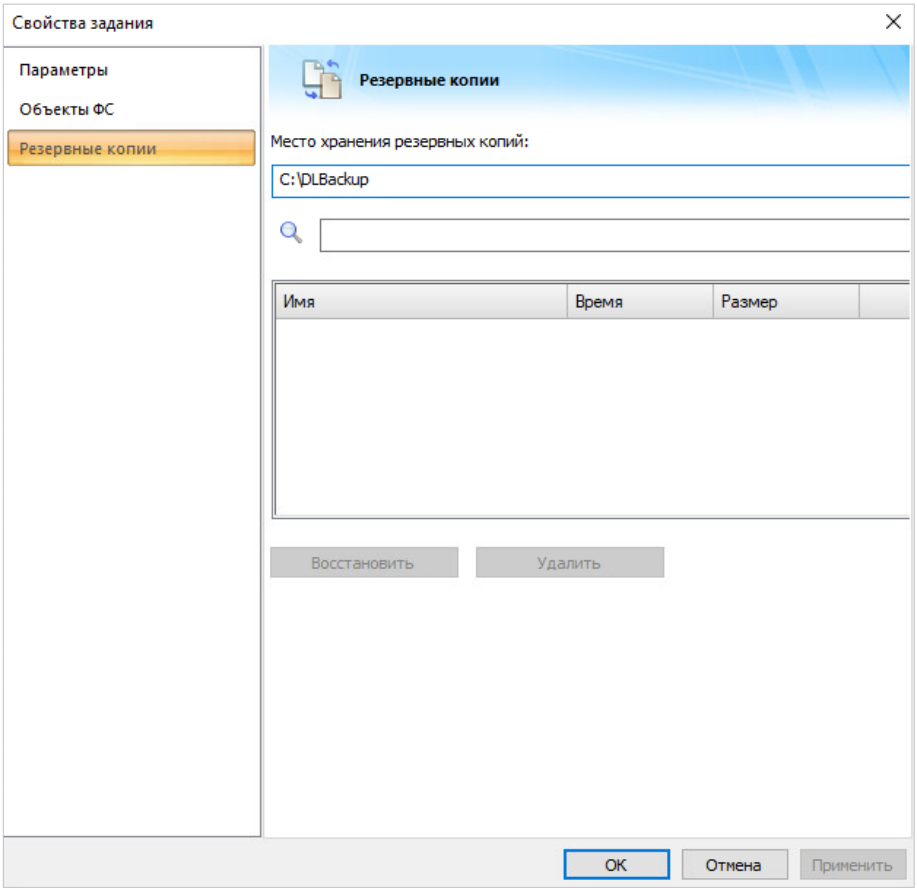


Рис. 221. Окно просмотра свойств задания

По завершению процедуры восстановления в графе *Выполнение* задания установится статус *Восстановление прошло успешно*.

Процедура восстановления реализована таким образом, что первоначально происходит очистка восстанавливаемых целевых объектов ФС. В случае, когда возникает ошибка при очистке каталога перед восстановлением, в журнале будет зафиксирована соответствующая запись с типом операции *Очистка каталога для восстановления*.

Для обновления списка и статуса заданий необходимо нажать кнопку **Обновить**.

Созданные задания запускаются с установленной периодичностью, однако, если необходимо запустить резервирование до запланированного времени, следует нажать кнопку **Запустить**.

Если параметры задания заданы, но напротив задания имеется значок  , то это означает, что задание по резервированию не выполняется. Чтобы активировать неактивное задание, необходимо нажать кнопку **Активировать**. При этом, если нет необходимости в периодическом выполнении задания, его можно запустить один раз, воспользовавшись кнопкой **Запустить**. Для прекращения выполнения активного задания необходимо выбрать его в списке заданий и нажать кнопку **Деактивировать**.

15 МЕЖСЕТЕВОЙ ЭКРАН

15.1 Назначение и общие принципы работы

Межсетевой экран (**МЭ**) является модулем **Dallas Lock 8.0** и предназначен для защиты рабочих станций и серверов от **НСД** посредством осуществления контроля и фильтрации, проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.

Для работы **МЭ** не требуется внесение изменений в структуру существующей сети.

15.1.1 Возможности межсетевого экрана

Установка, удаление, активация и деактивация межсетевого экрана описаны в главе 2 Установка и удаление системы защиты.

Модуль **МЭ** осуществляет защиту как физических, так и виртуальных машин и поддерживает работу со всеми основными сетевыми протоколами.

Задавать ограничения можно по работе служебных и прикладных протоколов, сетевых интерфейсов, портов и т. д. А также распределять уровни доступа среди пользователей, компьютеров, групп пользователей. Функции **МЭ** осуществляются посредством контроля и фильтрации сетевых пакетов в соответствии с набором таких параметров, как параметры сетевых протоколов, сегментов сети, исключения, учетные записи пользователей, сетевые интерфейсы и приложения.

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

Реализована возможность выполнить настройку правил **МЭ** для пользователей, работающих под различными уровнями доступа.

Работа **МЭ** осуществляется посредством:

- фильтрации сетевого трафика,
- работы правил исключения,
- разделения сетей на доверенные и не доверенные согласно сегментам сети,
- 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.

Сбор информации о работе сети ведется на всех компьютерах системы, на которых установлен **МЭ Dallas Lock 8.0.**

Модули **СОВ** и **МЭ** позволяют обнаруживать атаки внутри виртуальной сети VipNet.

15.2 Эксплуатация

Управление настройками межсетевого экрана доступно пользователям, которым назначена возможность изменения настроек **МЭ** — администраторам ЗАРМ **Dallas Lock** (по умолчанию членам группы *Администраторы*), и происходит из оболочки администратора во вкладке *Межсетевой экран*.

Для просмотра и изменения политик и других параметров **МЭ** пользователь должен быть указан в значении параметров **Межсетевой экран: Изменение настроек** и **Межсетевой экран: Просмотр настроек** категории **Права пользователей** либо состоять в группе, указанной в данном параметре.

15.2.1 Адреса

В данной категории отображается список локальных адресов компьютера, посредством которых к нему можно обратиться (рис. 222).

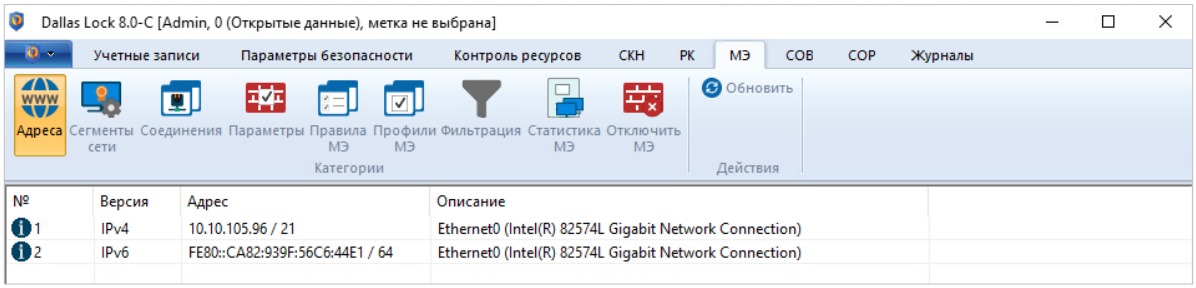


Рис. 222. Список адресов

15.2.2 Сегменты сети

Механизм **Сегменты сети** позволяет применять правила **МЭ** и фильтрации не безусловно, а в зависимости от параметров сети, через которую получен сетевой пакет. Доступно семь возможных сетевых сегментов сети, определяемых по адресам и используемым сетевым адаптерам. В случае, если для сетевого пакета не подходит ни один из активных сегментов сети — пакет будет считаться принадлежащем к сети, определенной сегментом сети *По умолчанию*. Для редактирования сегмента сети нужно выбрать его на информационной панели и нажать кнопку **Свойства** на панели **Действия**. Появится окно **Свойства сегмента сети**, в котором возможно задать IP-адрес или подсеть, выбрать сетевой интерфейс и ввести название сегмента сети (рис. 223).

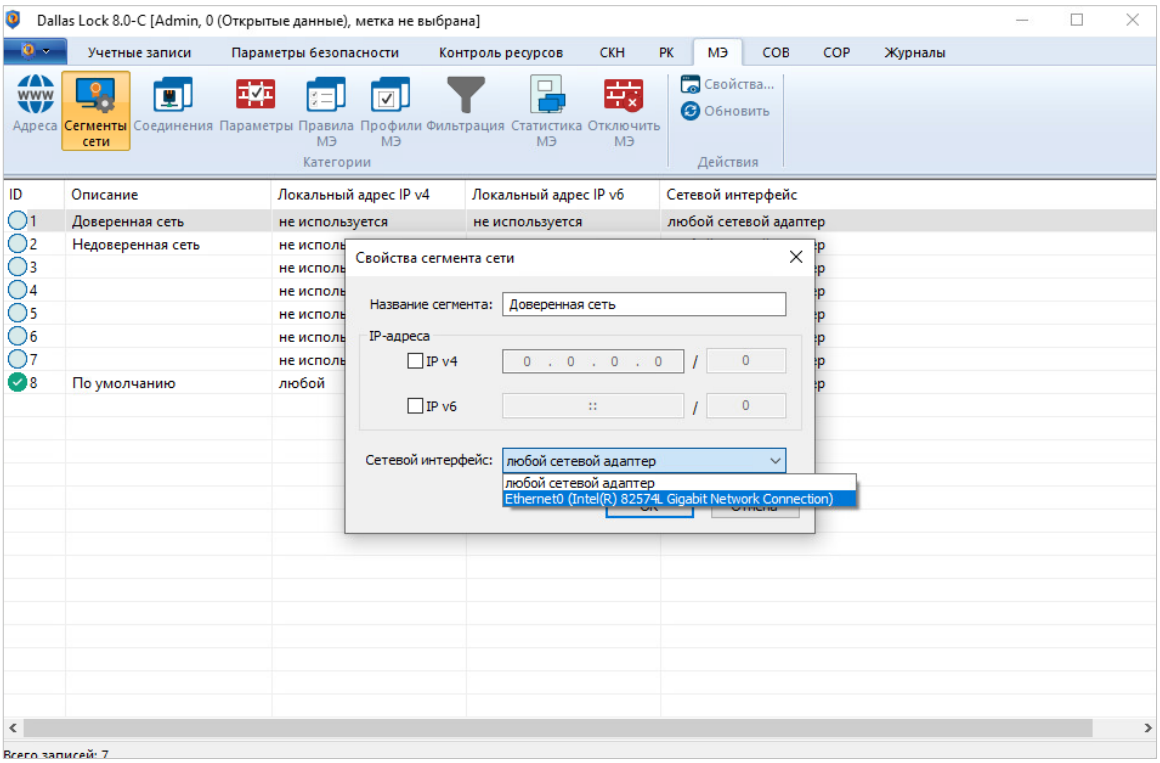


Рис. 223. Свойства сегмента сети

Пример 1

Администратор хочет разрешить использование сети Интернет только из доверенной (корпоративной) сети.

1. Администратор задал подсеть компании и сетевой адаптер для сегмента сети «Доверенная сеть».
2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сегмент сети *Доверенная сеть*, подраздел 15.2.5 Правила МЭ (рис. 224).

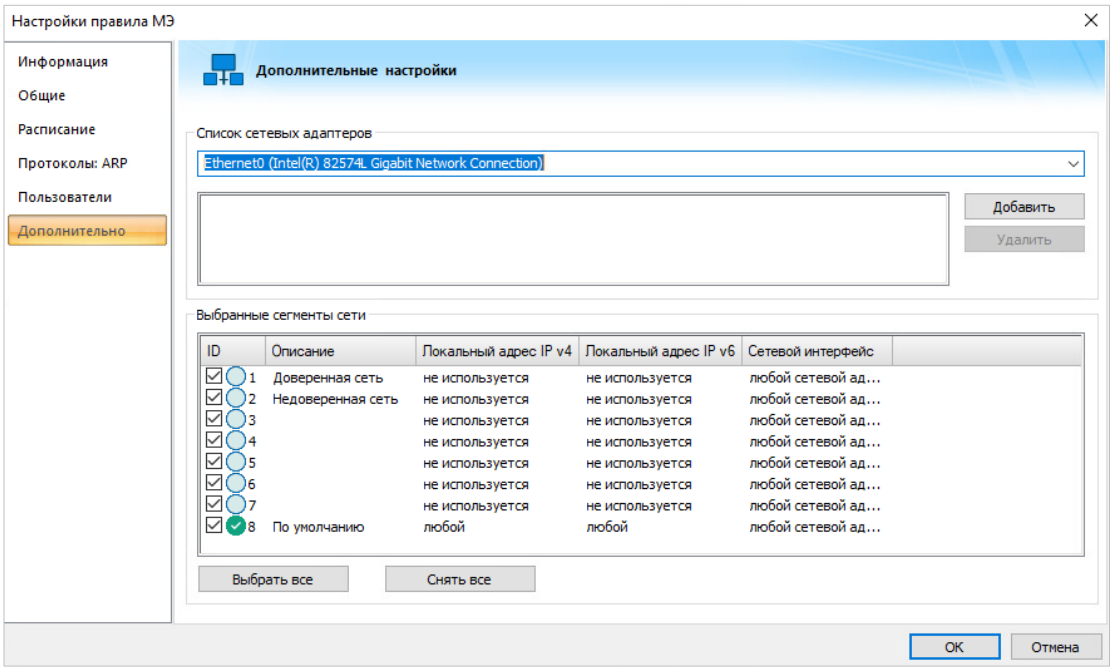


Рис. 224. Настройка правила МЭ

3. Администратор отключил параметр **Глобальное правило — пропускать пакеты по умолчанию**.

   В результате пользователь сможет пользоваться сетью Интернет на АРМ только подключившись к подсети компании через заданный сетевой адаптер.

Пример 2

Администратор хочет разрешить использование сети Интернет только через доверенную (корпоративную) сеть для надежной антивирусной проверки трафика и принудительной защиты всего трафика от перехвата.

1. Администратор задал подсеть компании для сегмента сети *Доверенная сеть*.
2. Администратор создал разрешающее правило на использование сети Интернет и выбрал для него сегмент сети *Доверенная сеть*, раздел 15.2.5 Правила МЭ.
3. Администратор создал разрешающее правило для VPN подключения и выбрал для него сегмент сети *По умолчанию*. Правило VPN подключения разрешит защищенное соединение с доверенной сетью из любых сетей. После установления соединения с доверенной сетью возможно использование сети Интернет при получении через VPN адреса из диапазона доверенной сети.
4. Администратор создал запрещающее правило для всех остальных подключений и выбрал для него сегмент сети *По умолчанию*. При этом необходимо, чтобы запрещающее правило было ниже по приоритету (проверялось после разрешающих правил).

В данной конфигурации для получения доступа к сети Интернет на АРМ из неизвестной сети, пользователю необходимо сначала установить VPN соединение к доверенной сети (которое должно быть сконфигурировано таким образом, чтобы выдать пользователю IP-адрес из доверенной сети, и предоставить маршрутизацию через доверенную сеть в интернет).

15.2.3 Соединения

В данной категории отображается список текущих сетевых соединений компьютера. В данном списке отображается детальная информация по каждому соединению с привязкой к процессам и ведением статистики (рис. 225).

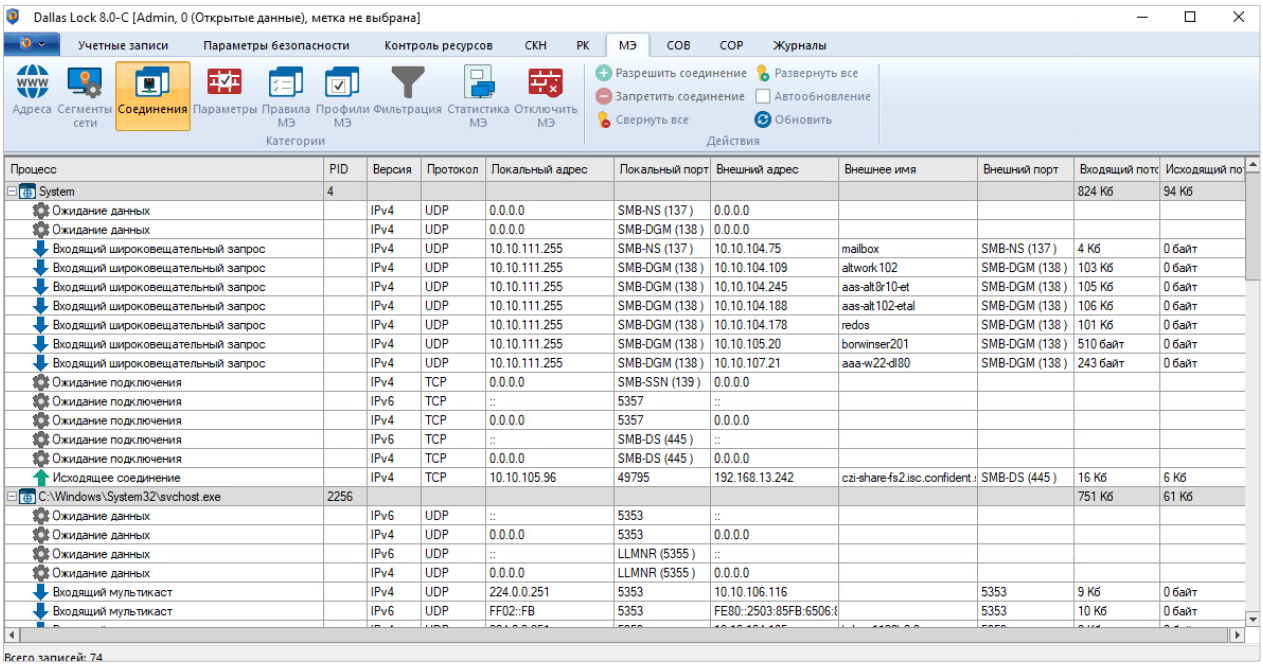


Рис. 225. Список соединений

Существует возможность запретить или разрешить соединение, создать запрещающее или разрешающее правило для соединения, подраздел 15.2.5 Правила МЭ, создать исключение для соединения, подраздел Исключения, свернуть или развернуть список соединений, и обновить информационную панель. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

Активированное действие **Автообновление** позволяет автоматически обновлять список соединений раз в 5 секунд.

15.2.4 Параметры

В данной категории для настройки доступны основные параметры МЭ (рис. 226).

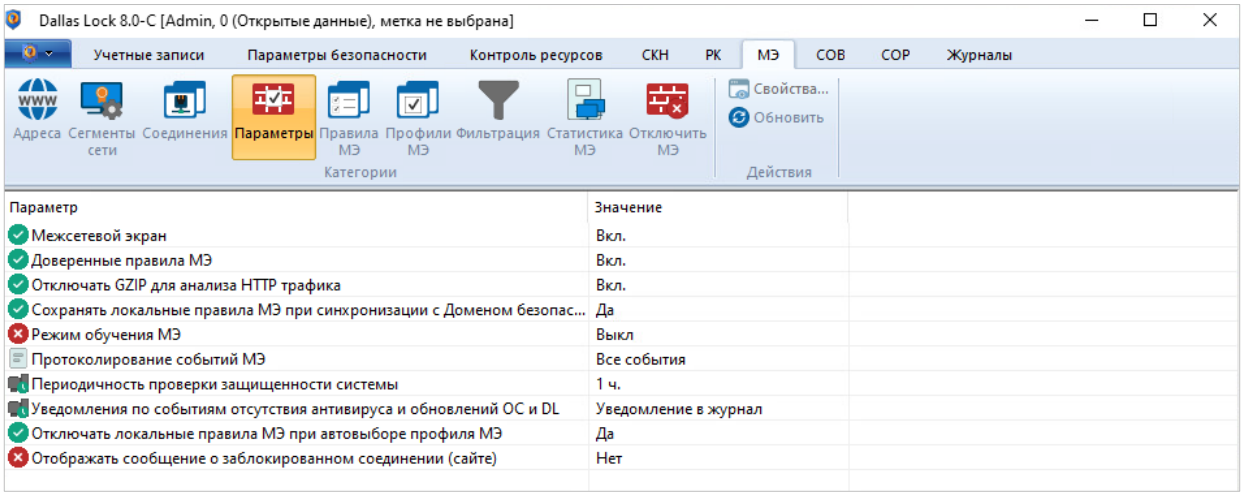


Рис. 226. Параметры МЭ

Управление параметрами осуществляется на панели **Действия** через нажатие кнопки **Свойства** при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню **свойства** интересующего пункта редактирования параметров безопасности.

Доступны следующие параметры:

Межсетевой экран
Данный параметр необходим для включения и отключения работы МЭ.
Доверенные правила МЭ
Данный параметр необходим для поддержания работы по умолчанию следующих протоколов:

- ARP;
- DNS;
- ICMP;
- DHCP;
- MSRPC;
- LDAP;
- DL (трафик управления **Dallas Lock**).

Данный параметр создан для осуществления бесперебойной работы базовых сетевых функций ОС вне зависимости от заданных пользователем настроек.

Наличие доверенных правил **МЭ** гарантирует возможность удаленного и централизованного управления по протоколам **DL** в случае ошибочного задания чрезмерных блокирующих правил.

Отключение доверенных правил **МЭ** не рекомендуется.

Отключать GZIP для анализа HTTP трафика

Данный параметр отключает сжатие трафика в независимости от настроек браузеров. Сжатие трафика ускоряет загрузку веб-страниц, но при этом препятствует возможности анализа трафика механизмами фильтрации **МЭ** (и при анализе сигнатур трафика **СОВ**). Если деактивировать данную политику — возможна некорректная работа механизма фильтрации (при использовании сайтами сжатия трафика).

Сохранять локальные правила МЭ при синхронизации с Доменом безопасности

Параметр позволяет использовать локальные правила **МЭ**, которые не подчинены списку правил **МЭ** на **СБ**. Если на клиенте **ДБ** включен данный параметр, то при синхронизации локальные правила не будут удалены.

Режим обучения МЭ

Параметр позволяет включить и настроить режим обучения **МЭ**, раздел Режим обучения МЭ.

Протоколирование событий МЭ

Данный параметр позволяет выбрать регистрируемые события об изменении конфигурации **МЭ**.

Периодичность проверки защищенности системы

Данный параметр позволяет настроить периодичность проверки защищенности системы с доступными интервалами от 10 мин до 1 дня. Доступна настройка (Включение/выключение; определение временного интервала, если доступно) оповещения об отсутствии обновлений для следующих объектов:

- обновление ОС — при двойном нажатии на объект, открывается окно со списком всех обновлений ОС с возможностью сортировки по дате установки обновления;
- обновление антивируса;
- обновление сетевых сигнатур.

Также в окне свойств доступна информация о последнем обновлении объектов и времени проведения последней проверки.

Уведомление по событиям отсутствия антивируса и обновлений ОС и DL

Параметр позволяет настраивать (Включение/выключение) способы уведомления по событиям отсутствия антивируса и обновлений ОС и **DL**. Доступны следующие способы уведомления:

- уведомление в системный tray,
- уведомление в журнал.

Отключать локальные правила МЭ при автопереключении профиля МЭ

С помощью данного параметра осуществляется настройка отключения локальных правил **МЭ** при автопереключении профиля **МЭ**. Значение по умолчанию *Да*.

Отображать сообщение о заблокированном соединении (сайте)

С помощью этого параметра можно включить или отключить отображение сообщения о заблокированном соединении (сайте) (рис. 227).



Рис. 227. Сообщение о заблокированном соединении

Режим обучения МЭ

Для настройки списка правил **МЭ** возможно использовать **Режим обучения МЭ**. Данный режим позволяет создавать разрешающие правила **МЭ** для текущих соединений пользователя в автоматическом и интерактивном режимах.

Чтобы выполнить настройку правил **МЭ** в автоматическом режиме используя режим обучения **МЭ**, необходимо:

1. Открыть категорию **МЭ** → **Параметры** и нажать два раза кнопкой мыши на параметр **Режим обучения МЭ**. Появится окно настройки и выбора режимов (рис. 228).

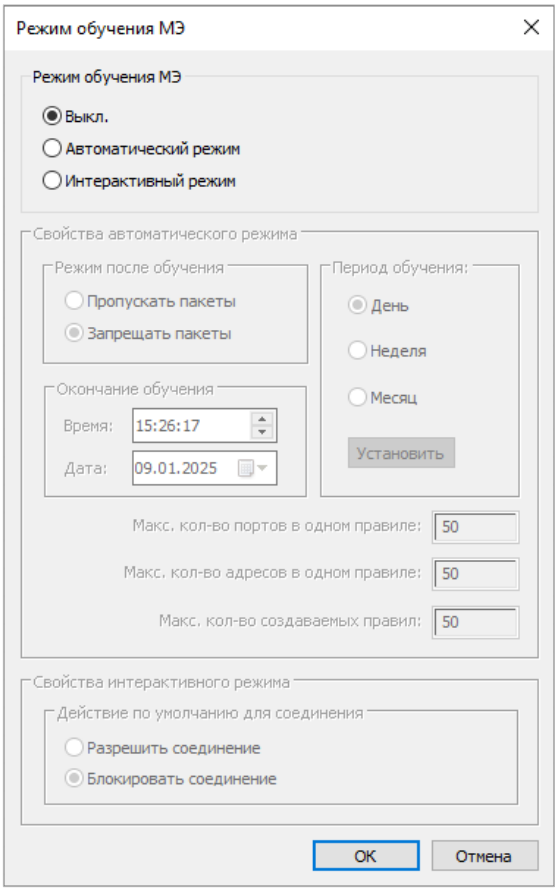


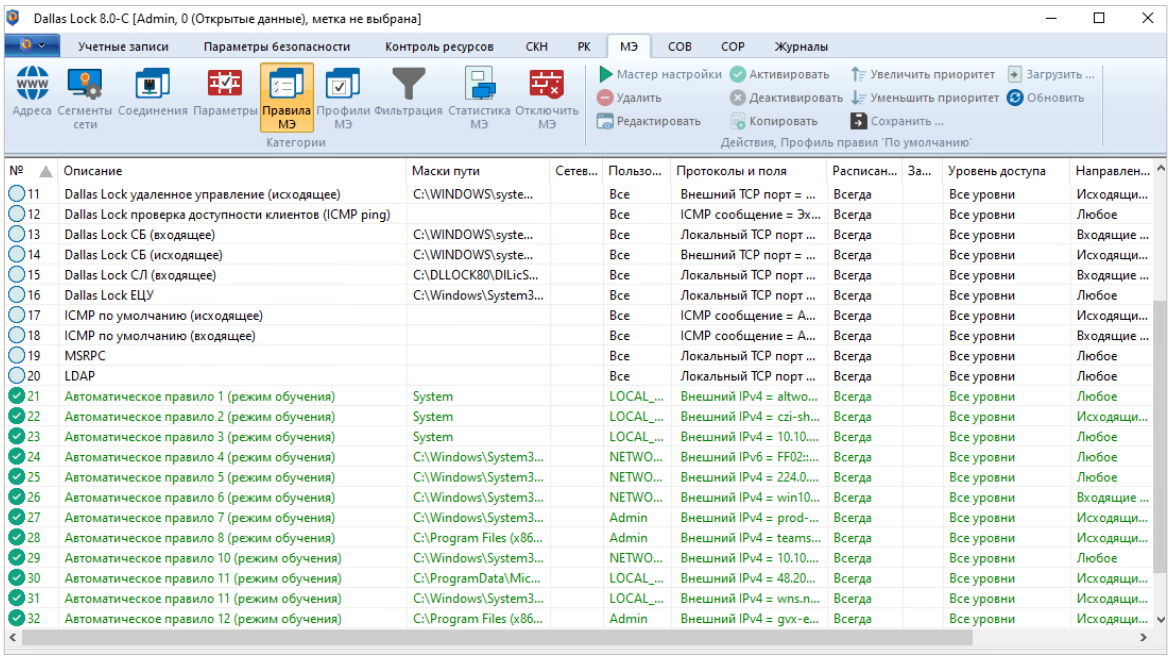
Рис. 228. Настройка автоматического режима обучения МЭ

2. Установить флаг *Автоматический режим*.
3. Выбрать режим работы МЭ после завершения режима обучения:
   - *пропускать пакеты* — устанавливает значение *Да* для параметра **Глобальное правило — пропускать пакеты по умолчанию**;

- *запрещать пакеты* — устанавливает значение *Нет* для параметра **Глобальное правило — пропускать пакеты по умолчанию**.

4. Установить дату и время окончания режима обучения. Есть возможность установить период времени: день, неделя и месяц.
5. Для гибкой настройки правил возможно указать максимальное количество портов и IP-адресов в одном правиле.
6. Осуществить вход на все те веб-ресурсы, с которыми пользователь имеет право работать (но не открывать ничего лишнего).
7. Следует помнить, что не для всех веб-ресурсов является достаточным просто их открыть. Некоторые веб-ресурсы загружают не все данные, а только необходимое для работы конкретного веб-ресурса, остальное подгружается динамически, в процессе работы. Поэтому лучше выполнить все основные действия на веб-ресурсе для работы.

   На этом этапе создаются автоматические локальные правила **МЭ** (далее — АЛП). В списке правил **МЭ** АЛП выделяются зеленым цветом.



№	Описание	Маски пути	Сетев...	Пользо...	Протоколы и поля	Расписан...	За...	Уровень доступа	Направлен...
11	Dallas Lock удаленное управление (исходящее)	C:\WINDOWS\syste...		Все	Внешний TCP порт = ...	Всегда		Все уровни	Исходящи...
12	Dallas Lock проверка доступности клиентов (ICMP ping)			Все	ICMP сообщение = Эх...	Всегда		Все уровни	Любое
13	Dallas Lock СБ (входящее)	C:\WINDOWS\syste...		Все	Локальный TCP порт ...	Всегда		Все уровни	Входящие ...
14	Dallas Lock СБ (исходящее)	C:\WINDOWS\syste...		Все	Внешний TCP порт = ...	Всегда		Все уровни	Исходящи...
15	Dallas Lock СЛ (входящее)	C:\DLLOCK80\DILicS...		Все	Локальный TCP порт ...	Всегда		Все уровни	Входящие ...
16	Dallas Lock ЕЦУ	C:\Windows\System3...		Все	Локальный TCP порт ...	Всегда		Все уровни	Любое
17	ICMP по умолчанию (исходящее)			Все	ICMP сообщение = А...	Всегда		Все уровни	Исходящи...
18	ICMP по умолчанию (входящее)			Все	ICMP сообщение = А...	Всегда		Все уровни	Входящие ...
19	MSRPC			Все	Локальный TCP порт ...	Всегда		Все уровни	Любое
20	LDAP			Все	Локальный TCP порт ...	Всегда		Все уровни	Любое
21	Автоматическое правило 1 (режим обучения)	System		LOCAL_...	Внешний IPv4 = altwo...	Всегда		Все уровни	Любое
22	Автоматическое правило 2 (режим обучения)	System		LOCAL_...	Внешний IPv4 = czi-sh...	Всегда		Все уровни	Исходящи...
23	Автоматическое правило 3 (режим обучения)	System		LOCAL_...	Внешний IPv4 = 10.10....	Всегда		Все уровни	Любое
24	Автоматическое правило 4 (режим обучения)	C:\Windows\System3...		NETWO...	Внешний IPv6 = FF02::...	Всегда		Все уровни	Любое
25	Автоматическое правило 5 (режим обучения)	C:\Windows\System3...		NETWO...	Внешний IPv4 = 224.0....	Всегда		Все уровни	Любое
26	Автоматическое правило 6 (режим обучения)	C:\Windows\System3...		NETWO...	Внешний IPv4 = win10...	Всегда		Все уровни	Входящие ...
27	Автоматическое правило 7 (режим обучения)	C:\Windows\System3...		Admin	Внешний IPv4 = prod-...	Всегда		Все уровни	Исходящи...
28	Автоматическое правило 8 (режим обучения)	C:\Program Files (x86...		Admin	Внешний IPv4 = teams...	Всегда		Все уровни	Исходящи...
29	Автоматическое правило 10 (режим обучения)	C:\Windows\System3...		NETWO...	Внешний IPv4 = 10.10....	Всегда		Все уровни	Любое
30	Автоматическое правило 11 (режим обучения)	C:\ProgramData\Mic...		LOCAL_...	Внешний IPv4 = 48.20...	Всегда		Все уровни	Исходящи...
31	Автоматическое правило 11 (режим обучения)	C:\Windows\System3...		LOCAL_...	Внешний IPv4 = wns.n...	Всегда		Все уровни	Исходящи...
32	Автоматическое правило 12 (режим обучения)	C:\Program Files (x86...		Admin	Внешний IPv4 = gvx-e...	Всегда		Все уровни	Исходящи...

Рис. 229. Создание правил МЭ с помощью режима обучения МЭ

Созданное АЛП может автоматически дополняться, до тех пор, пока не завершится режим обучения или пользователь не произведет модификацию АЛП в момент работы режима обучения. Под модификацией АЛП понимается любое изменение данного правила.

Если в процессе обучения будет выявлена сетевая атака, приводящая к созданию огромного количества АЛП, то в **Журнал управления политик** регистрируется ошибка и работа режима обучения автоматически завершится. Также будет удалены все созданные АЛП.

Если в процессе обучения произойдет выключение компьютера, то сохранятся только модифицированные пользователем АЛП.

8. После завершения режима обучения, созданные и модифицированные АЛП добавляются в конец списка правил **МЭ** (низший приоритет) и становятся локальными правилами. Правила, созданные с помощью режима обучения **МЭ**, выделяются синим цветом в списке правил **МЭ**.

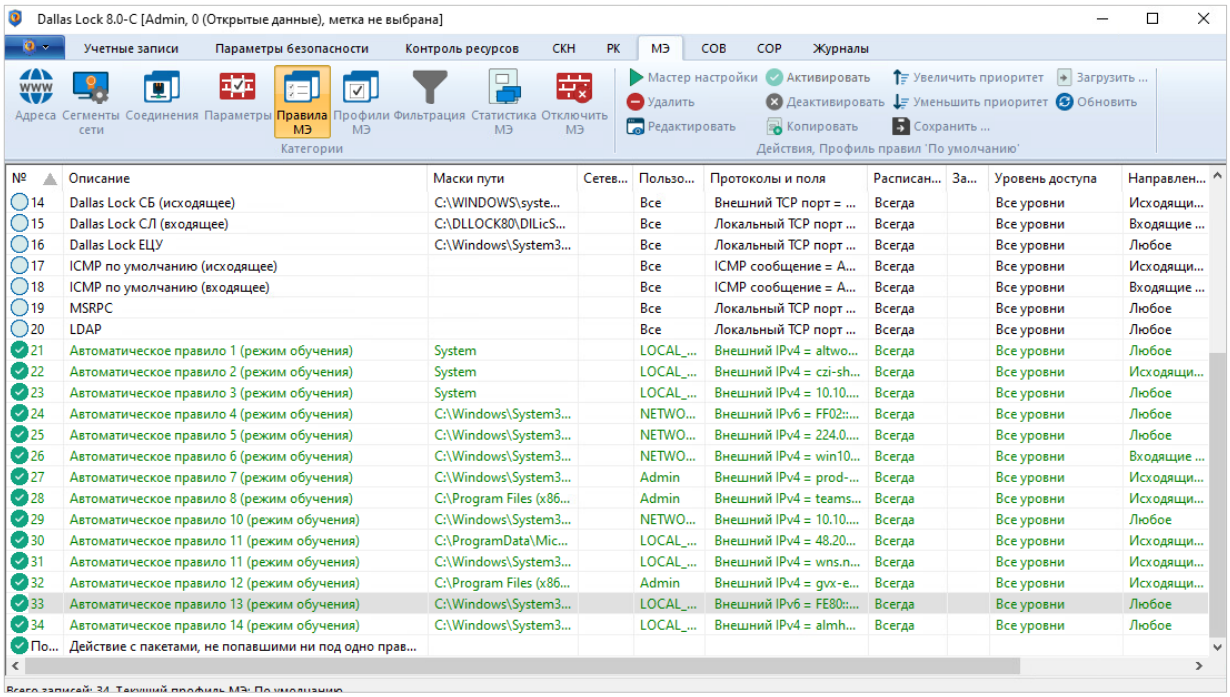


Рис. 230. Созданные правила МЭ с помощью режима обучения МЭ

Для ручного выключения режима обучения необходимо открыть категорию **МЭ** → **Параметры** и щелкнуть два раза кнопкой мыши на параметр **Режим обучения МЭ**. В появившемся окне установить флаг *Выкл*.

При включенном интерактивном режиме обучения сетевая активность будет анализироваться в соответствии с уже имеющимися правилами. Если для подключения нет доступных правил, пользователю при помощи диалогового окна будет предложено разрешить или запретить сетевое взаимодействие для приложения. Чтобы выполнить настройку правил **МЭ** в интерактивном режиме используя режим обучения **МЭ**, необходимо:

1. Открыть категорию **МЭ** → **Параметры** и щелкнуть два раза кнопкой мыши на параметр **Режим обучения МЭ**. Появится окно подтверждения включения данного режима (рис. 228).
2. Установить флаг *Интерактивный режим* (рис. 231).

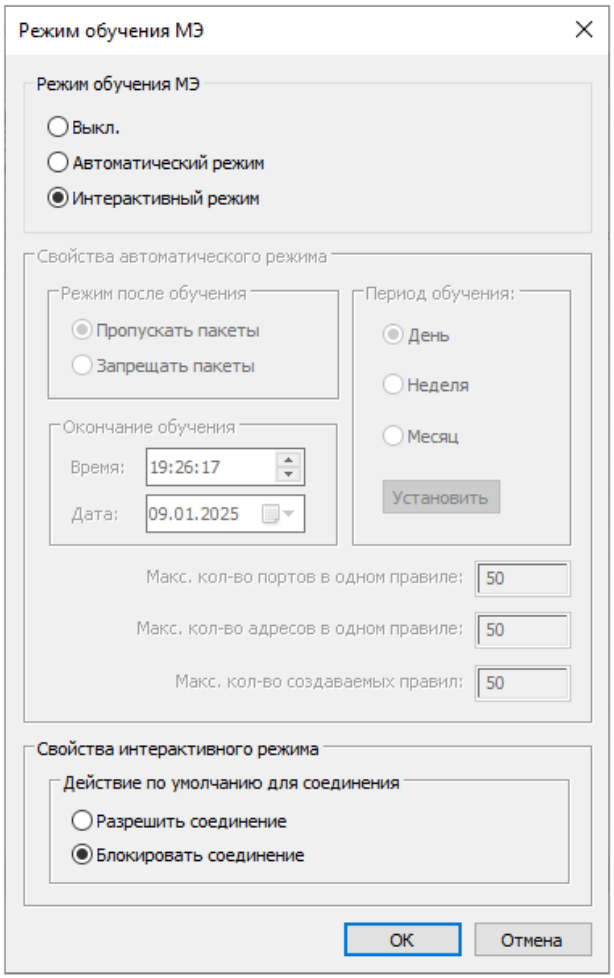


Рис. 231. Настройка интерактивного режима обучения МЭ

3. Установить флаг:
   - *Разрешить соединение*;
   - *Блокировать соединение*;
4. Нажать кнопку **ОК**.

   При первой попытке приложения выполнить сетевую активность, в зависимости от выбранного действия по умолчанию, соединение будет соответственно разрешаться или блокироваться. При этом будет отображаться окно **Интерактивное обучение МЭ** (рис. 232).

В случае, если для приложения с таким именем уже определено активное правило **МЭ**, удовлетворяющее текущим параметрам создания соединения, то окно **Интерактивное обучение МЭ** с возможностью создания правила для данного приложения отображаться не будет.

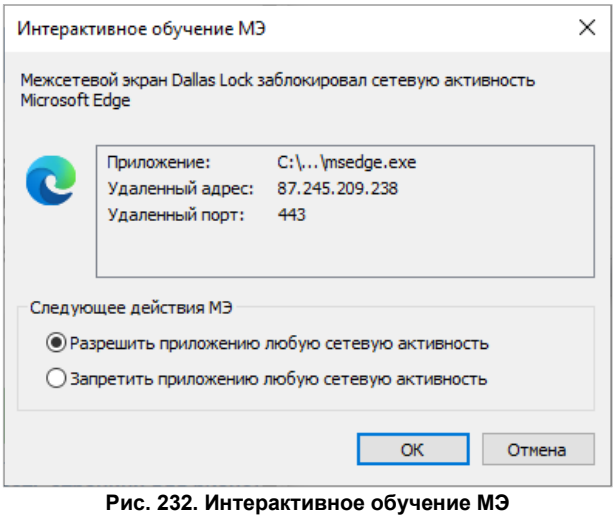


Рис. 232. Интерактивное обучение МЭ

5. Выбрать действие, которое необходимо выполнять **МЭ** для данного приложения:
   - *Разрешить приложению любую сетевую активность*;
   - *Запретить приложению любую сетевую активность*.

После выбора действия в списке правил **МЭ** появится новое правило интерактивного обучения. В случае, если окно **Интерактивное обучение МЭ** было закрыто без выбора действия, то правило не будет создано и при следующей сетевой активности данного приложения окно появится вновь (если не было создано правило для данного приложения и пользователя вручную).
Для того, чтобы окно **Интерактивное обучение МЭ** отобразилось снова, необходимо вручную удалить либо деактивировать правило **МЭ**, удовлетворяющее текущим параметрам создания соединения. В случае если правило было удалено, будет создано новое правило после выбора в окне **Интерактивное обучение МЭ** в случае, если правило было деактивировано — оно обновится в соответствии с заданными в окне значениями и автоматически станет активным.

15.2.5 Правила МЭ

Данная категория настроек является основным инструментом управления функциями межсетевого экрана и позволяет настраивать его работу.

Для перехода к управлению правилами необходимо открыть вкладку **МЭ** и выбрать категорию **Правила МЭ**.

На информационной панели находится список правил и основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д. (рис. 233).

При работе возможно наблюдать открытые порты 1000 и 1004 даже если создано запрещающее правило **МЭ**, но подключиться к этим портам невозможно, так как они используются службой DIIpsService.

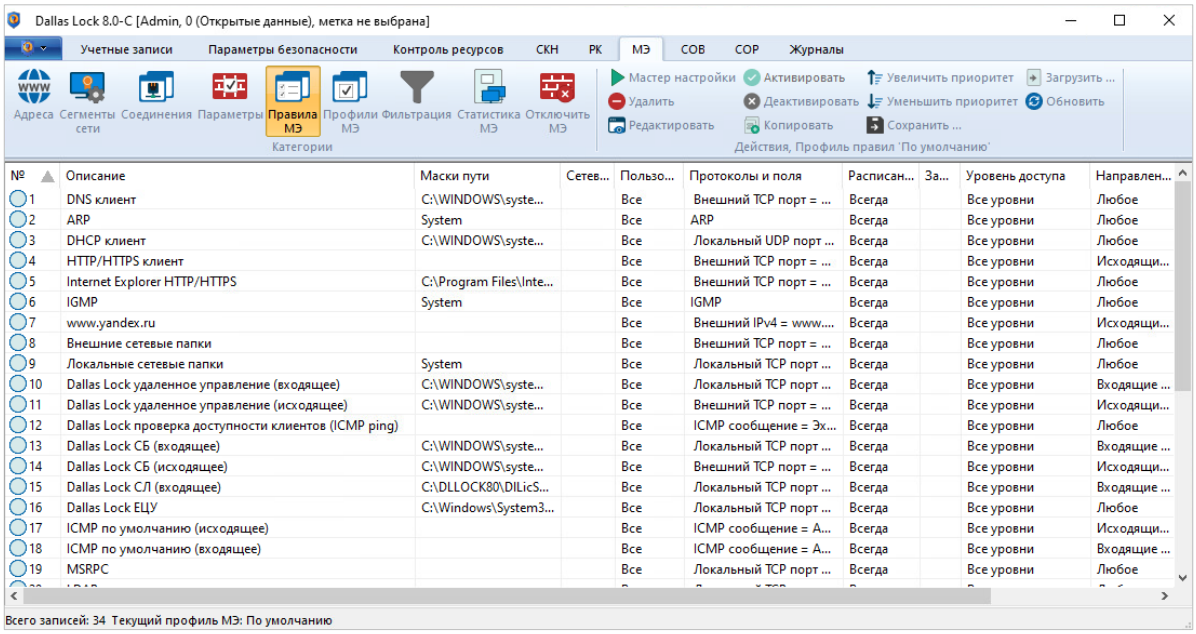


Рис. 233. Панель настройки правил межсетевого экрана

На каждом клиенте присутствуют следующие правила **МЭ**:

- правило по умолчанию (действие с пакетами, не попавшими ни под одно правило);
- общие правила **МЭ**;
- локальные правила **МЭ** (автоматические правила, создаваемые в режиме обучения, по умолчанию являются локальными, для изменения типа правила нужно выполнить: выбрать редактируемое правило → **Редактировать** на панели **Действия** → вкладка *Общие* → изменить значение параметра *Локальное правило*).

Локальные правила являются индивидуальными для каждого клиента. На панели настройки правил **МЭ** локальные правила выделяются синим цветом.

Существует возможность редактирования имеющегося шаблона, его удаление и обновление, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

Для редактирования имеющегося шаблона нужно нажать кнопку **Редактировать** на панели **Действия**. Откроется окно **Настройки правила МЭ**. В появившемся меню окна **Настройки правила МЭ** можно осуществить несколько уровней редактирования текущего шаблона.

В разделе *Информация* отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 234). В версии «С» раздел *Информация* дополнен параметром «*Мандатный уровень*», информирующий о том, для каких мандатных уровней применяется правило.

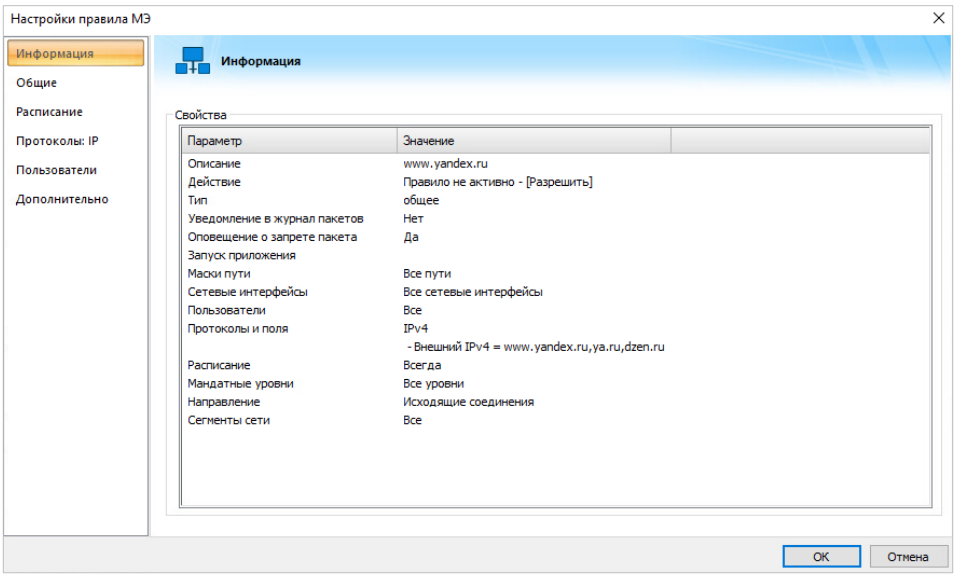


Рис. 234. Настройка правил межсетевого экрана

В разделе *Общие* представлены основные настройки правила (рис. 235):

- описание правила;
- действие, которое должно выполняться согласно правилу: запретить/разрешить;
- запустить приложение: указать путь к приложению, которое должно запуститься при срабатывании правила;
- применение правила только для указанных приложений: необходимо указать путь к приложению;
- параметры: необходимо указать все параметры (ключи), с которыми выполняется приложение, при указании приложения с неполным перечнем параметров корректное выполнение правила не гарантируется.

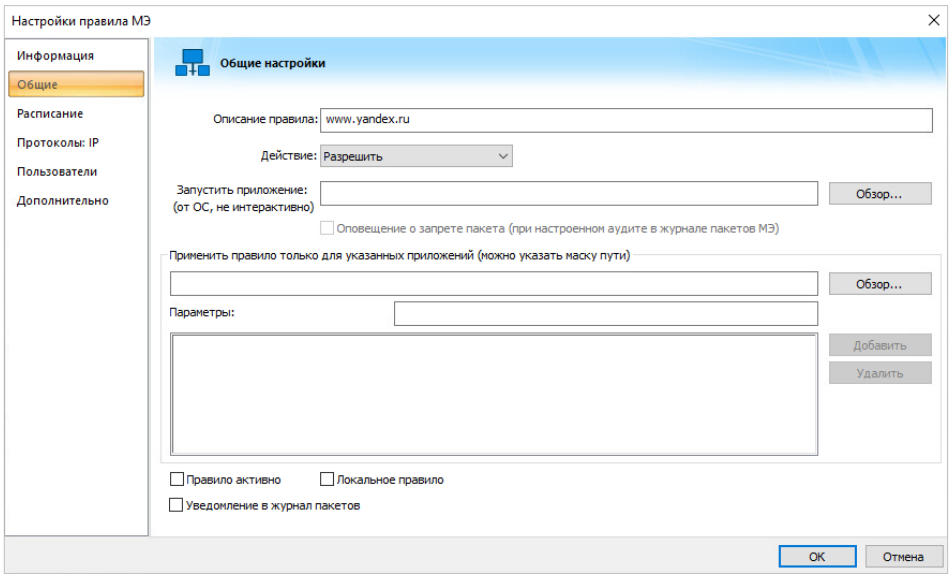


Рис. 235. Общие настройки правила МЭ

Если был задан параметр *Запустить приложение*, то при срабатывании правила, приложение запустится от имени ОС и запуск приложения будет осуществлен не интерактивно, то есть без взаимодействия с пользователем. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе *Расписание* составляется расписание контроля в соответствии с требованиями к правилу. В подразделе *Расписание работы* отображена группа полей для включения контроля по дням недели, часам и минутам. Активное время работы расписания правила отмечено синими цветом. Также для упрощения настройки правила в подразделах окна *Дополнительное управление расписанием работы* можно при нажатии на кнопки настроить работу правила. Изменения будут фиксироваться в подразделе *Расписание работы*. Для временного правила используется подраздел *Период действия правила*, в котором можно настроить временный период работы правила.

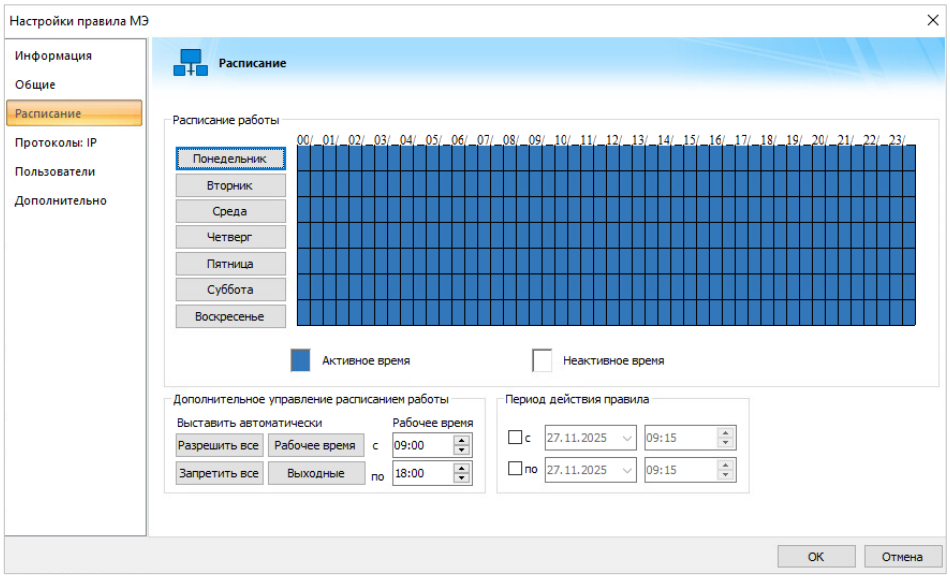


Рис. 236. Настройка расписания правила МЭ

В разделе *Протоколы* можно задать детальные настройки отображаемой информации по принимаемым/отправляемым пакетам: направление передачи (входящие пакеты, исходящие пакеты, любое направление передачи, входящие соединения, исходящие соединения), вид протокола и его параметры (рис. 237). Есть возможность выбрать следующие направления передачи:

- Входящие пакеты — если правило разрешающее, то разрешаются все входящие пакеты.
- Исходящие пакеты — если правило разрешающее, то разрешаются все исходящие пакеты.
- Любое направление передачи.
- Входящие соединения — если правило разрешающее, то при успешном входящем соединении разрешается обратное исходящее соединение. Если правило запрещающее, то запрещаются все входящие соединения.
- Исходящие соединения — если правило разрешающее, то при успешном исходящем соединении, разрешается обратное входящее соединение. Если правило запрещающее, то запрещаются все исходящие соединения.

Возможно использование DNS-адресов, но стоит учитывать, что это менее безопасно ввиду возможности атак на DNS-сервер, DNS-протокол и неожиданных внешних изменений DNS-записей их владельцами.

Для настройки доступа к некоторым веб-ресурсам, таким как «www.gosuslugi.ru», может потребоваться настройка разрешений на дополнительные ресурсы, в зависимости от настроек работы самого сайта. Например, на момент написания документации в случае доступа к ресурсу «www.gosuslugi.ru» для его корректной работы потребуется разрешение доступа к ресурсу «www.gu-st.ru». Подробнее то, какие дополнительные сайты требуются для работы основного, можно узнать через журнал запрещенных пакетов после настройки правила.

Для фильтрации протоколов, использующих различные и не зафиксированные порты, необходимо настроить правила **МЭ** таким образом, чтобы соединения (в том числе UDP) разрешались только для определенного списка портов, и все из этих портов были включены в список перехватываемых исходящих портов, раздел Настройки фильтрации. Таким образом, фильтрация протоколов будет осуществляться на всем диапазоне возможных портов сетевого трафика.

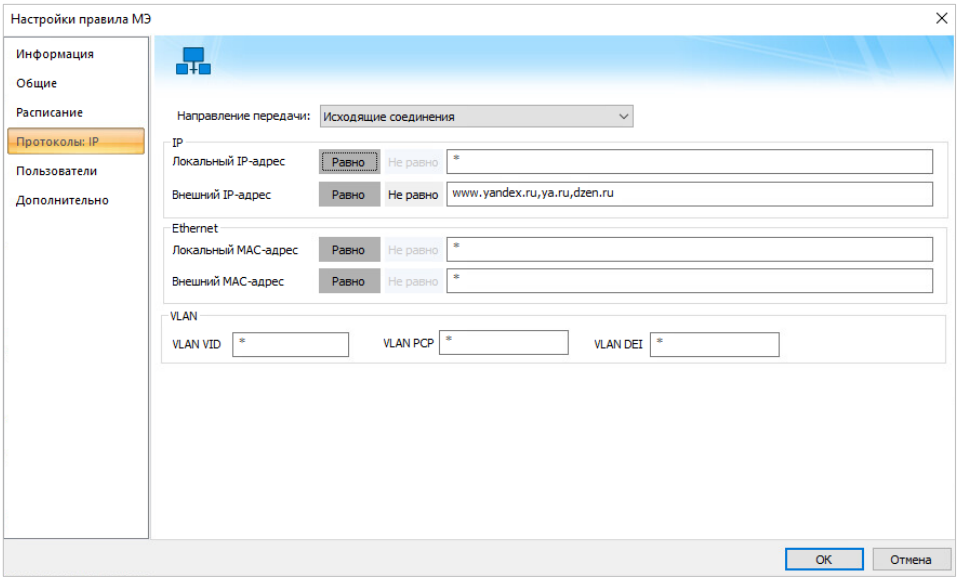


Рис. 237. Настройка протоколов

В разделе *Пользователи* отображается список пользователей, к которым будет применяться правило.

Отметив пункт *Автоматический поиск пользователей/групп* при последующем нажатии кнопок **Пользователи** и **Группы** будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки **Все** все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки **Удалить** (рис. 238). Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (параметр доступен только для Dallas Lock 8.0 редакции «С»).

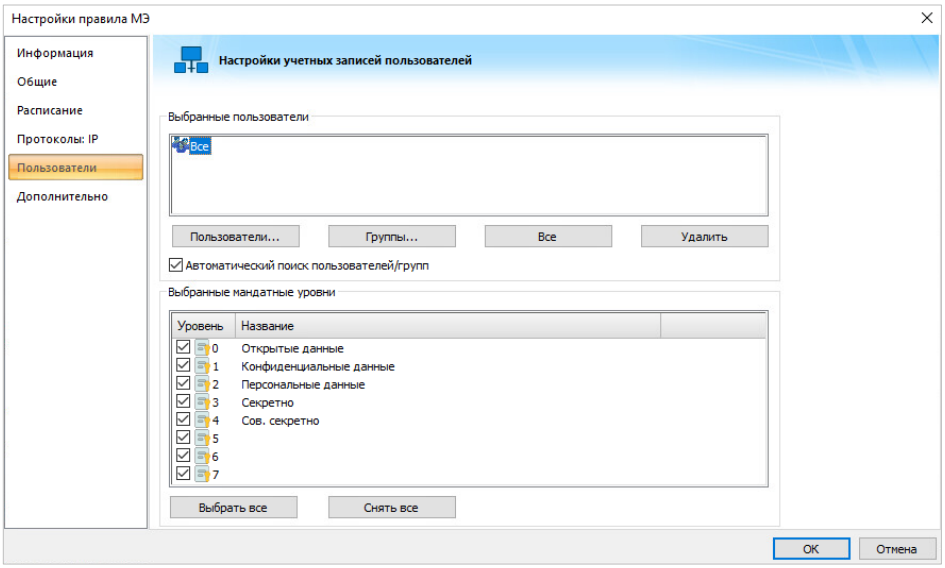


Рис. 238. Пользователи МЭ

В разделе *Дополнительно* существует возможность применения текущего правила **МЭ** только для определенных сетевых адаптеров и (или) сегментов сети. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку **Добавить**. Удаление производится выбором адаптера из списка и нажатием кнопки **Удалить**. Для редактирования списка сегментов сети правила **МЭ** необходимо отметить сегменты сети (рис. 239).

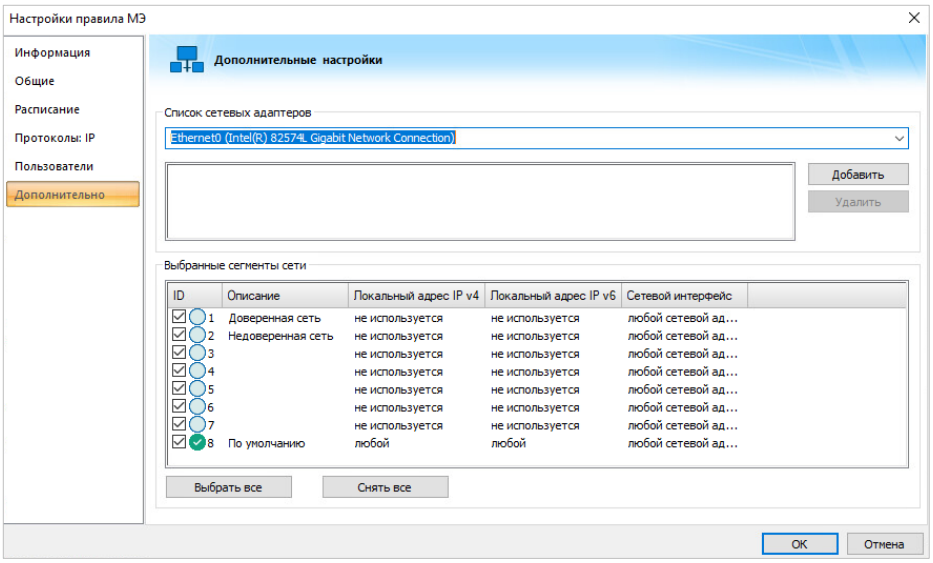


Рис. 239. Дополнительно

Задавать очередность исполняемых правил можно посредством назначения приоритетов. Правила с назначенным приоритетом выше, чем у других, будут проверяться в первую очередь. После срабатывания правила, проверка правил останавливается.

Например, созданы два правила.

Правило 1 запрещает отправку/прием почты по протоколам SMTP/POP3/IMAP.

Правило 2 разрешает пользоваться почтой по протоколам SMTP/POP3/IMAP для серверов mx.yandex.ru.

Рассмотрим случай, когда правила находятся в указанной последовательности. То есть **Правило 1** находится выше **Правила 2**, соответственно приоритет первого правила выше. В данном случае прием/отправка почты по указанным протоколам осуществляться не будет.

В случае если приоритет **Правила 2** будет выше приоритета **Правила 1**, то тогда работа по указанным протоколам будет осуществляться только через сервер mx.yandex.ru.

Процесс создания нового правила происходит по тем же настройкам, что и корректировка уже готового шаблона. Для создания нового правила нужно нажать правую клавишу мыши на информационной панели и выбрать **Мастер настройки** в контекстном меню или нажать ту же кнопку на панели действий. Откроется окно мастера создания правил **МЭ** (рис. 240). Создание нового правила осуществляется по шагам.

На шаге 1 мастера создания правил **МЭ** необходимо заполнить поле *Описание правила*, предназначенное для задания имени правила **МЭ**, и выбрать тип действия правила: запрещающее или разрешающее. По умолчанию указан тип действия *Запретить*.

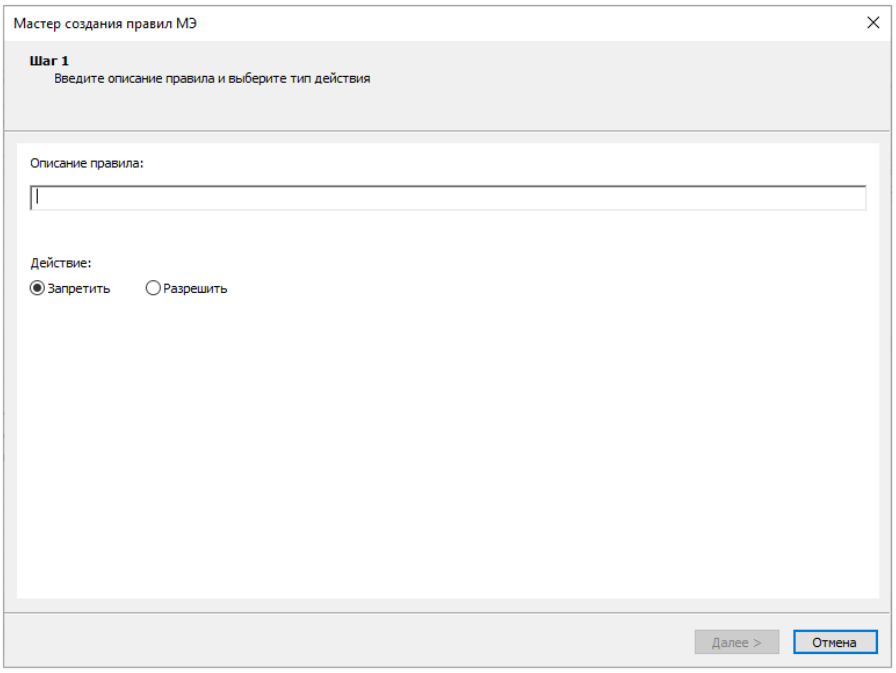


Рис. 240. Мастер создания правил МЭ. Шаг 1

На шаге 2 мастера создания правил **МЭ** (рис. 241) необходимо выбрать направление передачи и указать параметры создаваемого правила.

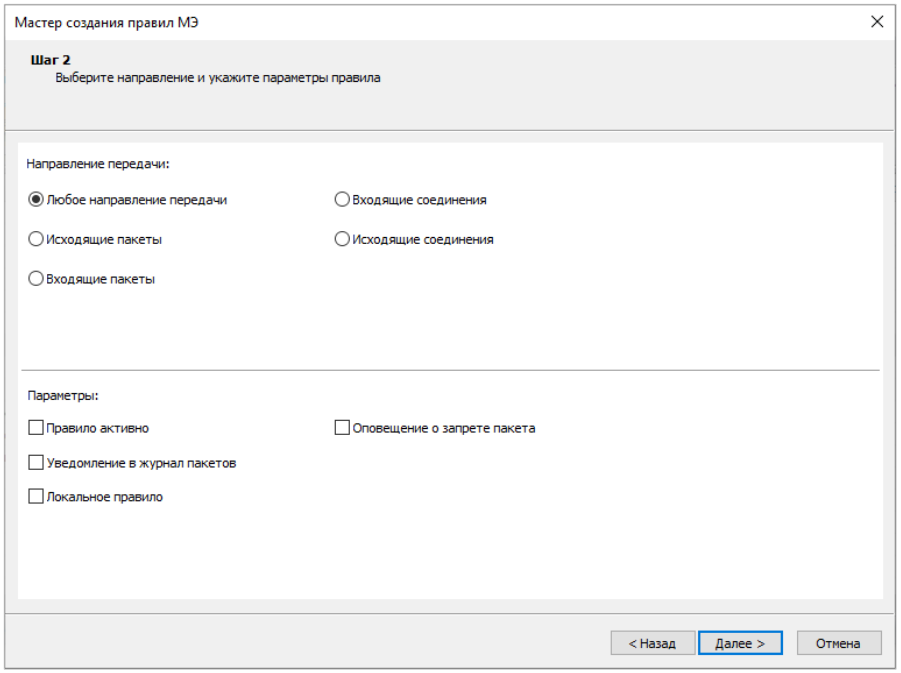


Рис. 241. Мастер создания правил МЭ. Шаг 2

Возможно выбрать следующие направления передачи:

- Любое направление передачи.
- Исходящие пакеты. Если правило разрешающее, то разрешаются все исходящие пакеты.
- Входящие пакеты. Если правило разрешающее, то разрешаются все входящие пакеты.
- Входящие соединения. Если правило разрешающее, то при успешном входящем соединении разрешается обратное исходящее соединение. Если правило запрещающее, то запрещаются все входящие соединения.
- Исходящие соединения. Если правило разрешающее, то при успешном исходящем соединении, разрешается обратное входящее соединение. Если правило запрещающее, то запрещаются все исходящие соединения.

Возможно активировать следующие параметры:

- **Правило активно**. При выключенном параметре созданное правило **МЭ** будет неактивно.
- **Уведомление в журнал пакетов**. При активном параметре осуществляется отображение фиксируемой информации в журнале.

- **Локальное правило**. При активном параметре создаваемое правило будет индивидуальным для клиента, на котором оно создано.
- **Оповещение о запрете пакета**. Параметр активен, если администратор безопасности на шаге 1 выбрал действие «Запретить», иначе параметр неактивен.

На шаге 3 мастера создания правил **МЭ** (рис. 242) осуществляется ввод локальных и внешних IP-адресов, локальных и внешних MAC-адресов и настройка параметров VLAN VID, VLAN PCP, VLAN DEI.

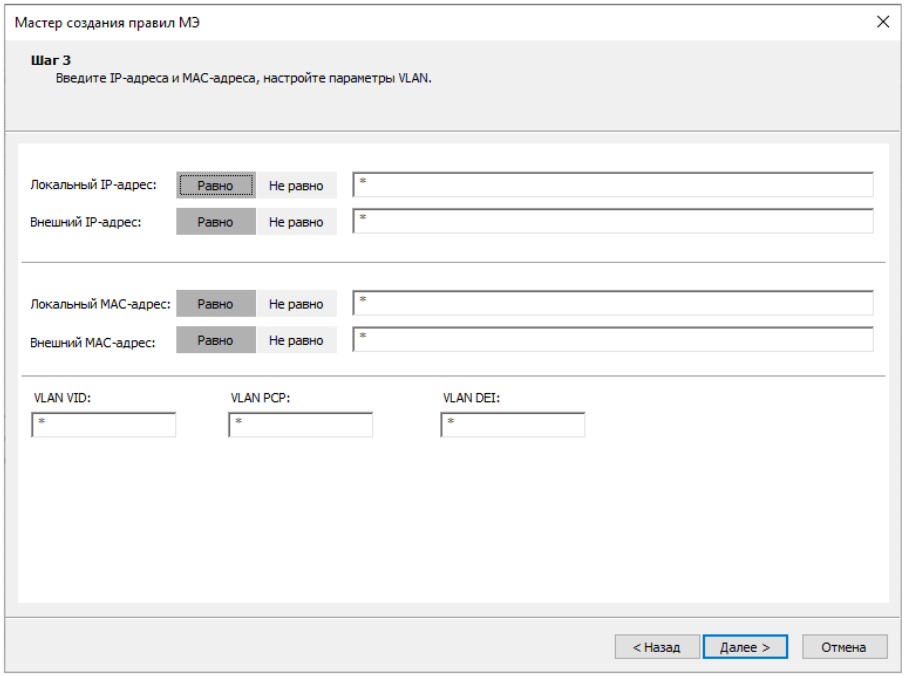


Рис. 242. Мастер создания правил МЭ. Шаг 3

Переключатели *Равно/Не равно* выполняют функцию аналогичных логических операций сравнения. По умолчанию у всех параметров выбрано значение *Равно*.

На шаге 4 мастера создания правил **МЭ** (рис. 243) предоставляется выбор типа правила **МЭ**. Типы правил объединяют сетевые протоколы в группы для удобства настройки правила **МЭ**. От выбранного типа правила будут зависеть доступные протоколы и параметры. После создания правила **МЭ** через редактирование правила смена протокола будет недоступна.

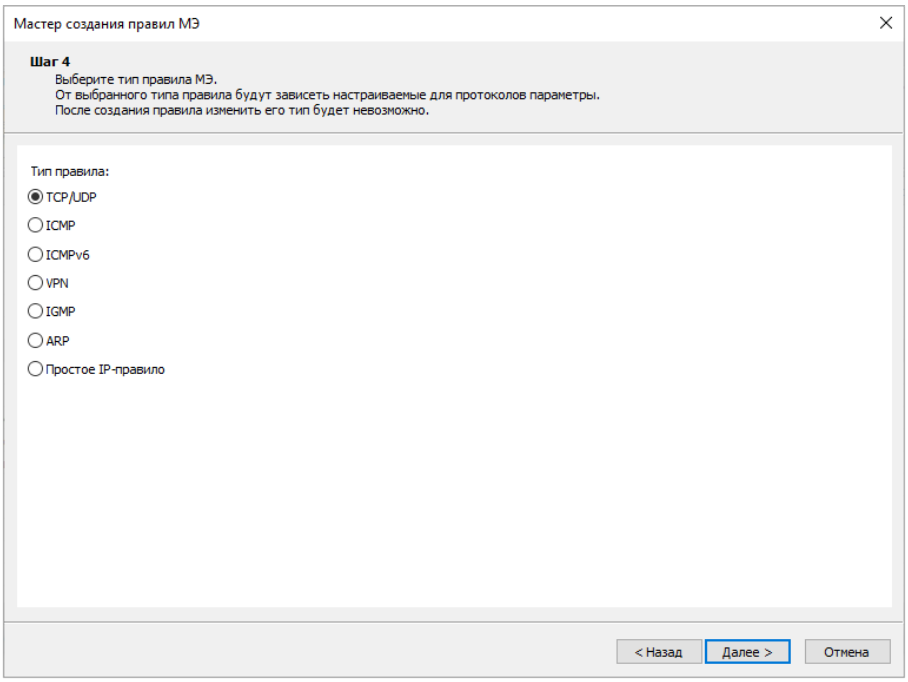


Рис. 243. Мастер создания правил МЭ. Шаг 4

Выбор типа правила **МЭ** доступен с помощью переключателя. По умолчанию выбран тип *TCP/UDP*. При выборе *Простое IP-правило* выбор типа правила **МЭ** не происходит, и мастер настройки правил **МЭ** переходит к шагу 6.

На шаге 5 мастера создания правил **МЭ** (рис. 244) осуществляется настройка протоколов и

параметров в зависимости от выбранного типа правила на шаге 4.

При выборе типа правила **МЭ** *TCP/UDP* на шаге 5 мастера доступны следующие настройки (рис. 244):

- поля с выбором локального и внешнего порта (для протоколов TCP и UDP);
- переключатели *Равно/Не равно* (по умолчанию у всех переключателей установлено значение *Равно*);
- кнопки **Наборы портов** позволяют выбрать необходимый порт из списка (рис. 245), доступен множественный выбор.

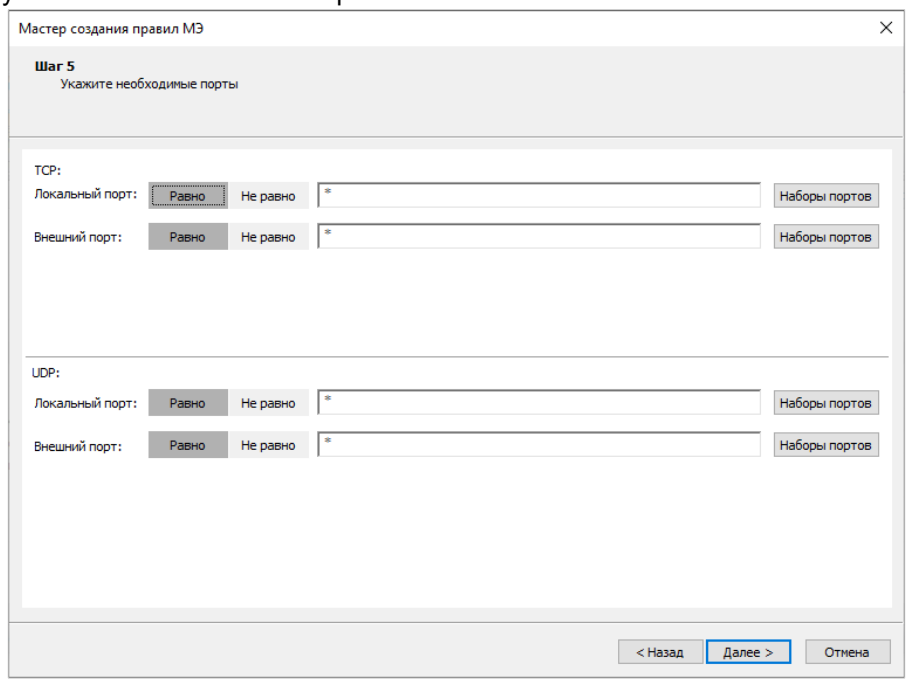


Рис. 244. Мастер создания правил МЭ. Шаг 5. Тип правила «TCP/UDP»

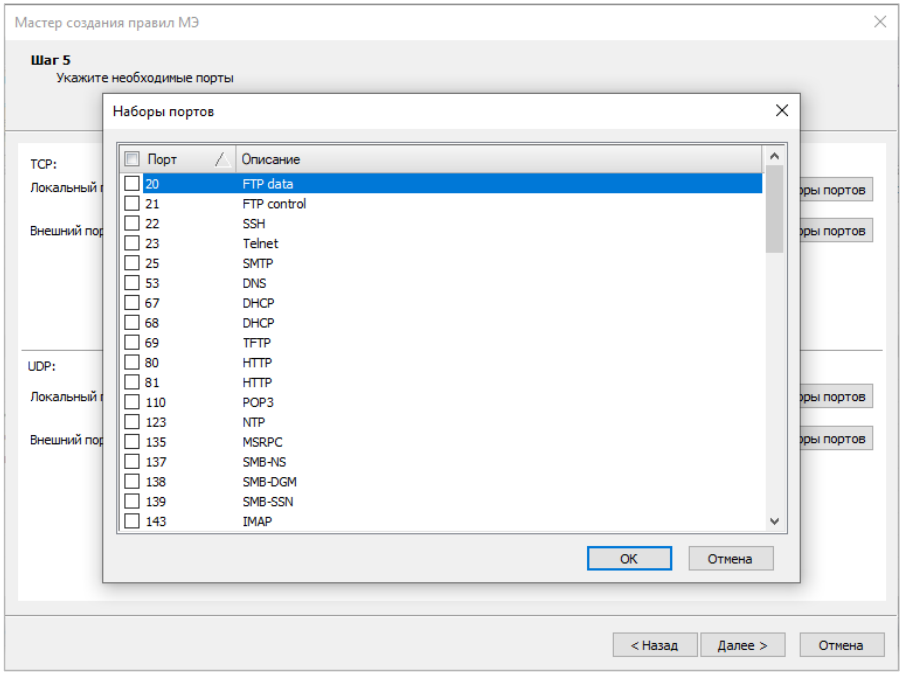


Рис. 245. Мастер создания правил МЭ. Шаг 5. Тип правила «TCP/UDP». Окно «Наборы портов»

При выборе типа правила **МЭ** *ICMP* или *ICMPv6* (рис. 246) на шаге 5 мастера доступен множественный выбор параметров протокола.

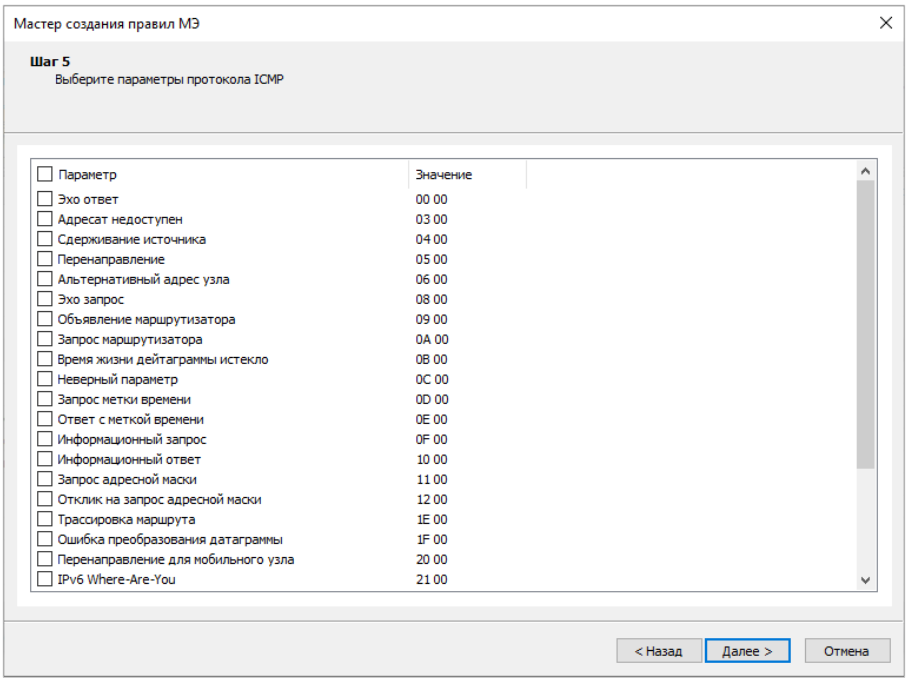


Рис. 246. Мастер создания правил МЭ. Шаг 5. Тип правила «ICMP» или «ICMPv6»

При выборе типа правила **МЭ** *VPN* (рис. 247) на шаге 5 мастера доступны следующие настройки:

- «*ESP SPI*». Числовое значение, которое связывается с конкретным набором параметров безопасности и представляет собой идентификатор, который используется для идентификации конкретного соединения VPN.
- «*AH SPI*». Числовое значение, которое связывается с конкретным набором параметров безопасности и позволяет узлам VPN правильно идентифицировать и проверять целостность данных, передаваемых между ними.
- «*GRE ID протокола*». Числовое значение, связанное с определенным туннелем VPN. Оно позволяет узлам VPN правильно маршрутизировать пакеты через соответствующий туннель и обеспечивает изоляцию трафика между различными туннелями.

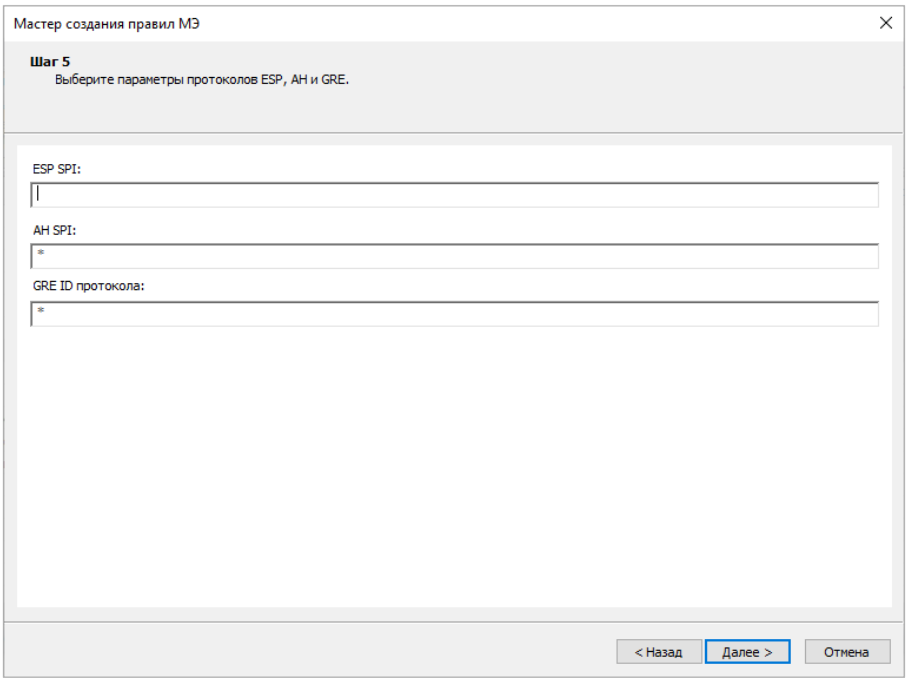


Рис. 247. Мастер создания правил МЭ. Шаг 5. Тип правила «VPN»

При выборе типа правила **МЭ** *IGMP* (рис. 248) на шаге 5 мастера необходимо выбрать параметры протокола IGMP. Возможен множественный выбор параметров.

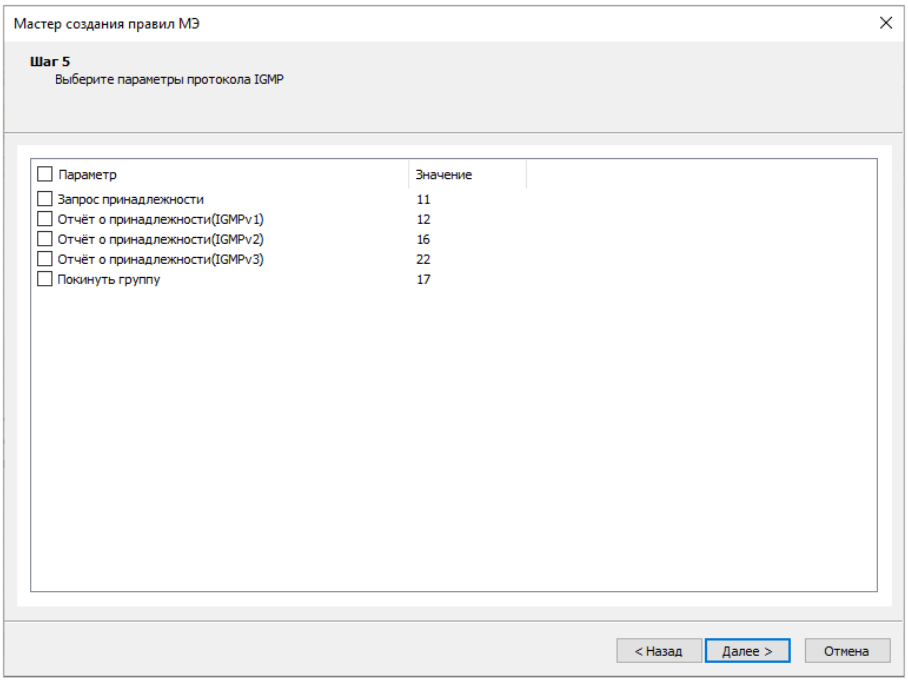


Рис. 248. Мастер создания правил МЭ. Шаг 5. Тип правила «IGMP»

При выборе типа правила МЭ *ARP* (рис. 249) на шаге 5 мастера необходимо настроить параметры протокола ARP.

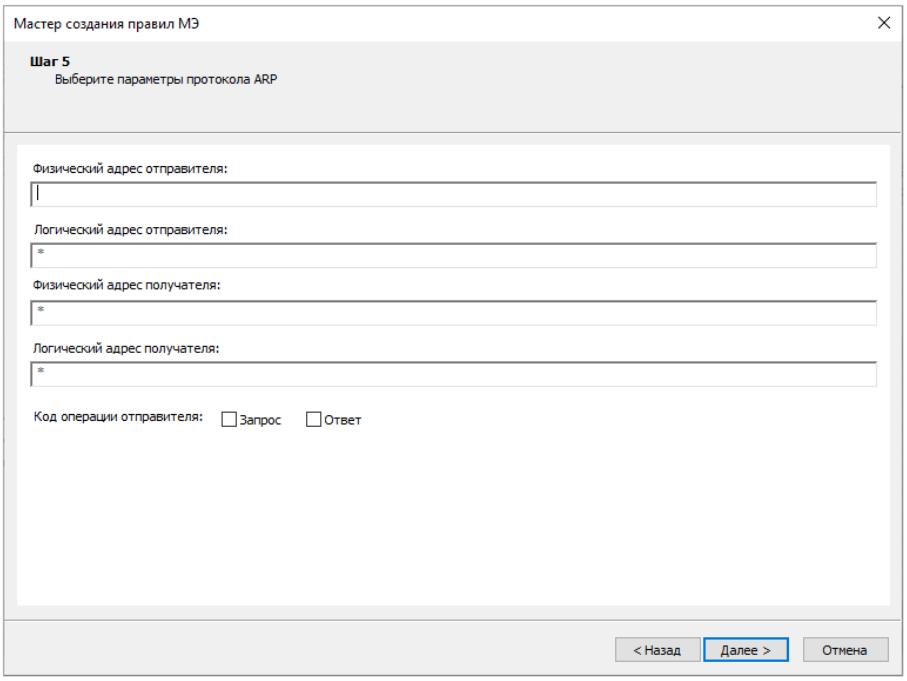


Рис. 249. Мастер создания правил МЭ. Шаг 5. Тип правила «ARP»

Возможно настроить следующие параметры:

- Физический адрес отправителя. Необходимо ввести MAC-адрес отправителя.
- Логический адрес отправителя. Необходимо ввести IP-адрес отправителя.
- Физический адрес получателя. Необходимо ввести MAC-адрес получателя.
- Логический адрес получателя. Необходимо ввести IP-адрес получателя.
- Код операции отправителя. С помощью чекбоксов предоставляется выбор кода операции: *Запрос* или *Ответ*.

На шаге 6 мастера создания правил **МЭ** (рис. 250) осуществляется настройка параметров приложений, на которые распространяется правило.

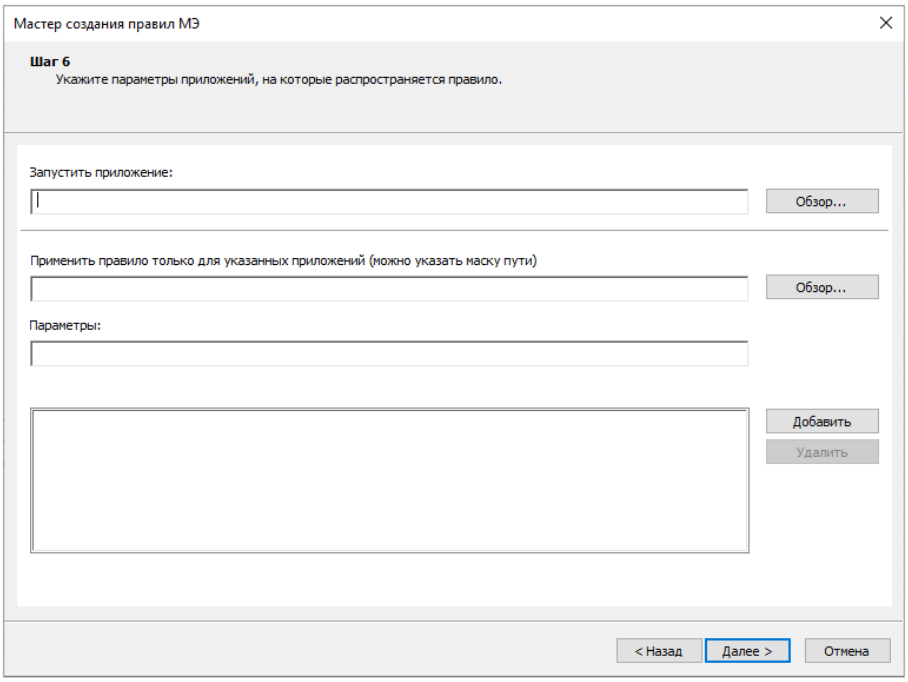


Рис. 250. Мастер создания правил МЭ. Шаг 6

Возможна настройка следующих параметров:

- Запустить приложение. Указывается путь к приложению, которое должно запуститься при срабатывании правила.
- Применить правило только для указанных приложений. Указывается путь к приложению, к которому будет применяться правило.
- Параметры. Указываются все параметры (ключи), с которыми выполняется приложение, при указании приложения с неполным перечнем параметров корректное выполнение правила не гарантируется.

Если был задан параметр **Запустить приложение**, то при срабатывании правила приложение запустится от имени ОС и запуск приложения будет осуществлен не интерактивно, то есть без взаимодействия с пользователем. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

На шаге 7 мастера создания правил **МЭ** (рис. 251) осуществляется настройка расписания работы правила. Параметры шага 7 и их функциональные возможности совпадают с параметрами на вкладке *Расписание* при редактировании уже существующего правила.

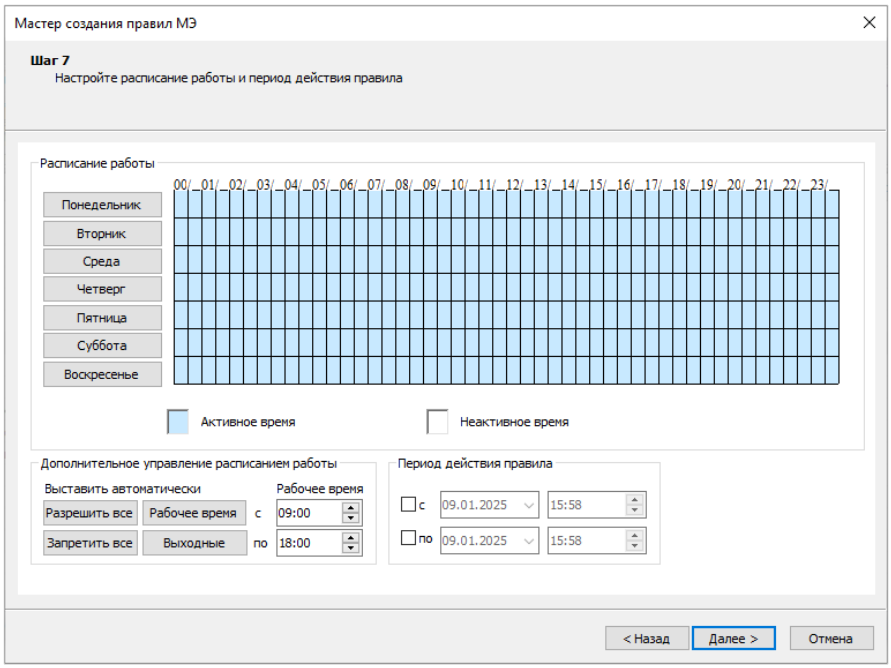


Рис. 251. Мастер создания правил МЭ. Шаг 7

На шаге 8 мастера создания правил **МЭ** (рис. 252) осуществляется настройка списка пользователей и групп пользователей, к которым будет применяться правило. Параметры шага 8 и их функциональные возможности совпадают с параметрами на вкладке *Пользователи* при редактировании уже существующего правила.

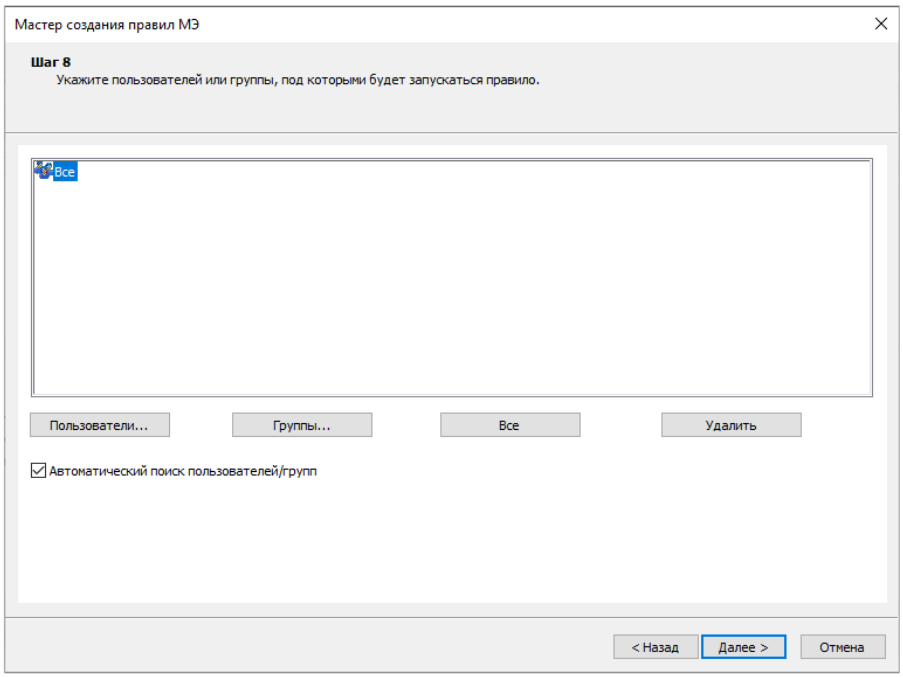


Рис. 252. Мастер создания правил МЭ. Шаг 8

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

.

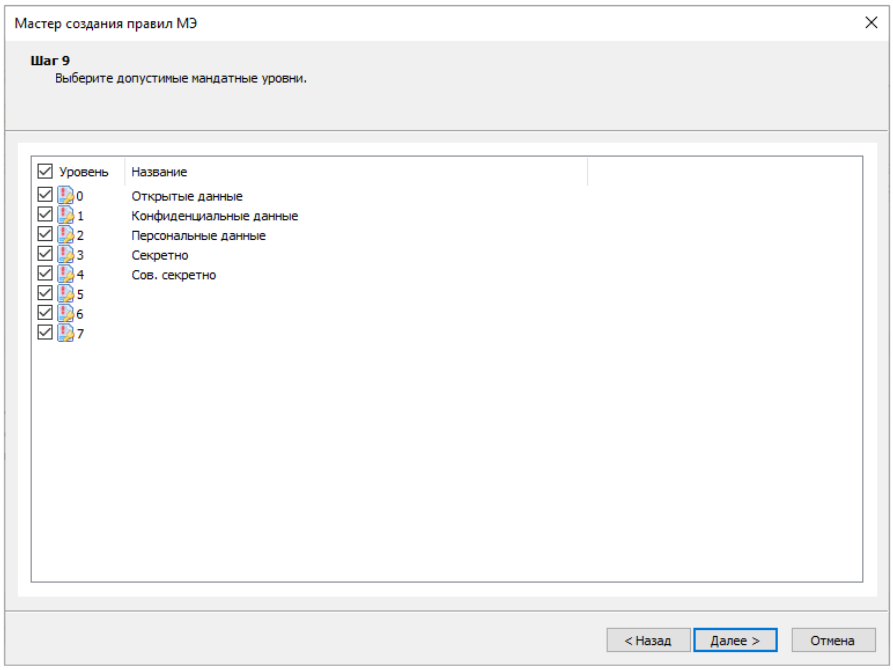


Рис. 253. Мастер создания правил МЭ. Шаг 9

На шаге 10 мастера создания правил **МЭ** (рис. 254) предоставляется возможность проверить введенные настройки до сохранения нового правила.

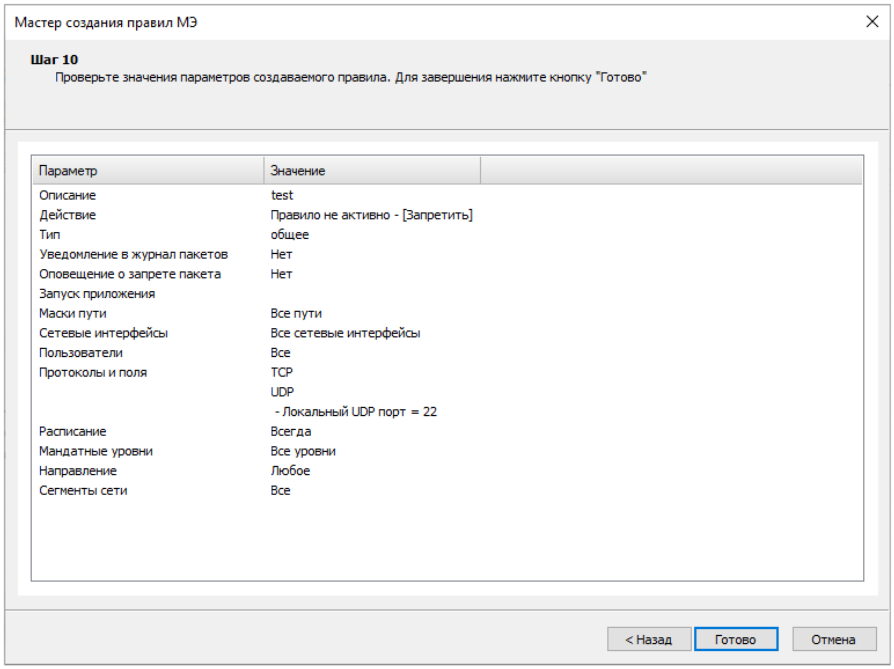


Рис. 254. Мастер создания правил МЭ. Шаг 10

Для завершения процедуры создания правила необходимо нажать кнопку **Готово**.

Рассмотрим пример создания нового правила.

Например, требуется создание правила для запрета передачи IM-Messaging (чат) трафика по протоколу ICQ.

Во вкладке *Межсетевой экран* выбрать категорию **Правила МЭ** и, щелкнув правой кнопкой мыши на информационном окне, в выпадающем меню выбрать **Мастер настройки**.

На шаге 1 указывается описание правила и устанавливается действие для правила «Запретить».

Для того, чтобы правило не распространялось на HTTPS (SSL) трафик, требуются уточнения. На шаге 3 добавляется протокол IPv4 с указанием «Внешний IP-адрес» и соответствующий адрес (получить IP-адрес DNS-имени login.icq.com можно через меню **Пуск** → **Выполнить** → **nslookup.exe.**). Далее на шаге 4 в списке протоколов указывается нужный тип протокола *TCP/UDP*. Далее на шаге 5 происходит настройка параметров выбранного протокола. Указывается внешний TCP порт «5190, 443», так как ICQ предусматривает работу с серверами по порту 5190 и, в случае безопасного подключения, по порту 443.

Конкретизированное правило будет работать только при точном совпадении указанных настроек. Правило, конкретизированное для протокола ICQ, сервера login.icq.com и клиента Miranda — не будет работать при любом несовпадении. Например, в случае если используется официальный клиент ICQ либо какой-то нестандартный сервер или порт. Конкретизированные правила удобны возможностью запретить всю работу по указанному протоколу, разрешая только определенный набор функций. Например, разрешить только работу с официальным сервером ICQ, только определенному пользователю и только с использованием определенного клиента. При создании такого разрешающего правила с детальными параметрами необходимо следующим правилом или правилом по умолчанию заблокировать трафик с отличными от указанных параметров.

IP-адреса, на которые ссылаются DNS-имена, могут изменяться. Также есть ситуации, когда для одного DNS-имени указываются несколько IP-адресов — в этом случае в графе «Внешний IP-адрес» на шаге 3 необходимо указать диапазон адресов, или их перечисление через запятую, например, «217.69.139.70, 94.100.180.70» для DNS-имени www.mail.ru (на момент написания данного руководства).

В случае **одновременного** задания нескольких параметров для одного протокола, например, одновременного задания пар «Локальный IP-адрес» **и** «Внешний IP-адрес» — для срабатывания правила должны выполниться **оба условия**. Это актуально и при указании пар «Локальный порт» и «Внешний порт» для протокола TCP: при указанном локальном порте 1025 и удаленном 80 правило работает для HTTP (80/TCP) трафика ТОЛЬКО в случае, если локальный порт равен 1025.

«Логическое И» действует между параметрами одного протокола, например, в случае протокола IPv4 логическое «И» действует с «Локальным» и «Внешним» адресом, в случае указания портов (TCP или UDP) — точное соответствие локальных и внешних портов (TCP и отдельно между собой UDP соответственно) и т. д.

Для правил *по умолчанию*, работоспособность которых зависит от параметра **Доверенные правила МЭ**, добавлен индикатор, который указывает на то, будет ли работать данное правило.
Черный индикатор указывает на то, что правило работать не будет, так как включены *Доверенные правила МЭ* (рис. 255). Если выключить доверенные правила, индикатор будет зеленым (в случае действия **Разрешить**) или красным (в случае **Запретить**).
В других правилах, которые не пересекаются с доверенными, данный индикатор не отображается.

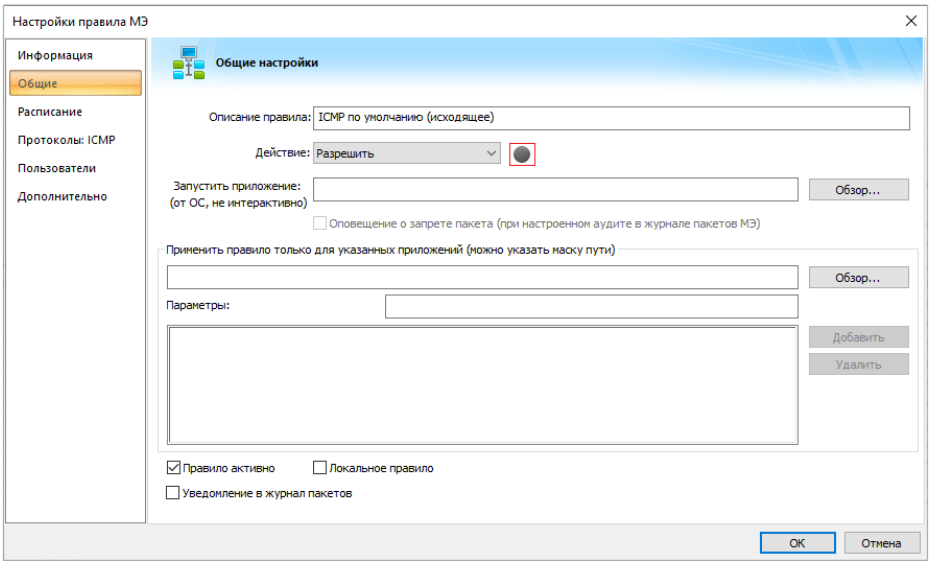


Рис. 255. Черный индикатор правила МЭ

15.2.6 Профили МЭ

Данная категория настроек представляет собой совокупность состояний правил **МЭ** (активировано/деактивировано) и значение для правила по умолчанию.

Для перехода к управлению профилей необходимо открыть вкладку *МЭ* и выбрать категорию **Профили МЭ**.

В профиль правил **МЭ** входят правила:

- правило по умолчанию,
- общие правила **МЭ**.

Предустановленные профили:

- «По умолчанию»,
- «Безопасная среда»;
- «Изоляция узла».

Профиль *Безопасная среда*, активируется по умолчанию при запуске любого приложения в режиме БС.

Профиль *Изоляция узла*, предоставляет возможность логически отделить компьютер от сети передачи данных с сохранением управления со стороны **ЕЦУ**. По умолчанию этот профиль отключен, но активируется при выполнении следующих условий:

- отсутствует антивирусное программное обеспечение;
- зафиксировано нарушение целостности контролируемых объектов;
- обнаружены действия, характерные для вирусов-шифровальщиков.

Для перехода к управлению правилами необходимо открыть вкладку *МЭ* и выбрать категорию **Профили МЭ** (рис. 256).

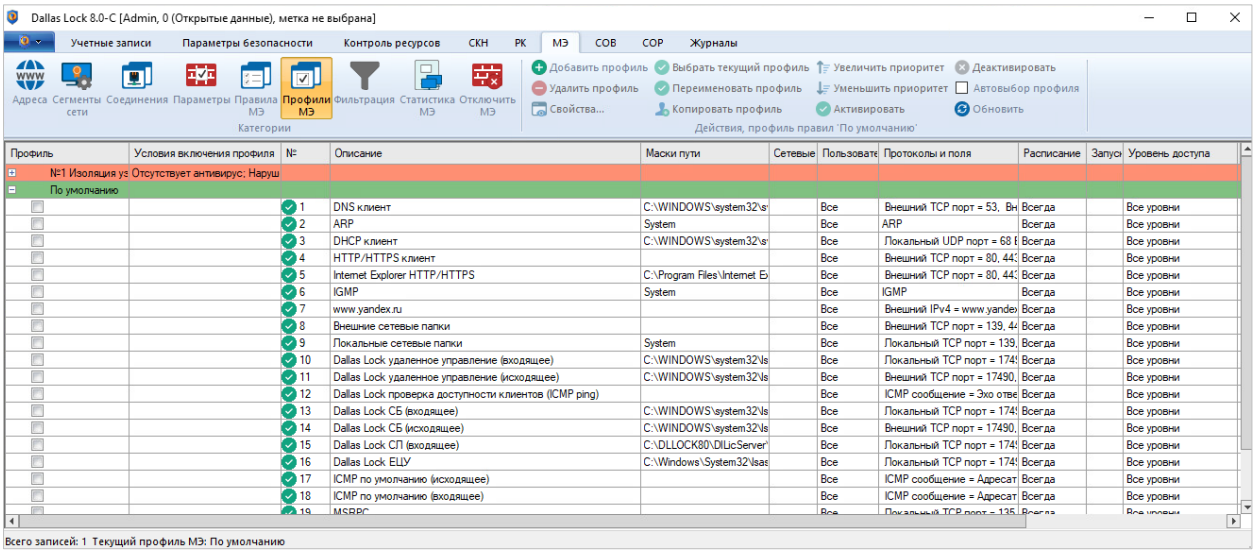


Рис. 256. Панель настройки профилей межсетевого экрана

На информационной панели находится список профилей, каждый из которых представляет из себя таблицу с полями:

- профиль («№*Приоритет профиля* *Имя профиля*» — для профилей с условием включения», «*Имя профиля*» — для ручных профилей);
- список условий включения профиля.

Для каждого профиля список правил **МЭ** одинаковый, но может быть индивидуально настроен. Чтобы посмотреть список правил **МЭ** с их настройками для конкретного профиля, нужно нажать на символ «+», находящийся слева от названия этого профиля. Список представляет из себя таблицу с полями (рис. 257):

- статус правила **МЭ** (активно/деактивировано), управление которым осуществляется путем переключения чекбокса, либо кнопками **Активировать**/**Деактивировать** на панели **Действия**;
- № правила **МЭ**;
- основные данные по ресурсам и пользователям, для которых они назначены: маски пути, сетевые интерфейсы, драйверы протоколов, пользователи и т. д.

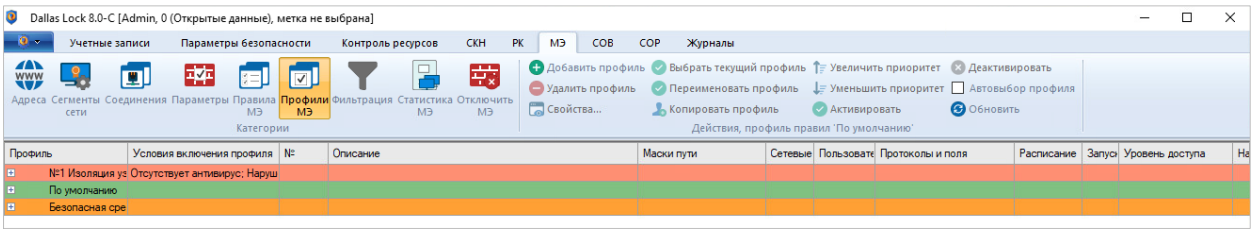


Рис. 257. Профили МЭ

Изменение параметров правил **МЭ** в режиме редактирования профилей **МЭ** невозможно. При выборе правила **МЭ** и нажатии кнопки **Свойства** на панели **Действия**, доступна только информация о настроенных для правила **МЭ** параметрах.

Для выбора условий включения профиля, необходимо выбрать его в таблице, нажать кнопку **Свойства** на панели **Действия** и перейти на вкладку *Общие* (рис. 258).

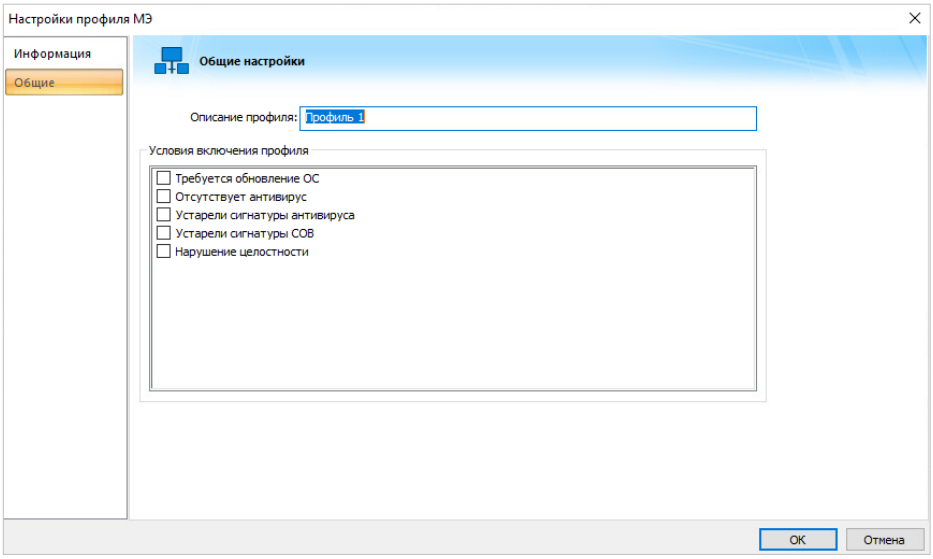


Рис. 258. Настройка автоматического включения профиля

Доступны следующие условия включения профиля:

- Требуется обновление ОС.
- Отсутствует антивирус.
- Устарели сигнатуры антивируса.
- Устарели сигнатуры СОВ.
- Нарушение целостности.
- Защита от вирусов-шифровальщиков.

При выборе нескольких условий включения профиля действует правило «ИЛИ», т. е. при срабатывании любого из выбранных условий — активируется профиль.

Каждое условие включения может принадлежать нескольким профилям, но при одинаковых условиях у разных профилей, должен сработать профиль с наивысшим приоритетом.

Если для профиля не указаны условия включения, то данный профиль считается ручным и переключается только по команде администратора кнопкой «Переключить профиль» на панели «Действия». После переключения профиля необходимо нажать кнопку **Обновить** на панели **Действия**.

Если ручному профилю задано хотя бы одно условие включения, ему присваивается самый низкий приоритет.

Для изменения приоритета профиля необходимо выбрать этот профиль и нажать кнопку **Увеличить приоритет** / **Уменьшить приоритет** на панели действия (рис. 259).

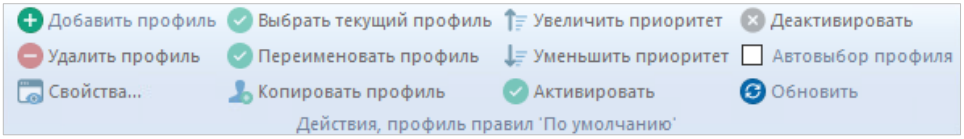


Рис. 259. Панель «Действия»

На панели **Действия** расположен параметр **Автовыбор профилей**, предназначенный для автоматического включения профилей в соответствии приоритетам и условиям включения. По умолчанию параметр отключен.

При отключенном параметре **Автовыбор профилей** доступны любые изменения списков профилей **МЭ** и правил **МЭ** (кроме редактирования правила в категории **Профиля МЭ**), в том числе их статус.

При автоматическом переключении профиля **МЭ** на клиенте появляется всплывающее уведомление на панели задач (рис. 260).

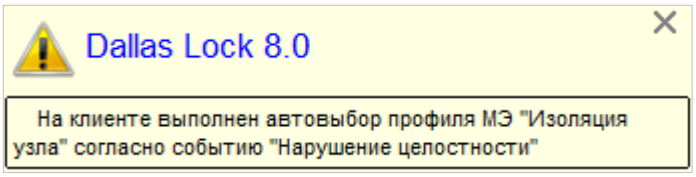


Рис. 260. Автопереключение профиля МЭ при срабатывании условия

При включенном параметре **СОВ → Параметры СОВ → Глобальные параметры → Маскирование датчика СОВ → Вкл.**, всплывающее уведомление об автопереключении профиля на клиенте не появляется.

После нейтрализации условий включения профиля выполняется автоматическое переключение на профиль **По умолчанию**.

При попытке смены профиля после его автоматического переключения появляется предупреждающее диалоговое окно о том, что для переключения необходимо отключить параметр **Автовыбор профиля** (рис. 261).

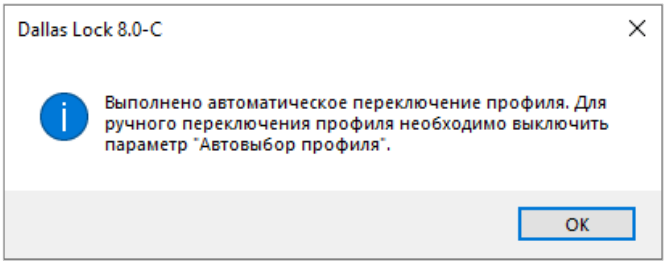


Рис. 261. Ручное переключение профиля при активном параметре «Автовыбор профилей»

Название текущего профиля **МЭ** отображается на нижней части панели в категориях **Профили МЭ** и **Правила МЭ** (рис. 262).

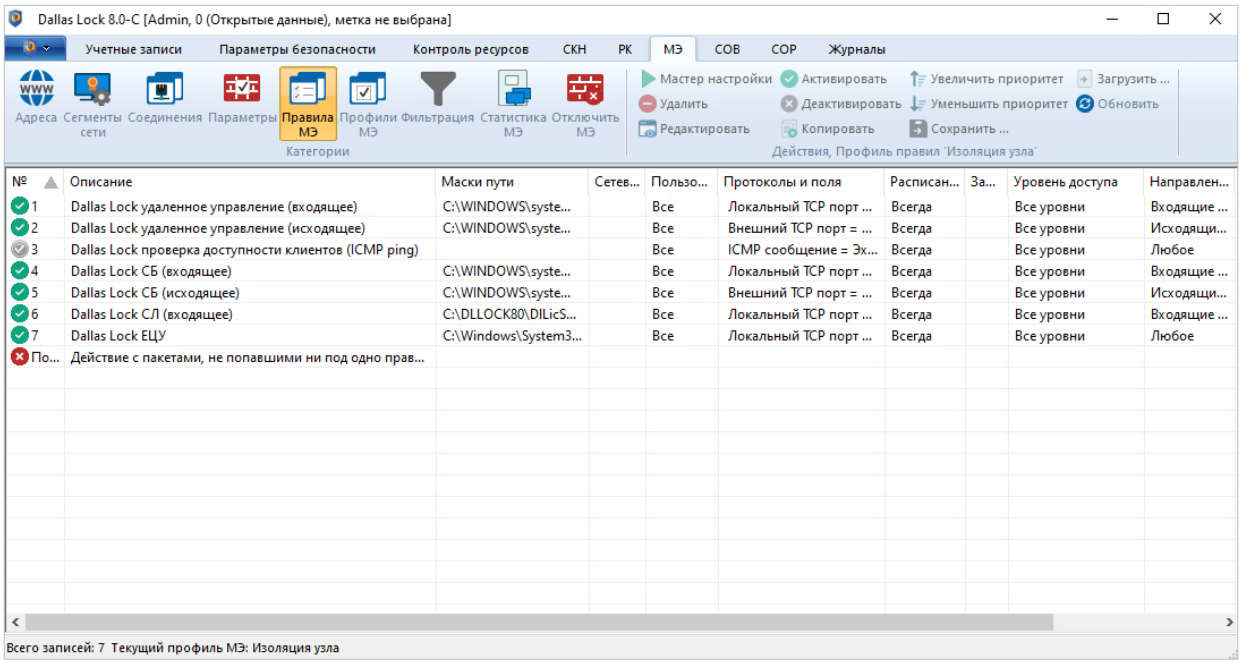


Рис. 262. Текущий профиль МЭ

15.2.7 Фильтрация

Посредством фильтрации возможно контролировать сетевой трафик по его содержимому (анализируется присутствие известных протоколов, медиа-контента и мобильный код) во всем фильтруемом трафике.

При установленном антивирусе для работы механизма фильтрации необходимо добавить файл «C:\DLLOCK80\DlIpsService.exe» в список исключений антивируса.

Настройки фильтрации

В данной категории доступны настройки фильтрации **МЭ** (рис. 263).

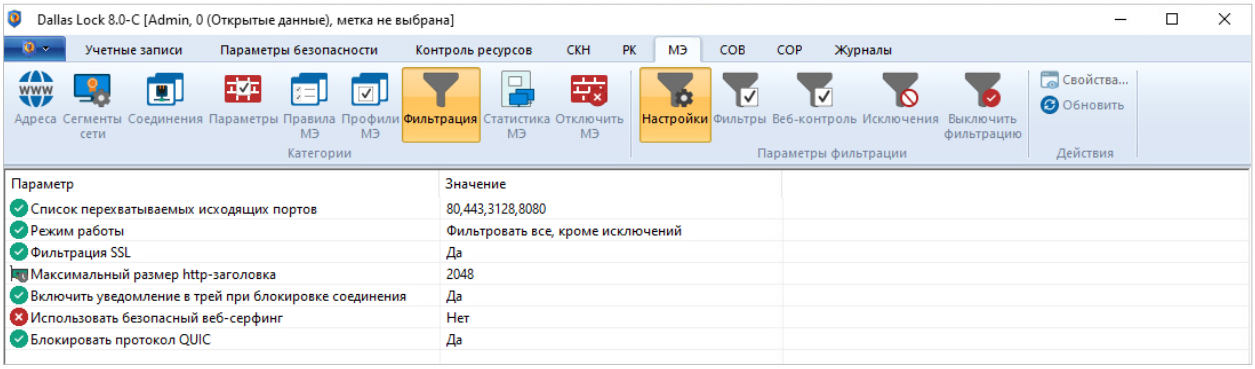


Рис. 263. Настройки фильтрации

Управление параметрами осуществляется на панели **Действия** через нажатие кнопки **Свойства** при выбранной строке параметра или посредством нажатия правой кнопки мыши и выборе в контекстном меню **Свойства** интересующего пункта редактирования параметров безопасности.

Список перехватываемых исходящих портов

Параметр позволяет задать список перехватываемых исходящих портов для фильтрации трафика. По умолчанию имеет значение: 80, 443, 3128, 8080. Диапазон портов указывается через «,», «-», также можно использовать слово «any» для указания всех портов. Анализ трафика ведется только для соединений, проходящих по указанным портам.

Смена настроек, связанных с формированием списка перенаправлений (Сегменты сети МЭ, Параметры МЭ/СОВ, Фильтрация МЭ, Сигнатуры трафика СОВ), приводит к освобождению всех ресурсов, занятых службой фильтрации, повторному созданию потоков и привязке портов для нового списка.

При возникновении ошибок в процессе формирования перенаправлений служба показывает всплывающее окно и добавляет запись в журнал политик.

Режим работы

Данный параметр позволяет выбрать режим работы фильтрации относительно добавленных исключений. Доступно два режима:

- фильтровать все, кроме исключений;
- фильтрация активна только для хостов-исключений. Фильтрация будет применяться только к добавленным исключениям.

Фильтрация SSL

Данный параметр позволяет осуществлять фильтрацию в том числе для HTTPS (SSL) соединений. При включении данного параметра осуществляется внедрение в HTTPS трафик и анализ трафика прозрачно для пользователя путем подмены SSL сертификата.

При включении параметра «Фильтрация SSL» возможно проявление конфликтов со сторонним ПО, детально проверяющим принадлежность своего SSL сертификата, например:

- блокировка скачивания обновлений ПО/

Для решения подобной проблемы необходимо добавить URL серверов обновлений ПО в список исключений (хосты из списка исключений не подвергаются подмене сертификата, при установленном режиме работы **Фильтровать все, кроме исключений**).

В целях обеспечения бесперебойного получения обновлений ОС служба обновлений ОС Windows исключена из анализа SSL трафика (подмена сертификата Microsoft не осуществляется) в любом режиме работы Фильтрации **МЭ**.

Инсталляторы некоторых приложений, чувствительных к подмене сертификата, могут не работать при включенном анализе SSL, поэтому для установки этих приложений нужно либо добавлять исключения, либо на время установки выключать анализ SSL.

Максимальный размер http-заголовка

Данный параметр позволяет осуществлять фильтрацию с целью выявления аномальности HTTP-заголовка по размеру. Доступны значения максимального размера HTTP-заголовка от 2048 символов до 16 384 символов. По умолчанию параметру присвоено значение 2048.

Включить уведомление в трей при блокировке соединения

Параметр предназначен для управления всплывающими уведомлениями при блокировке соединения. По умолчанию уведомления включены.

Использовать безопасный веб-серфинг

Данный параметр позволяет осуществлять безопасный веб-серфинг. Для настройки доступны следующие параметры:

- Phishing (интернет-мошенничество с целью получения доступа к конфиденциальным данным пользователей);
- Malware (использование веб-ресурсов, предназначенное для получения НСД к вычислительным ресурсам ТС или к информации, хранимой на ТС, с целью несанкционированного использования ресурсов ТС или нанесения ущерба владельцу информации путем копирования, искажения, удаления или подмены информации);
- Adult (контент только для взрослых).

Для каждого из параметров реализован выпадающий список настроек, способный принимать значения:

- «Блокировать» — ресурс проверяется с помощью сервиса «Safe Browsing API» по списку небезопасных интернет-ресурсов (создан и поддерживается Яндексом). В случае обнаружения запрашиваемого ресурса в указанном списке производится блокировка доступа к данному ресурсу. В браузере пользователю выводится сообщение о блокировке.
- «Журналировать» — ресурс проверяется с помощью сервиса «Safe Browsing API» по списку небезопасных интернет-ресурсов (создан и поддерживается Яндексом). В случае обнаружения запрашиваемого ресурса в указанном списке блокировка доступа к данному ресурсу не производится. При этом производится соответствующая запись в журнал.
- «Отключить» — никакие действия с проверкой ресурса не осуществляются.

По умолчанию безопасный веб-серфинг не используется.

Блокировать протокол QUIC

Параметр предназначен для блокирования передачи данных по протоколу QUIC.

Предусмотрена возможность одновременной настройки нескольких фильтров с помощью множественного выделения. При этом в окне "*Свойства фильтра*" будут показаны только те действия, которые применимы ко всем выбранным фильтрам.

Фильтры

На информационной панели расположены фильтры, анализирующие присутствие известных сетевых протоколов и мобильного кода в фильтрующемся трафике (рис. 264).

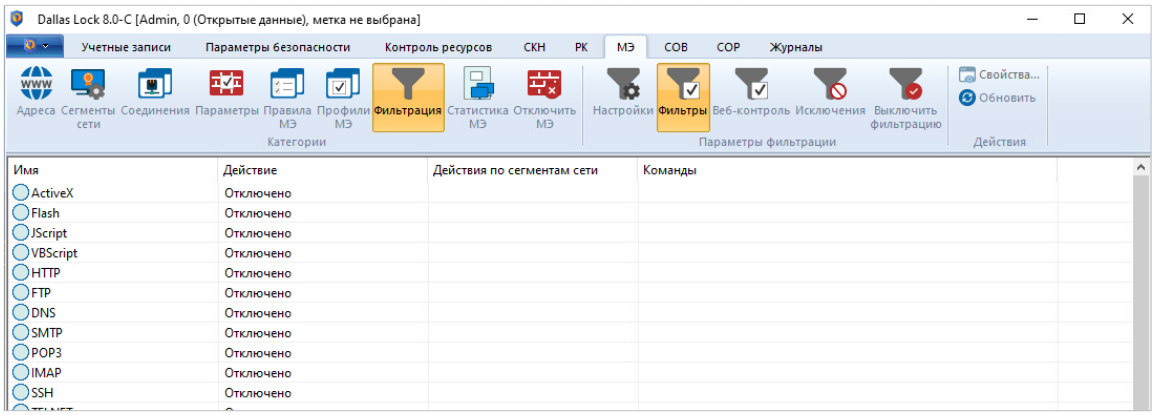


Рис. 264. Фильтры

Доступны следующие действия фильтрации для каждого отдельного фильтра:

- блокировать — при обнаружении блокируемого ресурса происходит его блокировка в браузере и событие заносится в журнал;
- вырезать — доверенному ресурсу разрешен доступ в браузере, остальные действия в браузере блокируются;
- журналировать – событие при выполнении заносится в журнал;
- отключено — выбранный фильтр отключен.

Для активации определенного фильтра нужно два раза щелкнуть левой кнопкой мыши по фильтру на информационной панели, после чего появится окно **Свойства фильтра**. Далее необходимо выбрать действие фильтра для всех сегментов сети или действия для каждого сегмента сети индивидуально, после чего нажать **ОК**.

Пример

Рассмотрим случай, когда требуется доверенный доступ к сайту «mail.ru», а для всех остальных необходимо вырезать ресурсы, содержащие мобильный код, чтобы исключить известные и неизвестные уязвимости браузеров.

Открыв категорию **Фильтрация** → **Исключения** необходимо нажать правой кнопкой на информационной панели и в контекстном меню выбрать **Добавить**. На информационной панели появится новое правило с пустым полем *URL*, где нужно ввести IP-адреса или DNS-имя соответствующего хоста или сайта. В данном случае введя «mail.ru», поле «Адрес» автоматически заполнится всеми IP-адресами, принадлежащими DNS-имени «mail.ru» (и, при необходимости, другим доверенным адресами).

Затем на вкладке **Фильтрация** → **Настройки** необходимо для параметра **Режим работы** выбрать режим **Фильтровать все, кроме исключений**.

Для фильтрации мобильного кода для всех остальных сайтов необходимо на вкладке **Фильтрация** → **Фильтры** включить фильтры мобильного кода (ActiveX, Flash, JScript, VBScript) с действием фильтра **Вырезать**.

При выполнении описанных настроек пользователю будет доступен хост «mail.ru» без ограничений, но для остального трафика фильтрация вырежет заданный мобильный код, значительно уменьшая возможность эксплуатирования уязвимостей браузеров.

После загрузки страницы веб-сервиса, в кэш браузера помещаются загруженные объекты (html-страница, flash-файл и т. п.). При последующих загрузках данной страницы веб-сервиса, flash-файл больше не будет передаваться по сети, как и html-страница. Поэтому для корректной работы фильтров необходимо очистить кэш браузера.

Для перехвата трафика по протоколу DTLS, необходимо выполнить одно из следующих действий.

1. Создать правило МЭ по блокировки протокола DTLS.

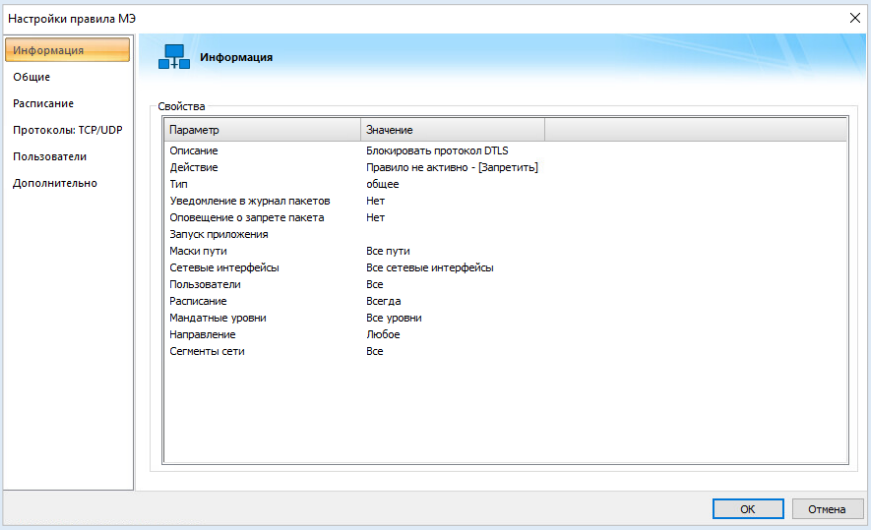


Рис. 265. Блокировка протокола DTLS (QUIC)

2. Отключить протокол в браузере на базе Chromium (например, Google Chrome, Edge Chromium) с помощью команды *//flags/#enable-quic.*

Пример: в поисковой строке Google Chrome набрать команду chrome*://flags/#enable-quic,* найти в списке строку «Experimental QUIC protocol» и отключить протокол.

Набор команд протоколов

Фильтры HTTP, SMTP, FTP, IMAP, POP3 и DNS могут осуществлять фильтрацию сетевого трафика с учетом команд протоколов. Для данных фильтров действие «вырезать» доступно, если не выбрана ни одна команда протокола.

По умолчанию кнопка **Набор команд** неактивна, однако станет доступной, если выбрано действие фильтра **Блокировать** или **Журналировать** (Рис. 266).

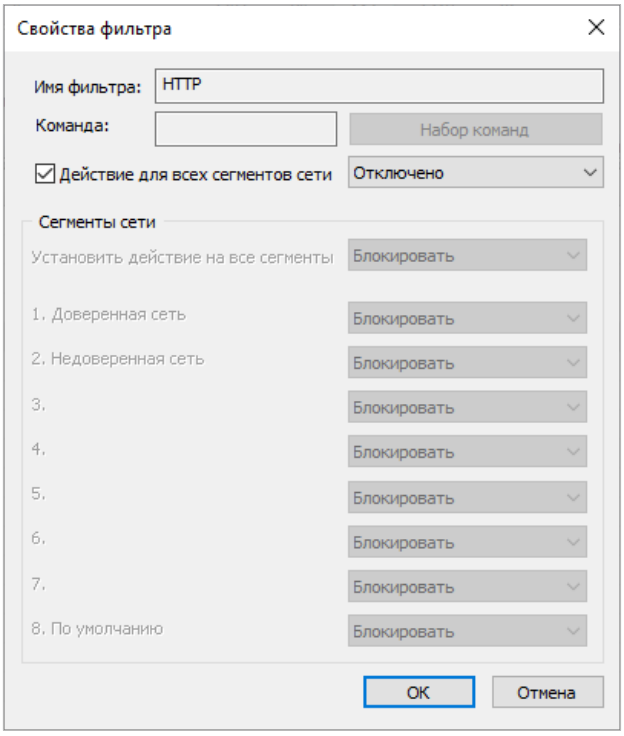


Рис. 266 Окно «Свойства фильтра»

В окне **Наборы команд** доступен выбор произвольного набора команд, функции поиска и сортировки команд (Рис. 267).

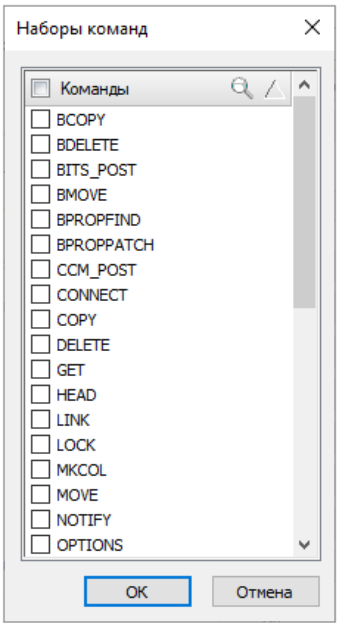


Рис. 267. Окно «Набор команд»

Таблица 12. Соотношение фильтров и доступных для них набора команд

№	Фильтр	Набор команд
1.	**HTTP**	GET, POST, PUT, SEARCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, NOTIFY, POLL, BCOPY, BDELETE, BMOVE, LINK, UNLINK, OPTIONS, HEAD, DELETE, TRACE, TRACK, CONNECT, SOURCE, SUBSCRIBE, UNSUBSCRIBE, PROPFIND, PROPPATCH, BPROPFIND, BPROPPATCH, RPC_CONNECT, PROXY_SUCCESS, BITS_POST, CCM_POST, SMS_POST, RPC_IN_DATA, RPC_OUT_DATA, RPC_ECHO_DATA
2.	**SMTP**	ATRN, AUTH, BDAT, CHUNKING, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, ONEX, QUEU, QUIT, RCPT, RSET, SAML, SEND, SOML, STARTTLS, TICK, TIME, TURN, TURNME, VERB, VRFY, X-ADAT, X-DRCP, X-ERCP, X-EXCH50, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN, XUSR
3.	**FTP**	ABOR, ACCT, ADAT, ALLO, APPE, AUTH, CCC, CDUP, CEL, CLNT, CMD, CONF, CWD, DELE, ENC, EPRT, EPSV, ESTA, ESTP, FEAT, HELP, LANG, LIST, LPRT, LPSV, MACB, MAIL, MDTM, MIC, MKD, MLSD, MLST, MODE, NLST, NOOP, OPTS, PASS, PASV, PBSZ, PORT, PROT, PWD, QUIT, REIN, REST, RETR, RMD, RNFR, RNTO, SDUP, SITE, SIZE, SMNT, STAT, STOR, STOU, STRU, SYST, TEST, TYPE, USER, XCUP, XCRC, XCWD, XMAS, XMD5, XMKD, XPWD, XRCP, XRMD, XRSQ, XSEM, XSEN, XSHA1, XSHA256
4.	**IMAP**	APPEND, AUTHENTICATE, CAPABILITY, CHECK, CLOSE, COMPARATOR, COMPRESS, CONVERSIONS, COPY, CREATE, DELETE, DELETEACL, DONE, EXAMINE, EXPUNGE, FETCH, GETACL, GETMETADATA, GETQUOTA, GETQUOTAROOT, IDLE, LIST, LISTRIGHTS, LOGIN, LOGOUT, LSUB, MYRIGHTS, NOOP, NOTIFY, RENAME, SEARCH, SELECT, SETACL, SETMETADATA, SETQUOTA, SORT, STARTTLS, STATUS, STORE, SUBSCRIBE, THREAD, UID, UNSELECT, UNSUBSCRIBE, X
5.	**POP3**	APOP, AUTH, CAPA, DELE, LIST, NOOP, PASS, QUIT, RETR, RSET, STAT, STLS, TOP, UIDL, USER
6.	**DNS**	A, AAAA, CNAME, SRV, TXT, SOA, NS, PTR

Если при активации фильтра указаны одна или несколько команд протоколов, то фильтрация сетевого трафика по данному фильтру будет производиться по протоколу с учетом выбранных команд. Фильтр будет применяться, если хотя бы одна из выбранных команд протокола будет присутствовать в сетевом трафике.

Срабатывание фильтров с поддержкой команд протоколов HTTP, SMTP, FTP, IMAP, POP3 и DNS регистрируется в **Журнале трафика** аналогично другим фильтрам, используемым в **DL 8.0**.

Пример

Администратору безопасности необходимо блокировать возможность копирования файлов в облачные хранилища (Google Диск, Яндекс Диск).

Для этого необходимо открыть категорию **Фильтрация** → **Параметры фильтрации** → **Фильтры**. Далее необходимо открыть фильтр *HTTP*, выбрать действие **Блокировать** и нажать на кнопку **Набор команд**. Из списка доступных команд выбрать *POST* и нажать на кнопку **ОК**.

В результате канал утечки файлов через облачные хранилища (Google Диск, Яндекс Диск) будет заблокирован. При этом необходимо учитывать, что это может повлиять на работу других приложений, требующих использования команды *POST* протокола *HTTP* (Рис. 268).

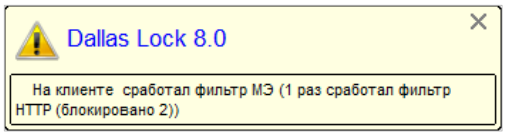


Рис. 268. Сообщение о блокировке

Веб-контроль

Принцип управления веб-контроля аналогичен принципу работы правил **МЭ**. Необходимо создать набор правил, которые могут быть запрещающими, разрешающими или информирующими. В правилах веб-контроля указывается на какие URL-адреса они действуют, к какому содержимому и для каких пользователей применяются. Правила проверяются в заданном порядке, после срабатывания правила, проверка прекращается. Если ни одно из существующих правил не сработало, применяется правило по умолчанию. После обработки правил веб-контроля возможны следующие события:

- доступ к запрошенной информации с сервера,
- уведомление пользователя о блокировке веб-ресурса,
- предупреждение о нежелательном доступе к запрошенному веб-ресурсу.

Для перехода к управлению правилами веб-контроля необходимо открыть подкатегорию **МЭ** → **Фильтрация** → **Веб-контроль**.

На информационной панели находится список правил веб-контроля и основные данные по ресурсам и пользователям, для которых они назначены: расписание, приложения, сайты, типы данных, ключевые слова и т. д. (рис. 269).

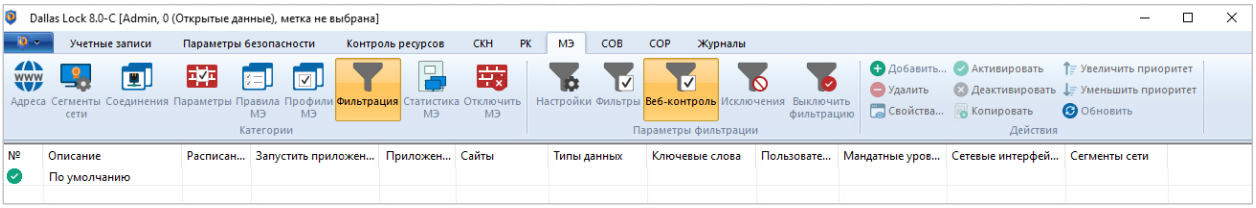


Рис. 269. Панель настройки правил веб-контроля

Существует возможность создания правила и копирования уже имеющегося, удаления, просмотра свойств и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

При создании правила веб-контроля появится окно **Создание правила веб-контроля** в котором доступно 6 разделов.

В разделе *Информация* отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 270). В версии «С» раздел *Информация* дополнен параметром **Мандатный уровень**, информирующий о том, для каких мандатных уровней применяется правило (параметр доступен только для Dallas Lock 8.0 редакции «С»).

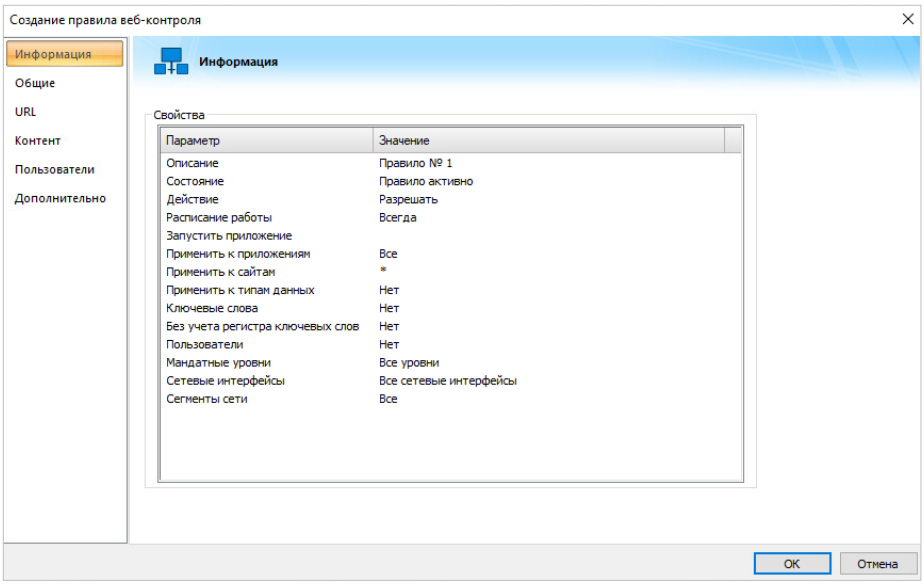


Рис. 270. Информация о правиле веб-контроля

В разделе *Общие* представлены основные настройки правила веб-контроля (рис. 271).

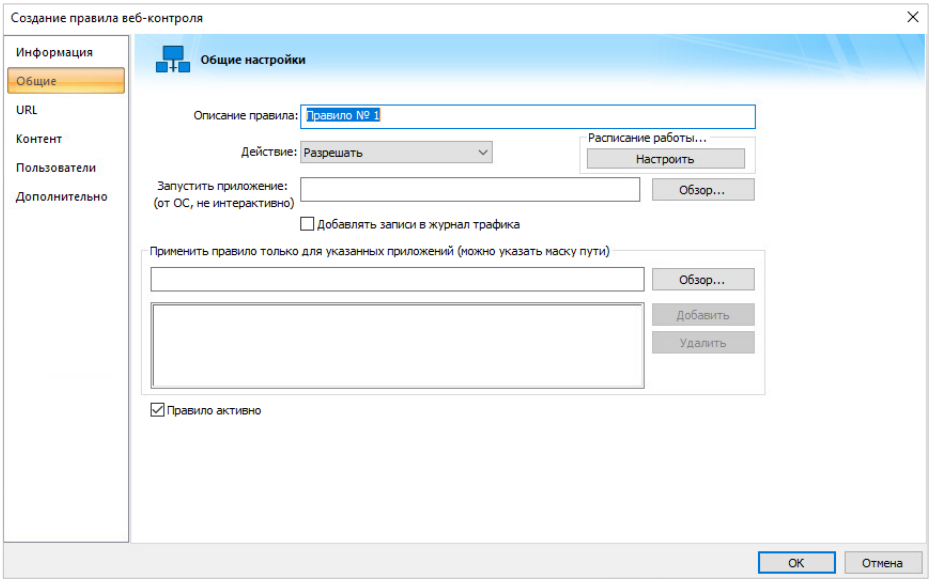


Рис. 271. Общие настройки правила веб-контроля

Если был задан параметр **Запустить приложение**, то при срабатывании правила, приложение запустится от имени ОС и не интерактивно. Данный параметр не привязан к пользователям и служит для расширения автоматической реакции на события.

В разделе *URL* можно задать URL-адреса веб-ресурсов, к которым будет применяться данное правило (рис. 272). URL-адрес должен быть задан в формате:

<хост>[/<URL-путь>][?<параметры>]<якорь>

Допускается использование символа маски «*», который заменяет любую последовательность символов, например, «mail.ru*». Список URL-адресов возможно загрузить из файла, если предварительно он был составлен и сохранен.

Составленный список URL-адресов должен быть сохранен в кодировке UTF-8 без маркера последовательности байтов (Byte Order Mark).

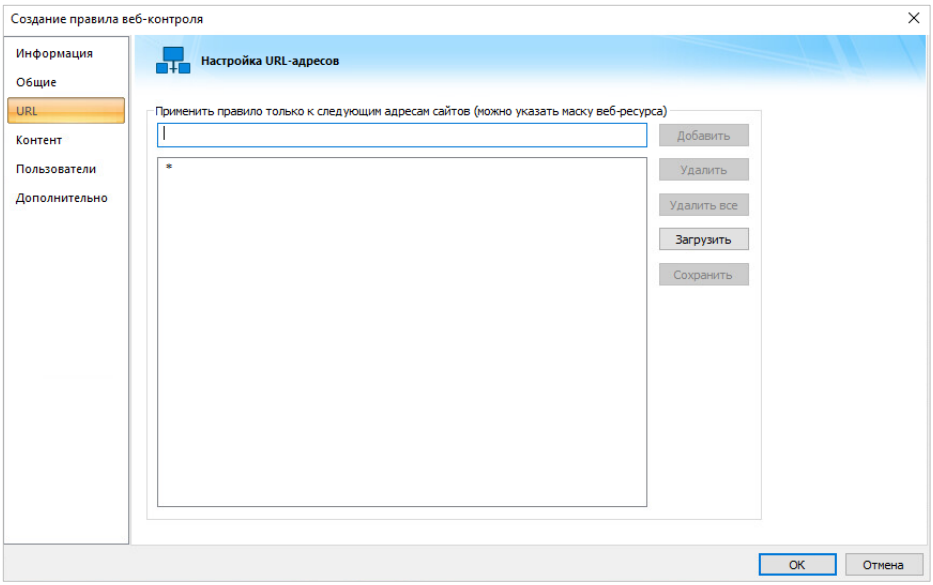


Рис. 272. URL-адреса

Раздел «Контент» позволяет настроить контроль доступа пользователей к веб-ресурсам по типам данных и ключевым словам, предотвращая показ нежелательного содержимого (рис. 273).

При фильтрации по типу данных (видео, звуковые файлы и т. д.) правило применяется ко всем веб-ресурсам, которые содержат любой из выбранных типов.

При фильтрации по ключевым словам, как правило применяется ко всем веб-ресурсам, которые содержат любое из введенных ключевых слов. Например, при наличии ключевых слов «открытые вакансии» и «калейдоскоп» для блокирования будет достаточно нахождения слова «калейдоскоп» или полного сочетания «открытые вакансии». Список ключевых слов возможно загрузить из файла, если предварительно он был составлен и сохранен. Возможна фильтрация ключевых слов без учета регистра.

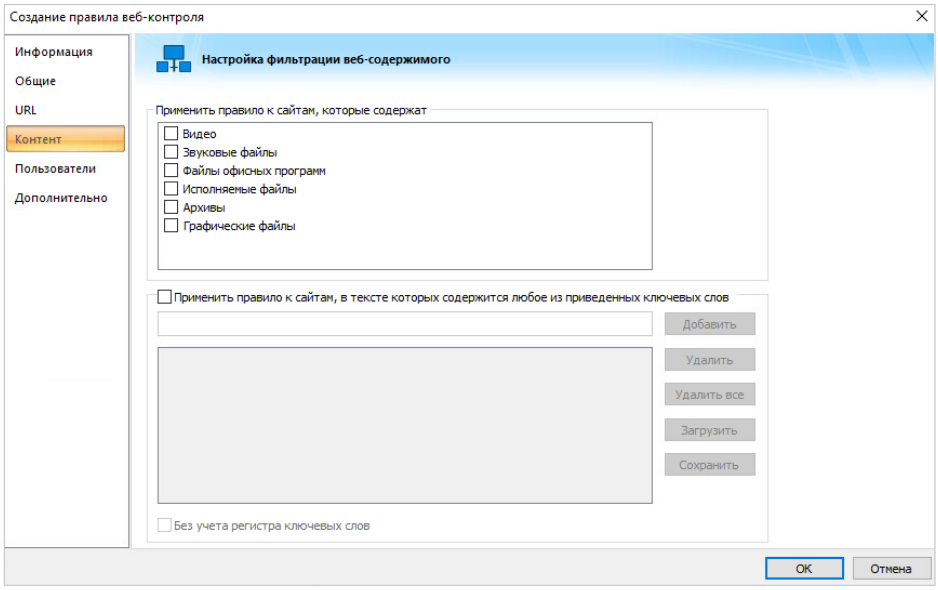


Рис. 273. Настройка блокируемого контента

В разделе «Пользователи» отображается список пользователей, к которым будет применяться созданное правило.

Отметив пункт *Автоматический поиск пользователей/групп* при последующем нажатии кнопок **Пользователи** и **Группы** будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки «Все» все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки **Удалить** (рис. 274). Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (параметр доступен только для Dallas Lock 8.0 редакции «С»).

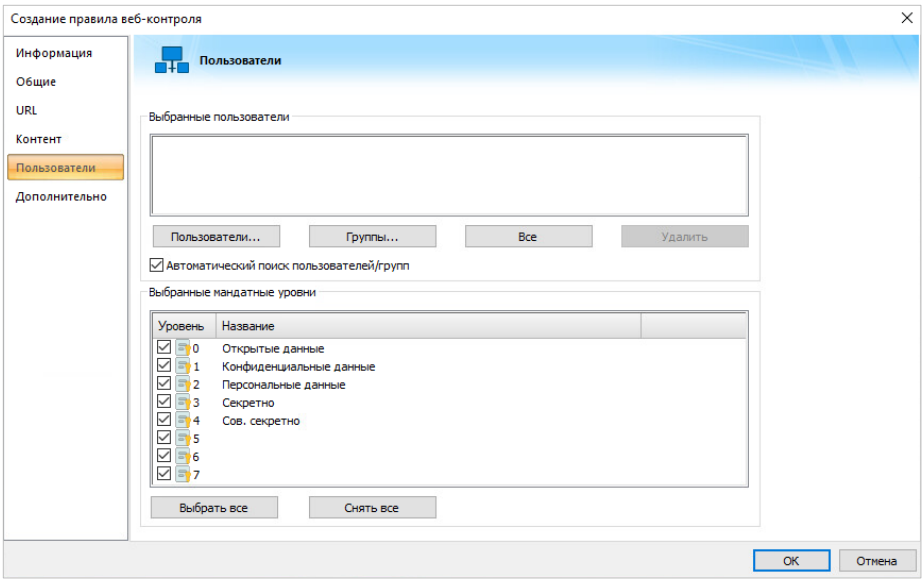


Рис. 274. Пользователи для правила веб-контроля

В разделе *Дополнительно* существует возможность применения текущего правила **МЭ** только для определенных сетевых адаптеров и (или) сегментов сети. Для редактирования списка адаптеров нужно выбрать из списка соответствующий адаптер и нажать кнопку **Добавить**. Удаление производится выбором адаптера из списка и нажатием кнопки **Удалить**. Для редактирования списка сегментов сети правила **МЭ** необходимо отметить сегменты сети (рис. 275).

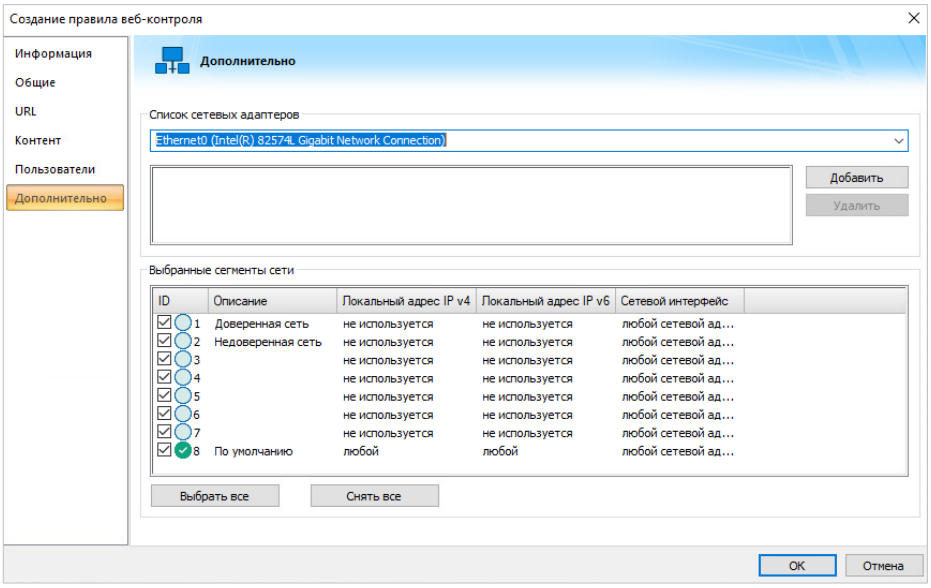


Рис. 275. Дополнительно

Для перехвата веб-контента необходимо выполнить одно из следующих действий.

1. Создать правило **МЭ** по блокировки протокола DTLS.

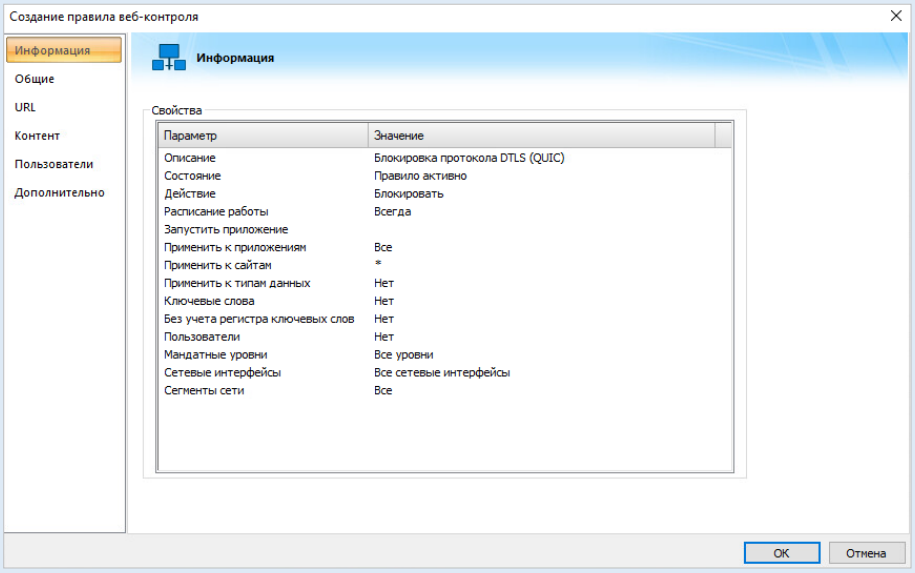


Рис. 276. Блокировка протокола DTLS (QUIC)

2. Отключить протокол DTLS в браузере на базе Chromium (например, Google Chrome, Edge Chromium) с помощью команды *//flags/#enable-quic.*

Пример: в поисковой строке Google Chrome набрать команду chrome*://flags/#enable-quic,* найти в списке строку «Experimental QUIC protocol» и отключить протокол.

Исключения

Исключения необходимы для работы с указанными хостами вне зависимости от настроенной фильтрации при режиме работы **Фильтровать все, кроме исключений** (рис. 277). При режиме работы «Фильтрация активна только для хостов-исключений», фильтрация будет применяться только к указанным в исключениях хостам.

Для создания правила исключения, необходимо выбрать действие **Добавить**, после чего на информационной панели появится новое правило с пустым полем, где необходимо ввести IP-адрес или DNS-имя, с указанием порта.

Для поддержания актуальных адресов хостов исключений, адреса исключений периодически обновляются.

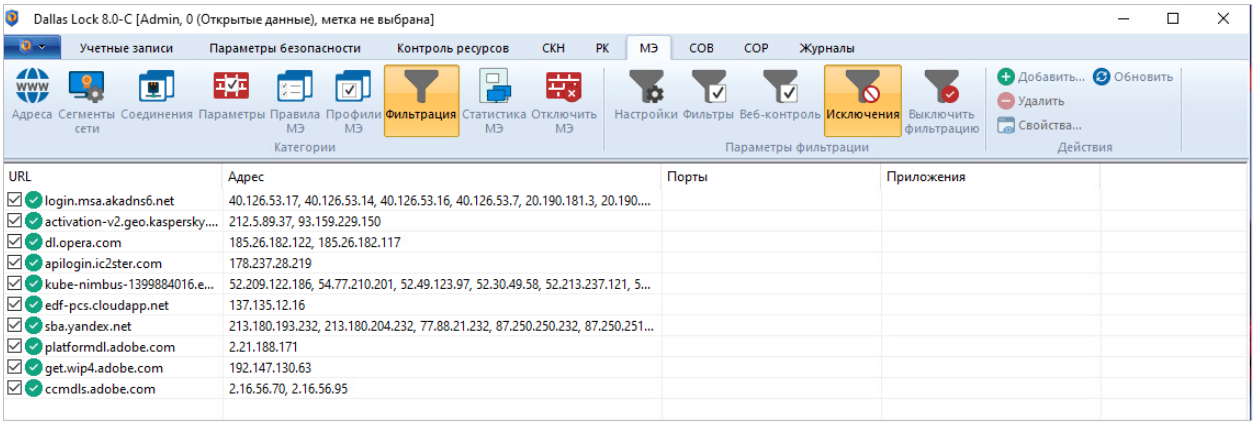


Рис. 277. Исключения фильтрации

Для того, чтобы удалить исключения нужно, выделив правило, нажать правой кнопкой мыши и выбрать в контекстном меню действие **Удалить**.

Выключение фильтрации

Для временного прекращения фильтрации **МЭ** необходимо нажать кнопку **Выключить фильтрацию** на вкладке *Фильтрация* и в появившемся окне подтвердить действие (рис. 278).

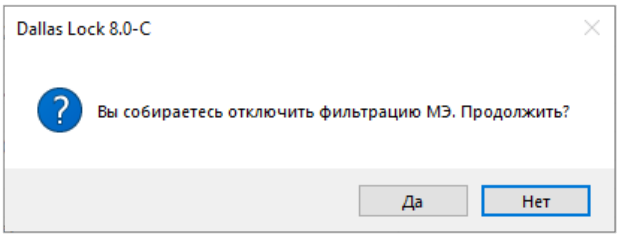


Рис. 278. Отключение фильтрации МЭ

15.2.8 Статистика МЭ

В категории **Статистика МЭ** содержится информация о принятом и отправленном трафике за указанный период. Полученные данные можно обновить и сбросить посредством нажатия соответствующих кнопок на панели **Действия**. Справа от панели находится диаграмма, отображающая статистику всего входящего и исходящего трафика с указанием количества информации и времени, когда она была получена.

Весь трафик

Параметр **Весь трафик** отображает объем информации, полученный за сутки, неделю, месяц или весь период работы **Dallas Lock**.

При ознакомлении с данными статистики нужно принимать во внимание то, что учет трафика производится с начала суток (00 часов 00 минут), с начала недели (понедельник), с первого дня месяца (1-е число отчетного месяца).

Для отображения информации нужно нажать кнопку **Весь трафик** на панели **Параметры статистики**. Панель действий включает в себя опции обновления и сброса текущей информации (рис. 279).

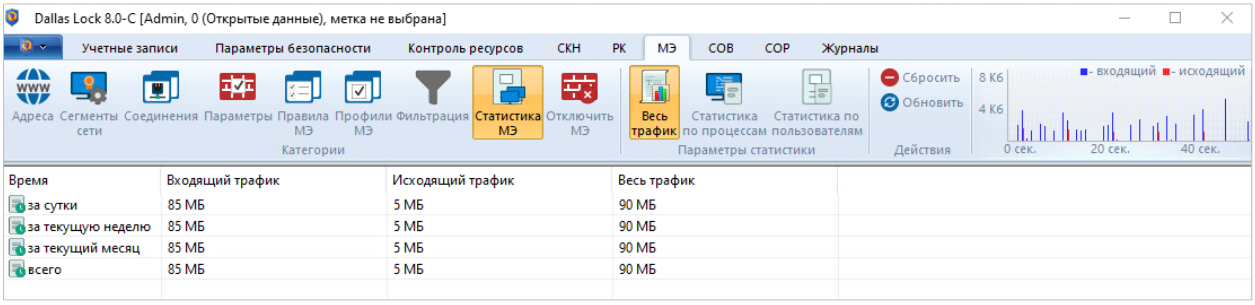


Рис. 279. Статистика межсетевого экрана

Статистика по процессам

В параметре **Статистика по процессам** отображается трафик, использованный рабочими процессами, с указанием отчетного периода (рис. 280).

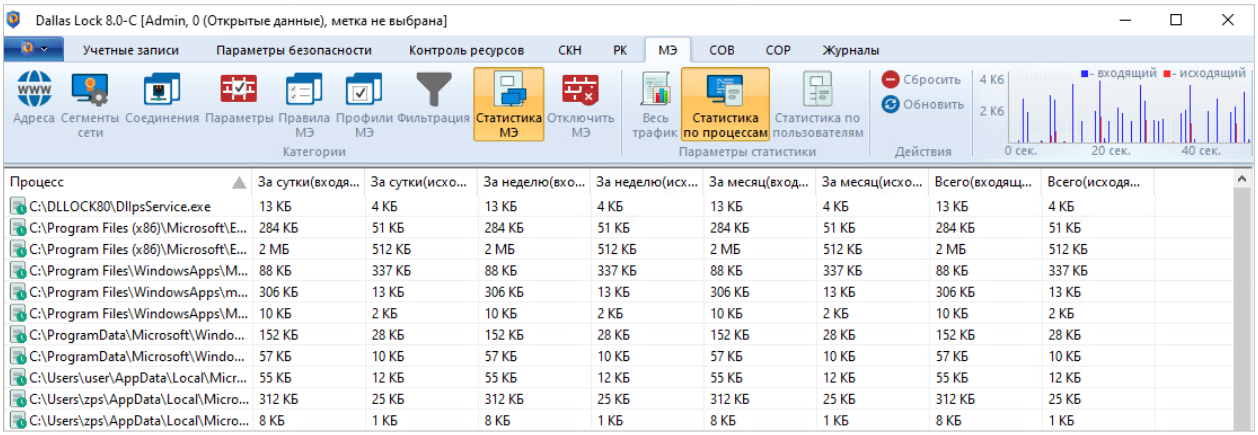


Рис. 280. Статистика по процессам

Статистика по пользователям

Статистика по пользователям показывает, сколько было отправлено/принято трафика во время работы каждого системного процесса за отчетный период (рис. 281).

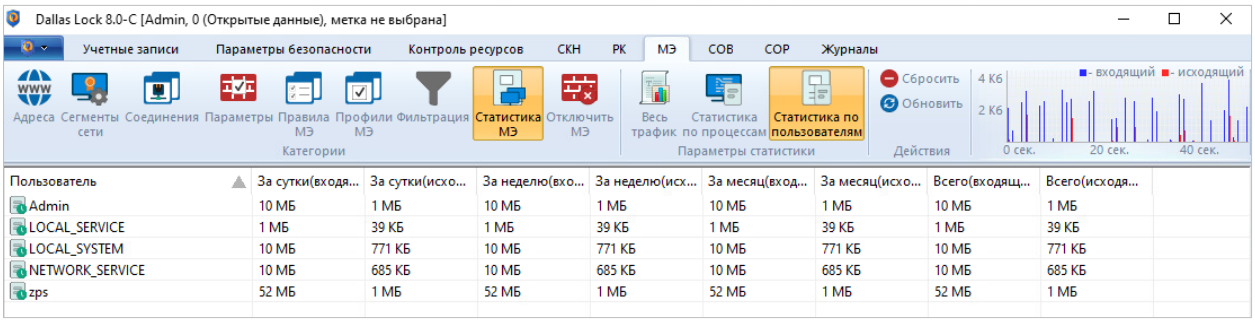


Рис. 281. Статистика по пользователям

15.2.9 Отключение МЭ

Для временного прекращения работы **МЭ** необходимо нажать кнопку **Отключить МЭ** и в появившемся окне подтвердить действие (рис. 282).

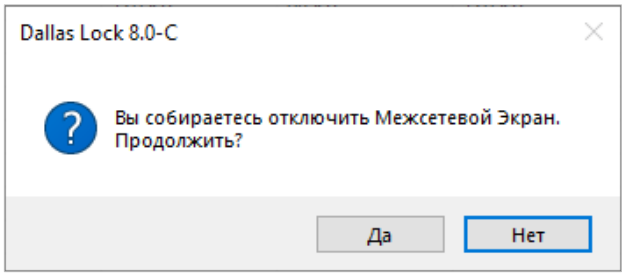


Рис. 282. Отключение межсетевого экрана

15.3 Журналы МЭ

В **Dallas Lock 8.0** реализована функция сбора и отображения информации о сетевых пакетах и установленных соединениях ТС (или компьютера).

Для того, чтобы ознакомиться с данной информацией, нужно открыть общую вкладку *Журналы* и выбрать **Журнал пакетов МЭ** или **Журнал соединений МЭ** или **Журнал трафика фильтрации МЭ**. По умолчанию журналы отключены, и сбор информации не ведется.

На панели **Действия** расположено три кнопки. При нажатии кнопки **Обновить** отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах **МЭ**, нужно нажать кнопку **Архивировать**. После этого в папке программы появится файл с архивом данных. Для открытия такого файла нужно использовать категорию **Журнал из файла** и в ее окне на панели действий нажать кнопку **Открыть журнал**, а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Кнопка **Экспорт** отвечает за сбор и конвертирование информации журналов межсетевого экрана в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку **Экспорт**, указать имя файла и выбрать место для его хранения.

При открытии **Журнала из файла**, в окне выбора файлов возможно выбрать несколько журналов одного типа. При выборе разных типов появится сообщение об ошибке.

Для начала фиксирования и отображения информации в журналах **МЭ** необходимо внести уточнения в параметры. Настройки журналов **МЭ** находятся во вкладке **Параметры безопасности → Политики аудита** и задаются через четыре параметра (рис. 283).

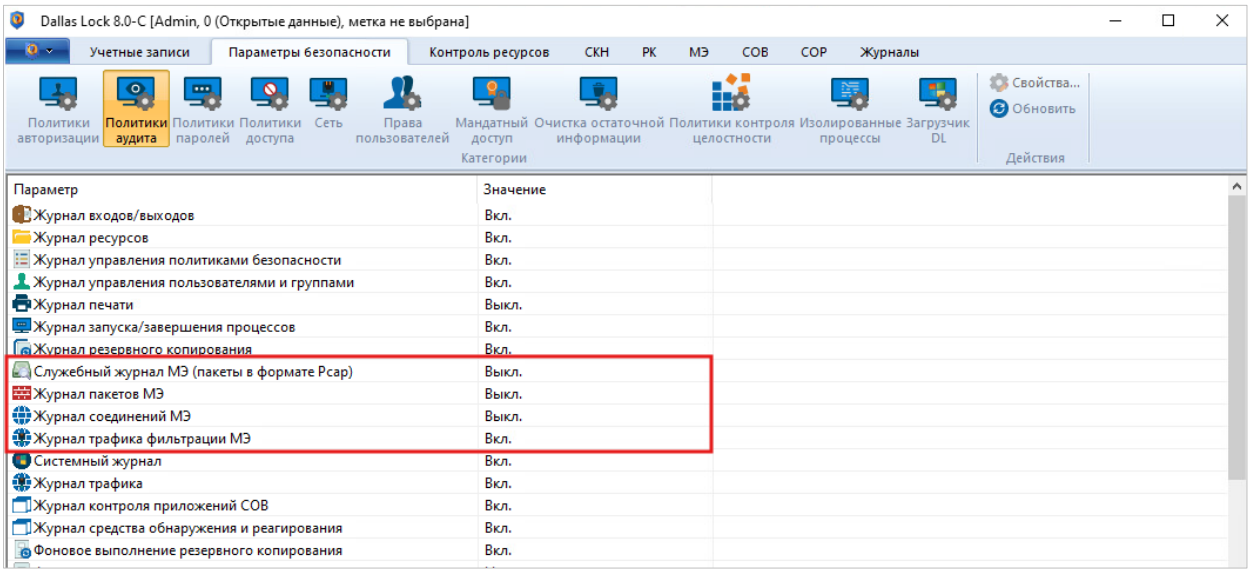


Рис. 283. Основные параметры работы журналов

15.3.1 Служебный журнал

Служебный журнал нужен для создания файла со списком всех зафиксированных пакетов в формате pcapng, в случае возможных проблем детектирования пакетов и может понадобиться при обращении в службу технической поддержки.

Чтобы включить служебный журнал **МЭ**, необходимо нажать правой кнопкой мыши на параметре **Служебный журнал МЭ (пакеты в формате Pcap)** и в появившемся окне выбрать пункт «*Вкл.*» и нажать кнопку **ОК** (рис. 284).

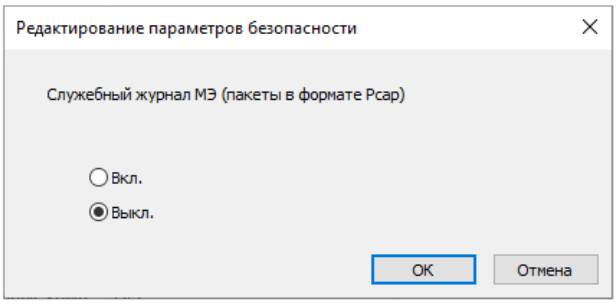


Рис. 284. Отключение ведения служебного журнала

Журнал располагается в папке DL, например, «C:\DLLOCK80\Firewall\Logs» и его имя может зависеть от названия используемого сетевого адаптера. Например, имя файла журнала может быть таким «C:\DLLOCK80\Firewall\Logs\VMware_Accelerated_AMD_PCNet_Adapter 2015-04-30.pcapng».

Данный журнал необходимо включать только в случае возможных проблем детектирования пакетов, иначе будет проводиться слишком подробный аудит, что может привести к росту объема лог-файлов и уменьшению свободного места на жестком диске, а также к падению производительности работы в целом.

15.3.2 Журнал пакетов МЭ

Журнал пакетов содержит в себе сведения об отправленных и принятых сетевых пакетах, прошедших через межсетевой экран.

Для того чтобы включить **Журнал пакетов МЭ** необходимо перейти на вкладку **Параметры безопасности** → **Политики аудита**, нажать правой кнопкой мыши на **Журнал пакетов МЭ**, выбрать **Свойства** и в появившемся окне выбрать пункт «*Вкл.*» и нажать кнопку **ОК** (Рис. 285).

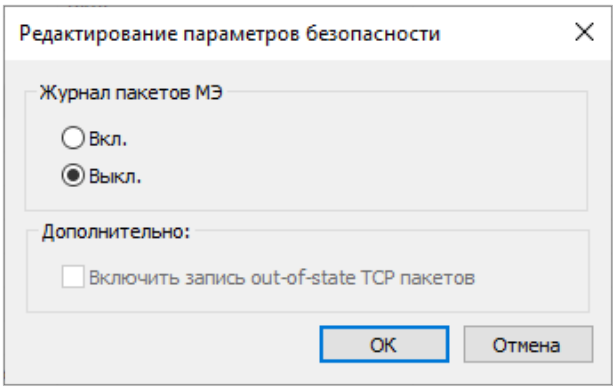


Рис. 285. Свойства журнала пакетов МЭ

Для отображения фиксируемой информации в журнале необходимо настроить правила межсетевого экрана, раздел 15.2.5 Правила МЭ. Следует на вкладке *Общие* в окне **Настройки правила МЭ** активировать правило и пункт *Уведомление в журнал пакетов* (Рис. 286).

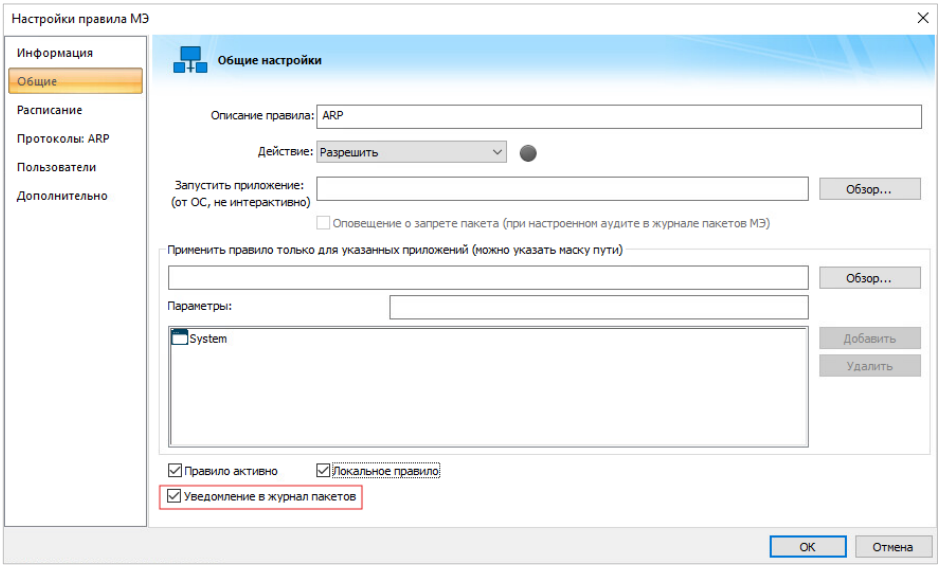


Рис. 286. Настройка уведомления в журнал пакетов

После настройки правил межсетевого экрана в журнале пакетов во вкладке *Журналы* начнется сбор и отображение информации по указанным при настройке сетевым пакетам (рис. 287).

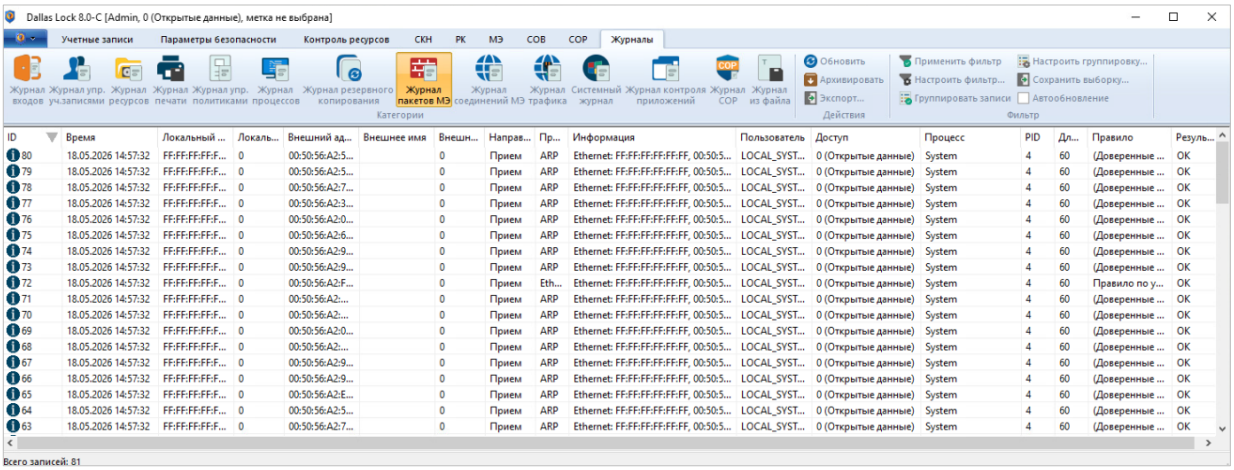


Рис. 287. Журнал пакетов МЭ

15.3.3 Журнал соединений

Журнал соединений отображает информацию об осуществленных в процессе работы **МЭ** сетевых соединениях. Для осуществления дальнейших настроек необходимо перейти на вкладку *Параметры безопасности*, выбрать параметр **Журнал соединений МЭ** и вызвать окно настройки журнала через контекстное меню или панель **Действия** (рис. 288).

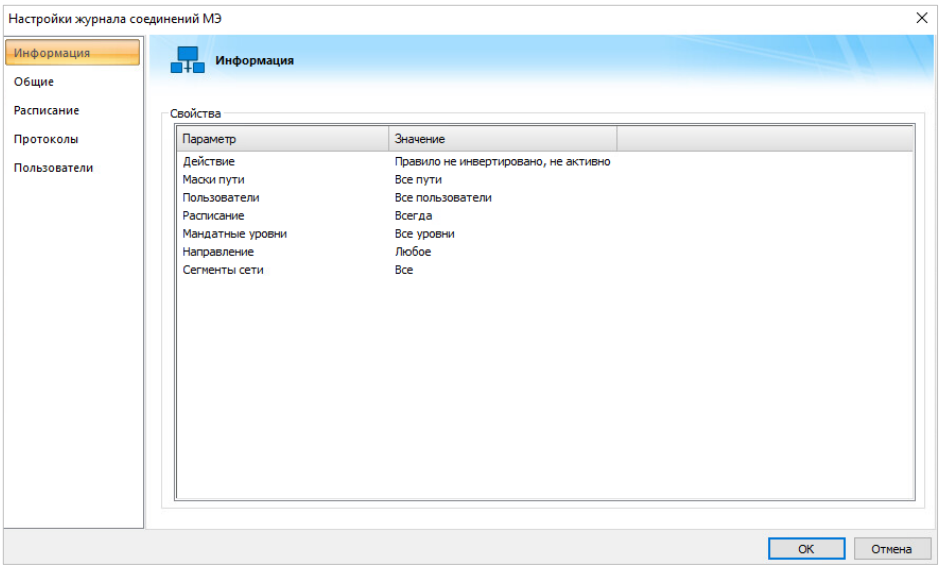


Рис. 288. Настройки журнала соединений МЭ

Настройки отображения информации, собранной журналом соединений **МЭ** идентичны настройкам правил работы межсетевого экрана, раздел 15.2.5 Правила МЭ. Исключение составляет отсутствие пункта *Дополнительно* и описание правила, оно присваивается по умолчанию.

Параметр «Мандатный уровень» доступен только для Dallas Lock 8.0 редакции «С».

После настройки параметров в журнале соединений в общей вкладке *Журналы* начнется сбор и отображение информации по указанным при настройке сетевым соединениям (рис. 289).

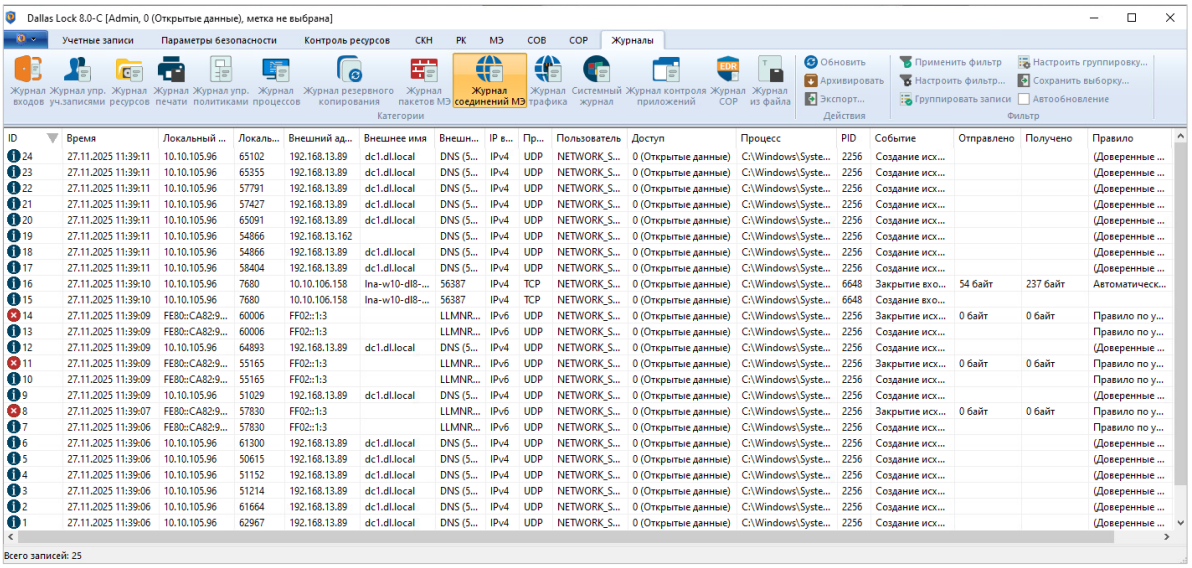


Рис. 289. Журнал соединений МЭ

15.3.4 Журнал трафика фильтрации МЭ

Журнал трафика фильтрации **МЭ** нужен для аудита трафика фильтрации для **МЭ**.

Чтобы включить журнал трафика фильтрации **МЭ**, необходимо нажать правой кнопкой мыши на параметре **Журнал трафика фильтрации МЭ** и в появившемся окне выбрать пункт «*Вкл.*» и нажать кнопку **Ок**.

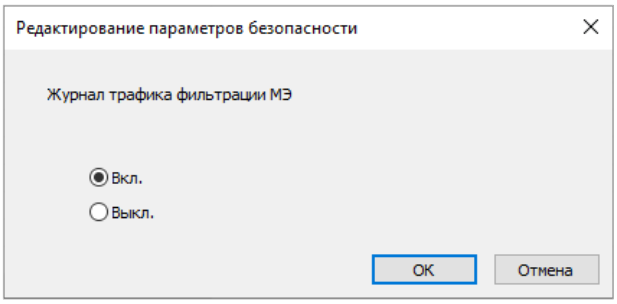


Рис. 290. Включение журнала трафика фильтрации МЭ

Журнал располагается в папке DL, например, «C:\DLLOCK80\Logs» и его имя может зависеть от названия используемого сетевого адаптера. Например, имя файла журнала может быть таким «C:\DLLOCK80\Logs\Journal.lg8».

16 СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

16.1 Назначение и общие принципы работы

СОВ Dallas Lock является модулем **Dallas Lock 8.0**, расширяющим функциональные возможности модуля **Межсетевой экран**. **СОВ Dallas Lock** обеспечивает обнаружение и блокирование основных угроз безопасности, выполняет одновременно функции и сетевой, и хостовой системы обнаружения вторжений, дополнительно детально анализирует некоторые отдельные сетевые протоколы.

Модуль **СОВ** может быть установлен без активного модуля **МЭ**. В случае активности модуля **МЭ** модуль **СОВ** расширяет возможности **МЭ**. В случае неактивного модуля **МЭ** модуль **СОВ** работает независимо.

16.1.1 Возможности системы обнаружения вторжений



Установка, удаление, активация и деактивация системы обнаружения воздействий описаны в разделе 2.2.

СОВ Dallas Lock обеспечивает защиту как от внутренних (локальных) нарушителей, так и от внешних нарушителей, включая угрозы со стороны сетей международного информационного обмена.

Ключевые особенности **СОВ**:

- возможность использования сигнатурных и эвристических методов для анализа сетевого трафика, журналов ОС и приложений на предмет нештатных ситуаций, а также попыток проведения вторжений;
- возможность обновления сигнатур сетевых атак и сигнатур анализа журналов ОС и приложений;
- обеспечение защиты от атак на сетевые протоколы на различных уровнях модели OSI;
- осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для недоверенных приложений;
- возможность анализа аномалий в поведении ОС и пользователей для выявления нештатных ситуаций;
- возможность анализа собранных данных **СОВ** о сетевом трафике в режиме, близкому к реальному масштабу времени.



Модули **СОВ** и **МЭ** позволяют обнаруживать атаки внутри виртуальной сети VipNet.

Настройка **СОВ** доступна пользователям, которым назначена возможность изменения настроек **СОВ**, — администраторам ЗАРМ **Dallas Lock** (по умолчанию членам группы *Администраторы*) и происходит из оболочки администратора во вкладке *СОВ*.

Для просмотра и изменения политик и других параметров **СОВ** пользователь должен быть указан в значении параметров **СОВ: Изменение настроек** и **СОВ: Просмотр настроек** категории **Права пользователей** либо состоять в группе, указанной в данном параметре.

16.2 Основное

В категории **Основное** доступен просмотр статистики, обновлений и назначенных портов.

16.2.1 Статистика СОВ

В блоке **Основное** → **Статистика** отображаются следующие данные (рис. 291):

- статус **СОВ**;
- информация о состоянии сигнатур трафика;
- статистика по:
  - сетевым атакам,
  - сигнатурам трафика,
  - подозрительной активности.

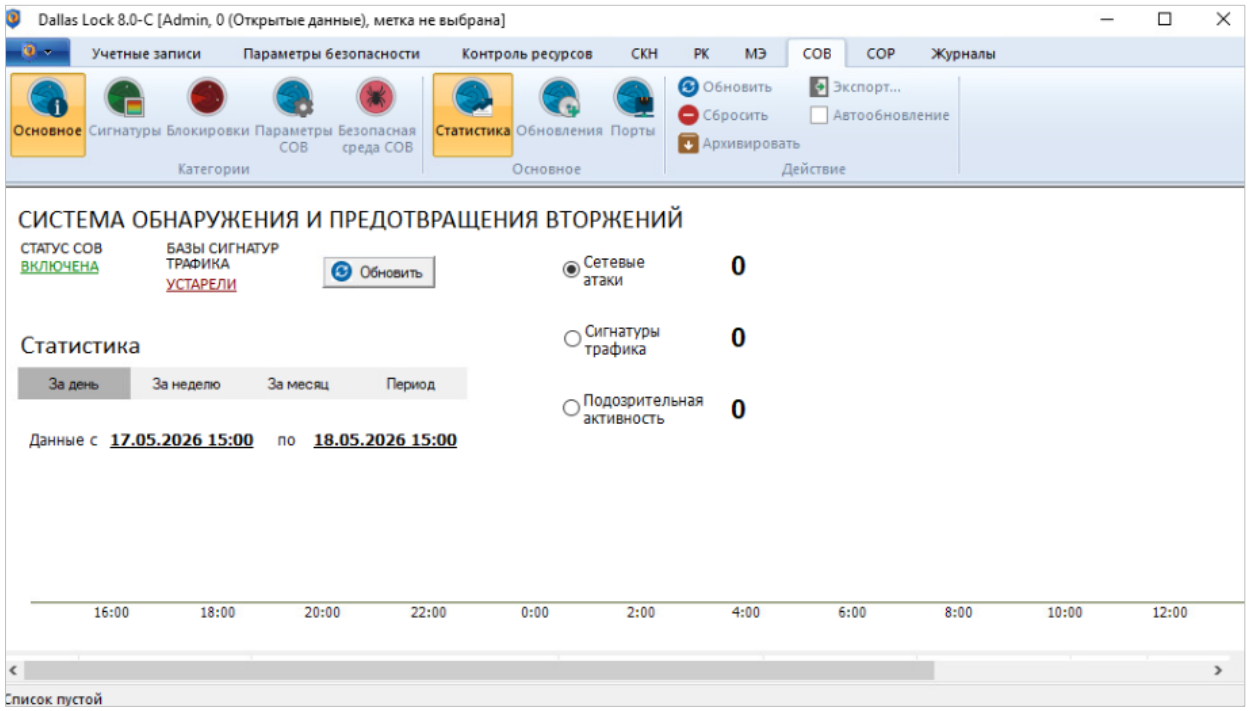


Рис. 291. Статистика сетевых атак

Статистика может быть отображена за день, неделю, месяц или другой выбранный период времени.

При ознакомлении с данными статистики нужно принимать во внимание то, что учет трафика производится с начала суток (00 часов 00 минут), с начала недели (понедельник), с первого дня месяца (1-е число отчетного месяца).

Данные по статистике отображаются в гистограмме и в журнале под ней. События в журнале можно упорядочить по необходимому значению, кликнув на кнопку с названием столбца статистики. Дважды кликнув по записи в журнале, можно получить полную информацию.

Панель действий позволяет обновить, сбросить статистику **СОВ**.

Для архивации собранной статистики необходимо нажать кнопку **Архивировать**. Архивация записей будет произведена в формате «*.lg8».

По команде **Экспорт…** возможно экспортировать записи журнала статистики в одном из следующих форматов:

- Текст (видимы на экране);
- Текст (разделитель — табуляция);
- CSV (разделитель — точка с запятой);
- HTML;
- XML.

16.2.2 Обновления

Подкатегория *Обновления* отображает такую информацию как: название модуля, текущую версию обновления БРП, комментарий и статус работы автоматического обновления (рис. 292).

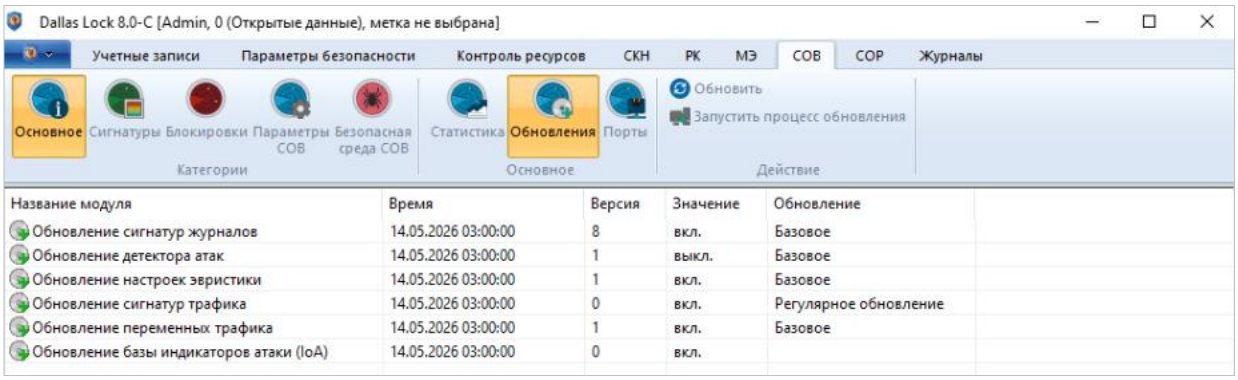


Рис. 292. Обновления

16.2.3 Порты

Подкатегория *Порты* отображает следующую информацию (рис. 293):

- Порты TCP для входящих и исходящих соединений (которые проверяются активными сигнатурами трафика).
- Порты UDP для входящих и исходящих соединений (которые проверяются активными сигнатурами трафика).
- Количество анализируемых входящих и исходящих TCP и UDP портов (которое проверяется активными сигнатурами трафика).
- Количество активных сигнатур трафика и журналов.

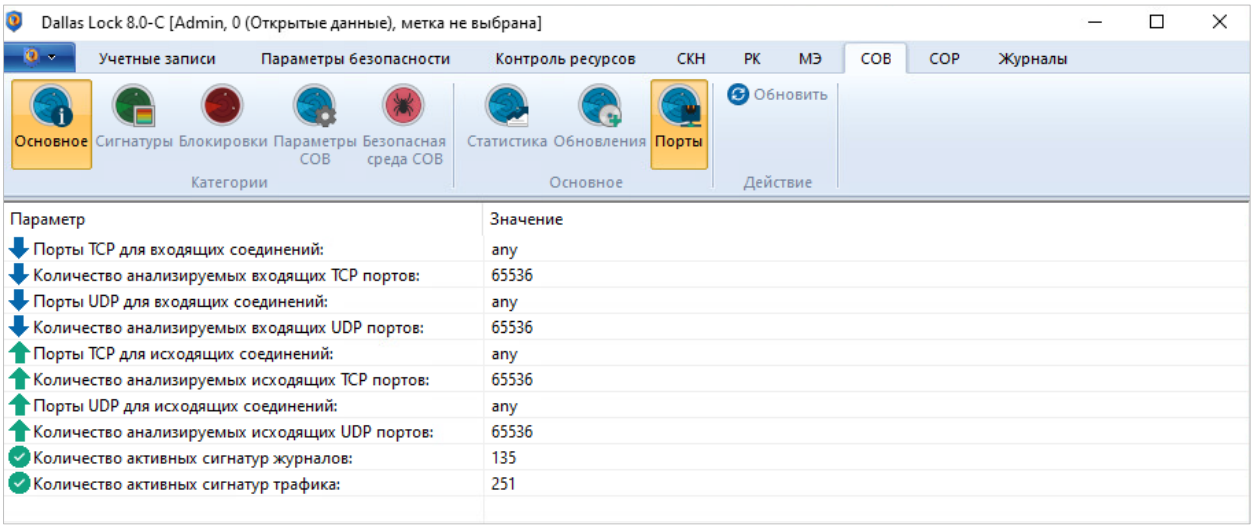


Рис. 293. Статистика портов

При двойном нажатии левой кнопкой мыши по одной из категории портов, откроется окно с детальным описанием.

16.3 Настройки сигнатур

Данная категория является инструментом управления сигнатурами **СОВ**. По умолчанию содержит готовые шаблоны наиболее типовых сигнатур.

Для перехода к управлению сигнатурами необходимо открыть вкладку *СОВ* и выбрать категорию **Сигнатуры**.

Если пользователь активировал/деактивировал сигнатуру через панель действий или контекстное меню, то она не считается измененной пользователем. При обновлении сигнатур каждая сигнатура заменяется только в том случае, если она не редактировалась пользователем через диалог редактирования настроек (т. е. не считается измененной пользователем) и находится в отключенном состоянии.

16.3.1 Сигнатуры журналов

На информационной панели находится древовидная структура сигнатур журналов и сведения о них: ID и статус правила, уровень тревоги, частота срабатывания и т. д. (рис. 294).

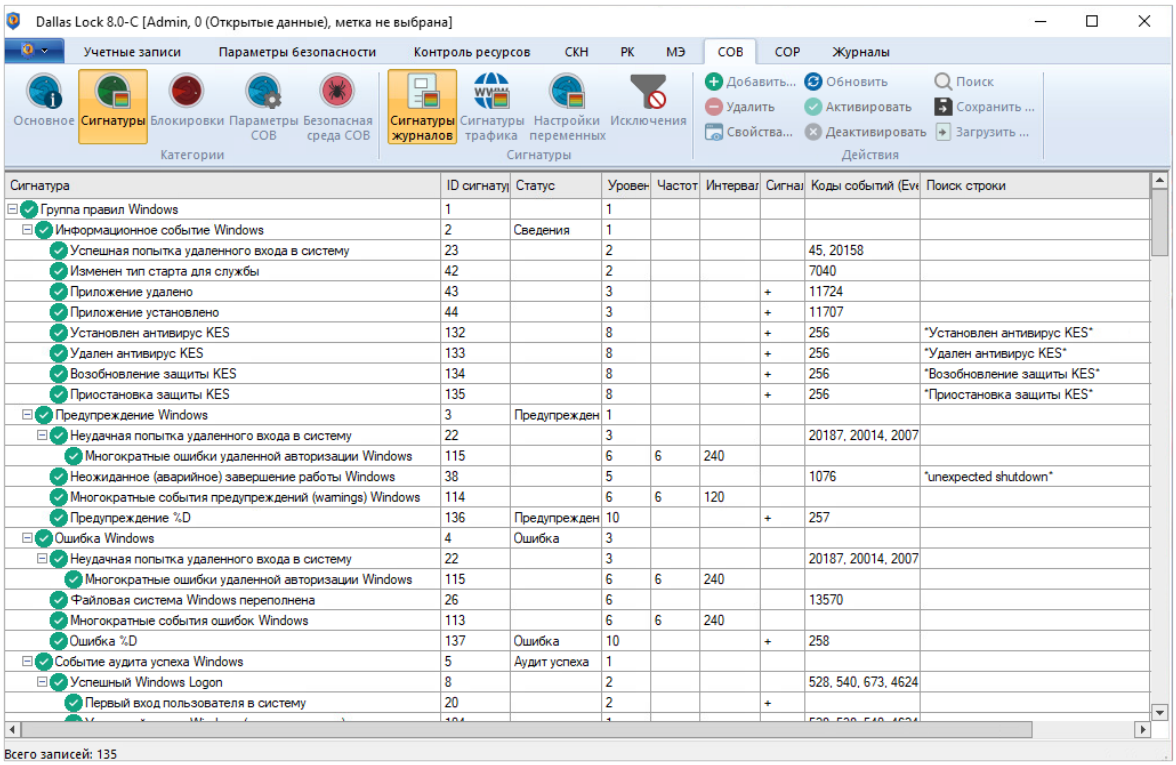


Рис. 294. Информационная панель настройки сигнатур журналов

Сигнатуры журналов анализируют журналы Windows. Данные сигнатуры делятся на две группы правил.

В зависимости от состояния сигнатуры значки могут принимать следующий вид:

— сигнатура активирована;

— сигнатура деактивирована;

— сигнатура активирована, но не функционирует, так как родительская сигнатура деактивирована.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели (рис. 295). Для отображения поисковой строки необходимо нажать на кнопку **Поиск** на панели **Действия**.

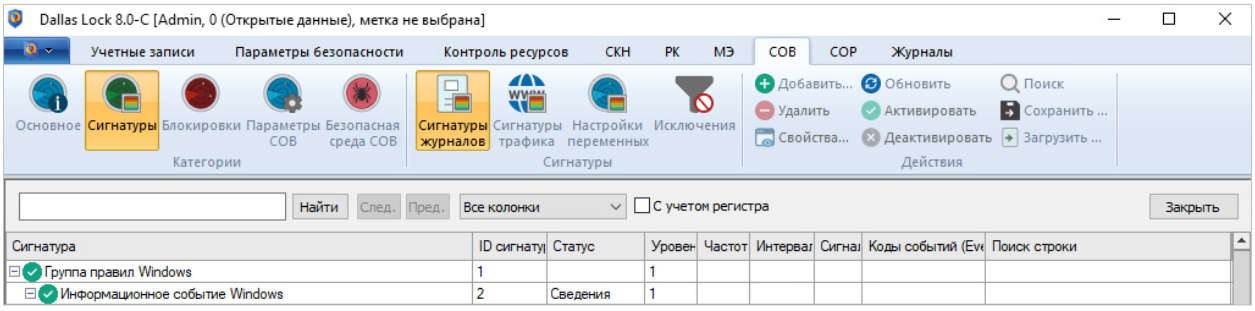


Рис. 295. Поиск по ключевым словам

Для того, чтобы изменить сигнатуру, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие **Свойства**.

Существует возможность добавления новой сигнатуры, ее удаление, активации, деактивации, поиска и обновления. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

В меню **Настройка сигнатуры журналов** можно осуществить несколько уровней настроек текущей сигнатуры.

В разделе *Информация* отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 296).

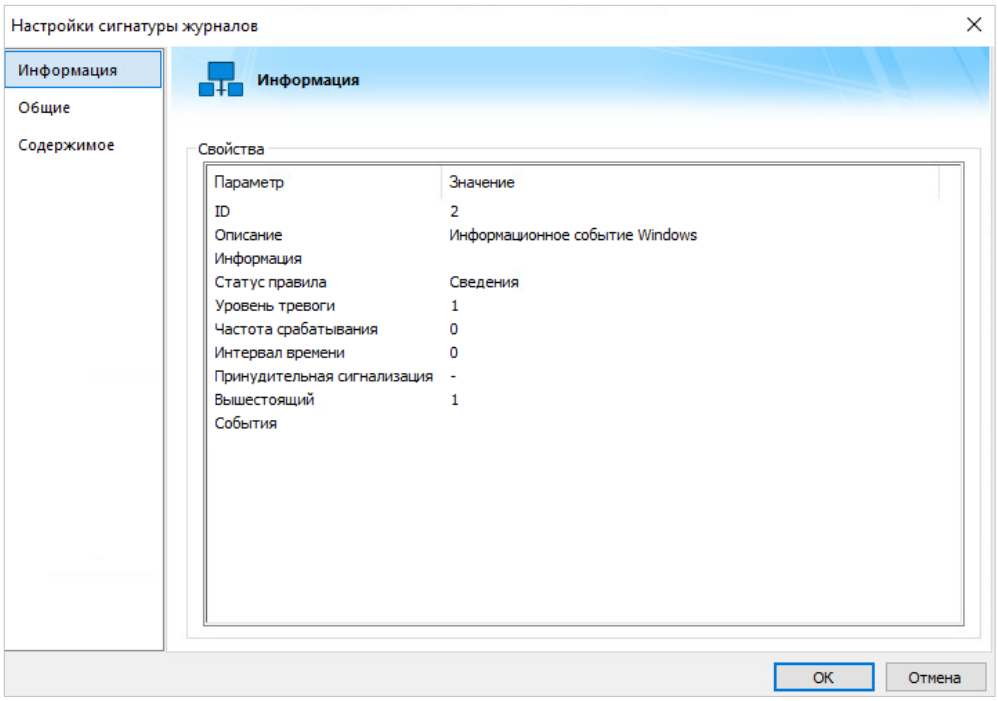


Рис. 296. Информация

В разделе *Общие* представлены основные настройки сигнатуры (рис. 297).

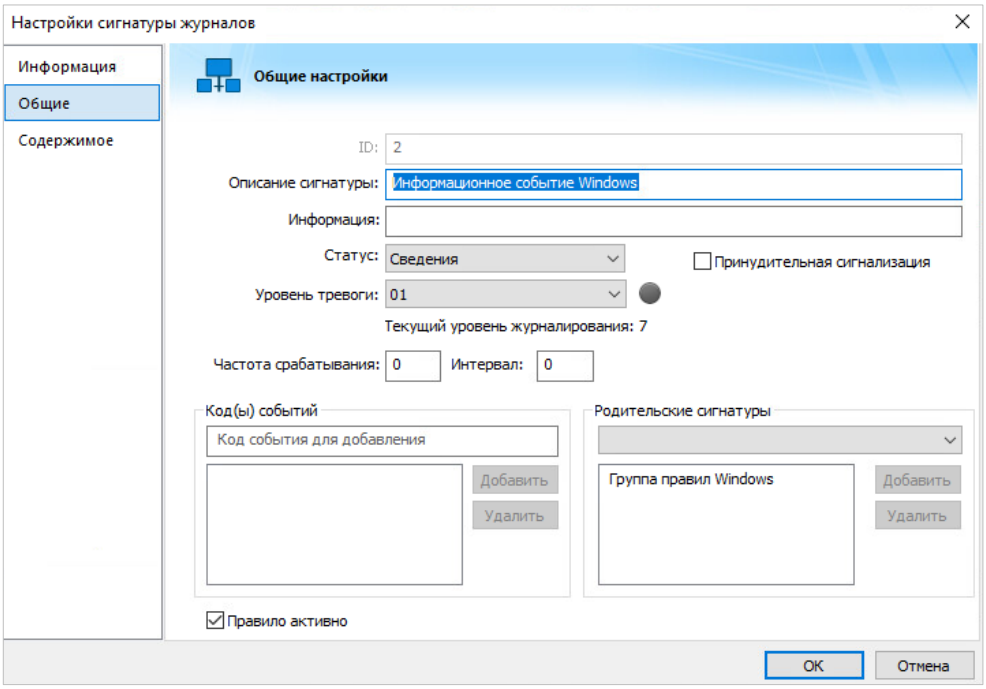


Рис. 297. Общие

В разделе *Содержимое* возможно указать ключевые слова (маску), которые должны содержаться в тексте описания события для срабатывания данной сигнатуры (рис. 298).

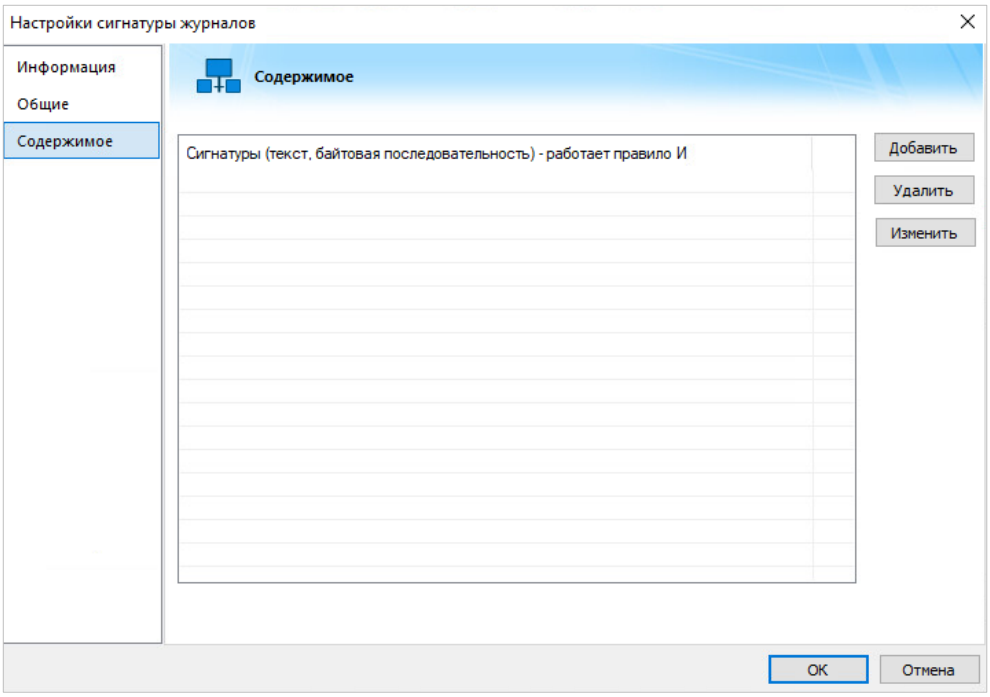


Рис. 298. Содержимое

При отключении родительской сигнатуры дочерние сигнатуры будут неактивны. Включенные, но нефункционирующие сигнатуры, отмечаются иконкой восклицательного знака.

Действия по изменению сигнатур журналов фиксируются в журнале управления политиками.

16.3.2 Сигнатуры трафика

На информационной панели находится список сигнатур трафика и сведения о них: действие, протокол, источник, порт источника, направление и т. д. (рис. 299).

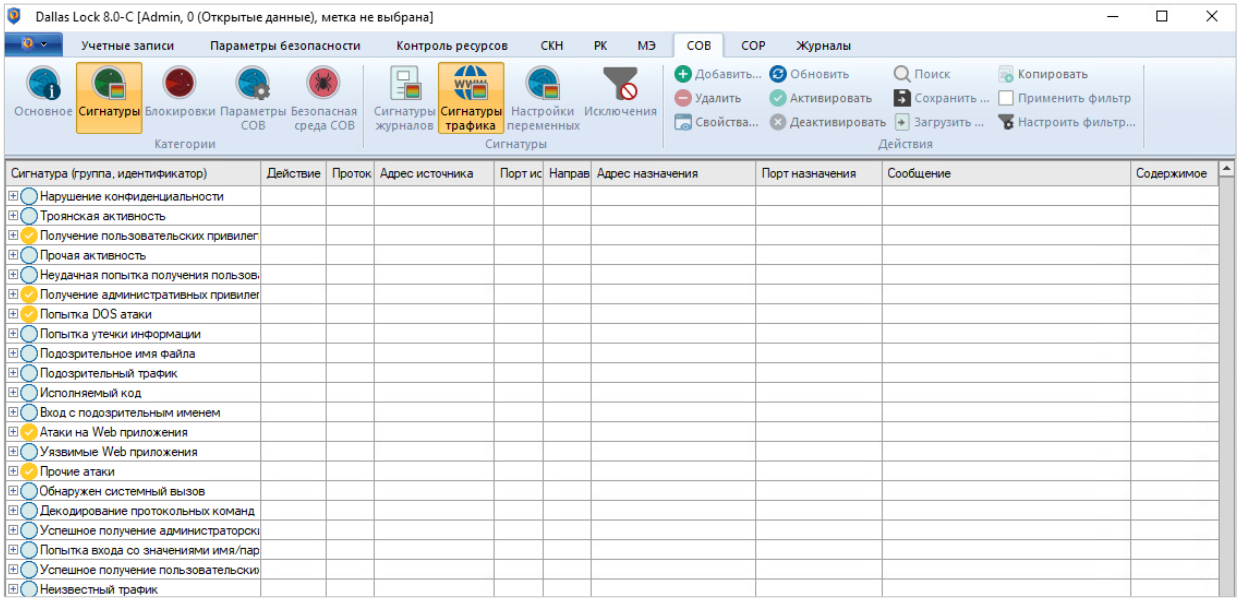


Рис. 299. Информационная панель настройки сигнатур трафика

В зависимости от состояния сигнатуры трафика, значки могут принимать следующий вид:

- — сигнатура или вся группа активированы;
- — сигнатура или вся группа деактивированы;
- — активированы не все сигнатуры, входящие в группу.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск

по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку **Поиск** на панели **Действия**.

Для того, чтобы изменить сигнатуру трафика, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие **Свойства**. Кроме редактирования существующих сигнатур, есть возможность добавления новых сигнатур, удаление, активация, деактивация и поиск. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

В меню **Настройка сигнатуры трафика** можно осуществить несколько уровней настроек текущей сигнатуры.

В разделе *Информация* отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 300).

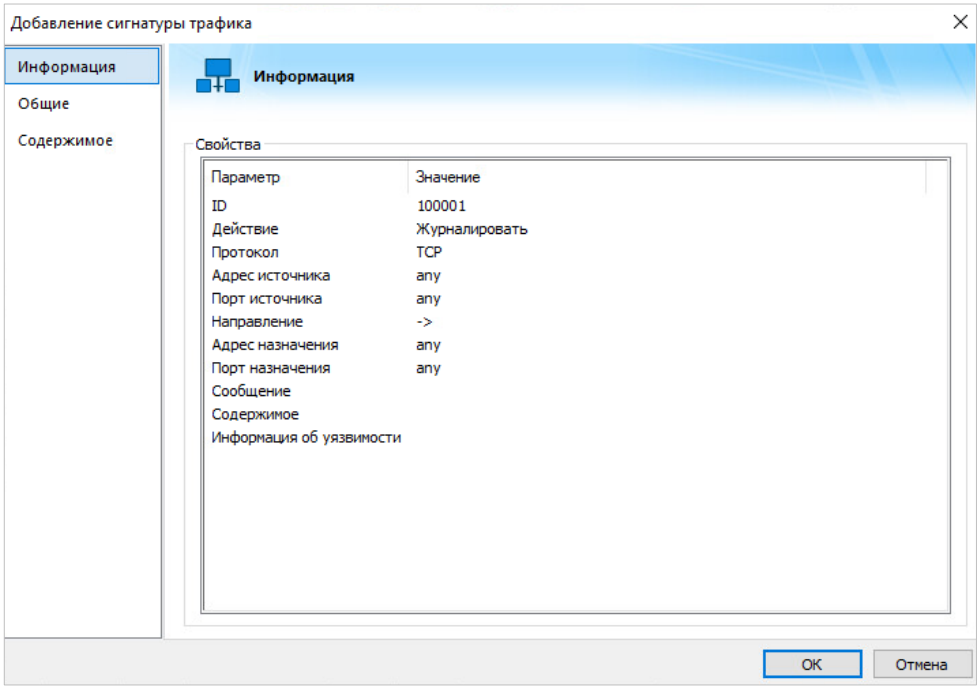


Рис. 300. Информация

В разделе *Общие* представлены основные настройки сигнатуры (рис. 301). Для упрощения настройки адресов и портов доступен выпадающий список для выбора переменных **СОВ**, подраздел 16.3.3 Настройки переменных.

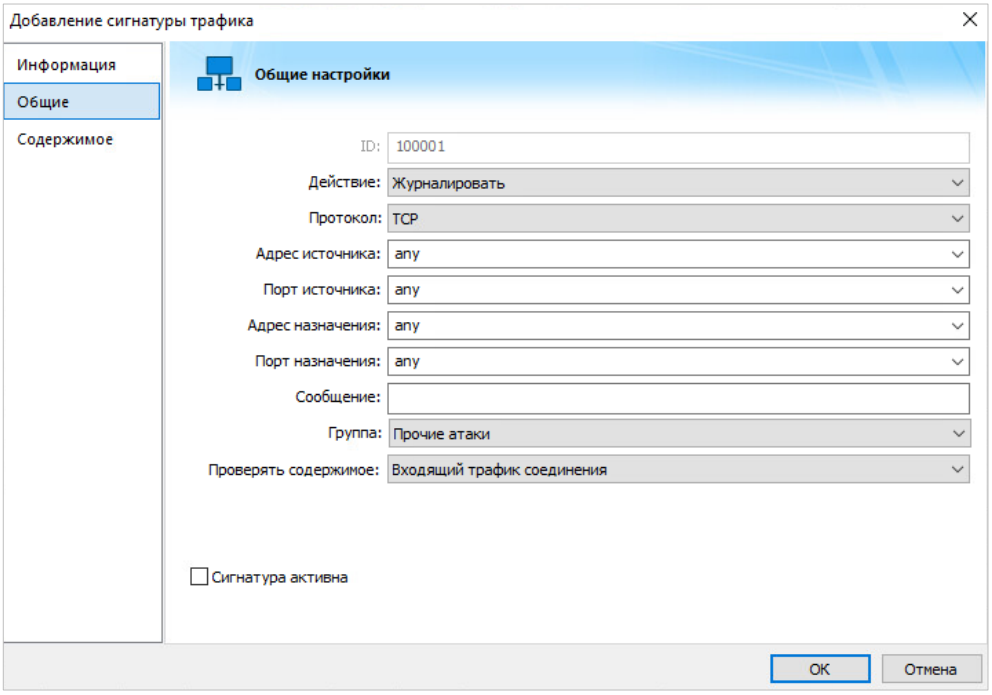


Рис. 301. Общие

В разделе *Содержимое* для срабатывания сигнатуры необходимо добавить ключевые слова или байтовую последовательность, которая должна будет содержатся в проходящем сетевом трафике (рис. 302). Данный раздел активен только при ручном создании сигнатур трафика. Содержимое сигнатур трафика, поставляемых компанией **ООО «Конфидент»**, может быть закрыто для просмотра.

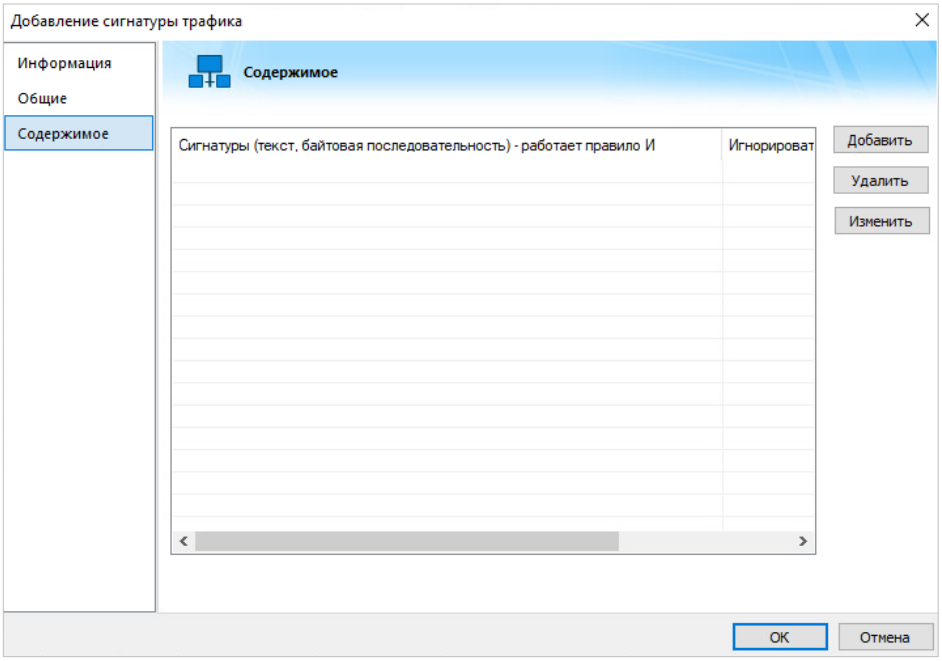


Рис. 302. Содержимое

При добавлении ключевых слов и байтовых последовательностей (сигнатур содержимого) допускается использование специальных символов «*» и «?», где:

- «?» – произвольный символ;
- «*» – произвольная последовательность символов.

Для формирования цепочек позиционных взаимосвязей между сигнатурами содержимого в редакторе предусмотрены поля *within* и *distance*. Допустимые значения: «-» (по умолчанию) и от 1 до 65535.

Поле *distance* – это минимальное расстояние от предыдущей сигнатуры (или от начала потока, если это первая сигнатура) в байтах.

То есть distance = N, где N > 0, указывает на то, что эта сигнатура содержимого должна находиться в трафике на расстоянии не менее N байт после предыдущей сигнатуры (или от начала потока, если это первая сигнатура).

Поле *within* – это максимальное расстояние от значения в поле *distance* в байтах.

То есть within = N, где N > 0, указывает на то, что эта сигнатура содержимого должна находиться в трафике на расстоянии не более distance + N байт после предыдущей сигнатуры. Если это первая сигнатура, то поле *within* — недоступно.

Значение поля *within* должно быть больше либо равно размеру сигнатуры в байтах.

Значение «-» указывает на отсутствие требований к минимальному и/или максимальному расстоянию между сигнатурами.

Если выбран параметр «Игнорировать регистр», то регистр символов не будет учитываться при поиске этой сигнатуры содержимого в трафике.

Пример

Сигнатуры (текст, байтовая последовательность) – работает правило И	within	distance
GET	-	5
login	6	4
admin	-	2
pass	8	-
success	-	-

В приведенном примере:

- сигнатура *GET* должна находиться на расстоянии не менее 5 байт от начала потока данных;
- сигнатура *login* должна находиться на расстоянии от 4 до 10 байт после *GET*;
- сигнатура *admin* должна находиться на расстоянии не менее 2 байт после *login*;
- сигнатура *pass* должна находиться на расстоянии не более 8 байт после *admin*;
- сигнатура *success* может находиться в любом месте потока данных относительно *GET*, *login*, *admin* и *pass*, в том числе до них и между ними.

При создании новых сигнатур трафика важно учитывать алгоритм их проверки:

1. **СОВ** проверяет сетевой трафик на соответствие протоколу, адресам и портам источника и назначения, указанным в настройках сигнатуры, и при обнаружении совпадения (в любом направлении) анализирует это соединение на содержимое.
2. Анализ соединения на содержимое выполняется в зависимости от параметра **Проверять на содержимое** либо только входящего трафика соединения, либо только исходящего трафика соединения, либо всего трафика этого соединения.
3. При обнаружении всех ключевых слов и байтовых последовательностей, указанных на вкладке *Содержимое*, сигнатура срабатывает. При этом выполняется **Действие**, указанное на вкладке *Общие*.

Пример

С сайта «www.lenta.ru» идет подозрительный трафик, поэтому необходимо разорвать соединение и заблокировать адрес.

Процесс создания новой сигнатуры происходит по тем же настройкам, что и корректировка уже готовой. Для создания новой сигнатуры нужно нажать правую клавишу мыши на информационной панели и выбрать **Добавить** в контекстном меню или нажать ту же кнопку на панели действий.

В разделе **Общие** устанавливается действие **Разорвать соединение и блокировать адрес**, после чего указывается нужный тип протокола *TCP*. Далее необходимо ввести адрес и порт источника, а также адрес и порт назначения. В данном случае требуется изменить только поле *Порт назначения* и ввести порт «*80*». После выбрать группу *Подозрительный трафик*. Параметр **Двунаправленная** позволяет отслеживать трафик в обоих направлениях — в данном примере в этом нет необходимости.

Далее в разделе *Содержание* необходимо нажать **Добавить** и ввести ключевое слово «lenta.ru», которое будет содержаться в исходящем трафике с сайта «www.lenta.ru». После нажать кнопку **ОК** и активировать созданную сигнатуру.

Для более гибкой настройки условий обнаружения сигнатуры можно использовать **Переменные трафика**, подраздел 16.3.3 Настройки переменных.

Сигнатура сработает ТОЛЬКО при точном совпадении указанных настроек. В случае **одновременного** задания нескольких ключевых слов или байтовых последовательностей для одной сигнатуры, например, два ключевых слова — для срабатывания сигнатуры должны выполниться **оба условия**.

Действия по изменению сигнатур трафика фиксируются в журнале управления политиками.

16.3.3 Настройки переменных

Параметр **Настройки переменных** позволяет задать сетевые адреса внутренней и внешней сети, серверы, TCP и UDP порты, используемые в сети, а также группировать их, чтобы затем использовать в пределах нескольких сигнатур, подраздел 16.3.2 Сигнатуры трафика. (рис. 303). При изменении значения переменной любая сигнатура, которая использует данную переменную, обновится в соответствии с новым значением переменной.

Переменные бывают двух типов — переменные диапазона адресов и переменные диапазона портов.

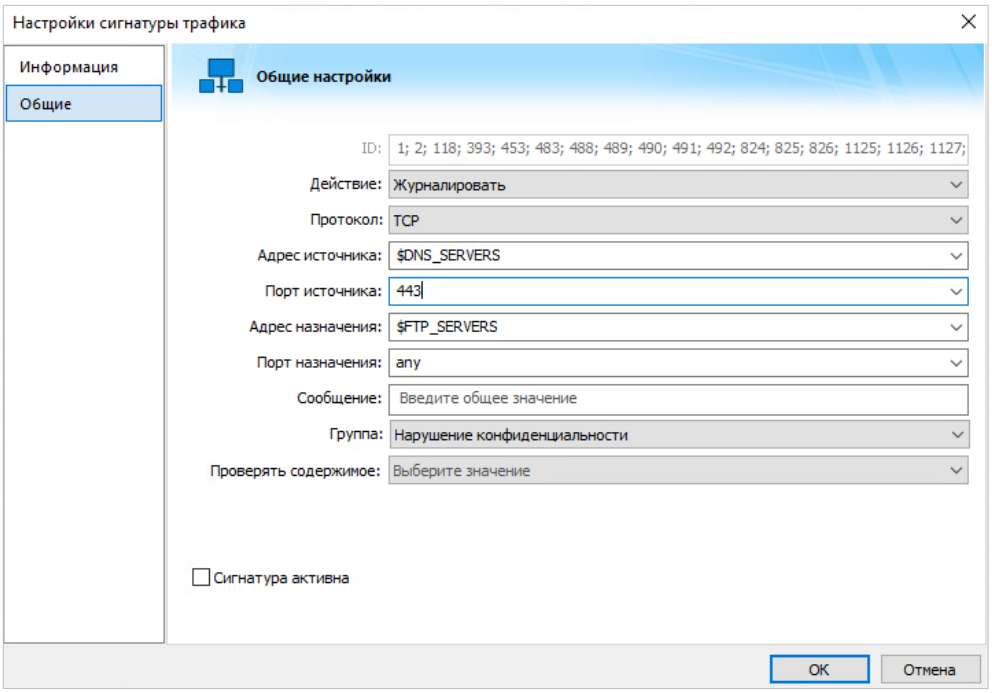


Рис. 303. Настройки сигнатуры трафика

На информационной панели находится список переменных трафика с их значениями (рис. 304).

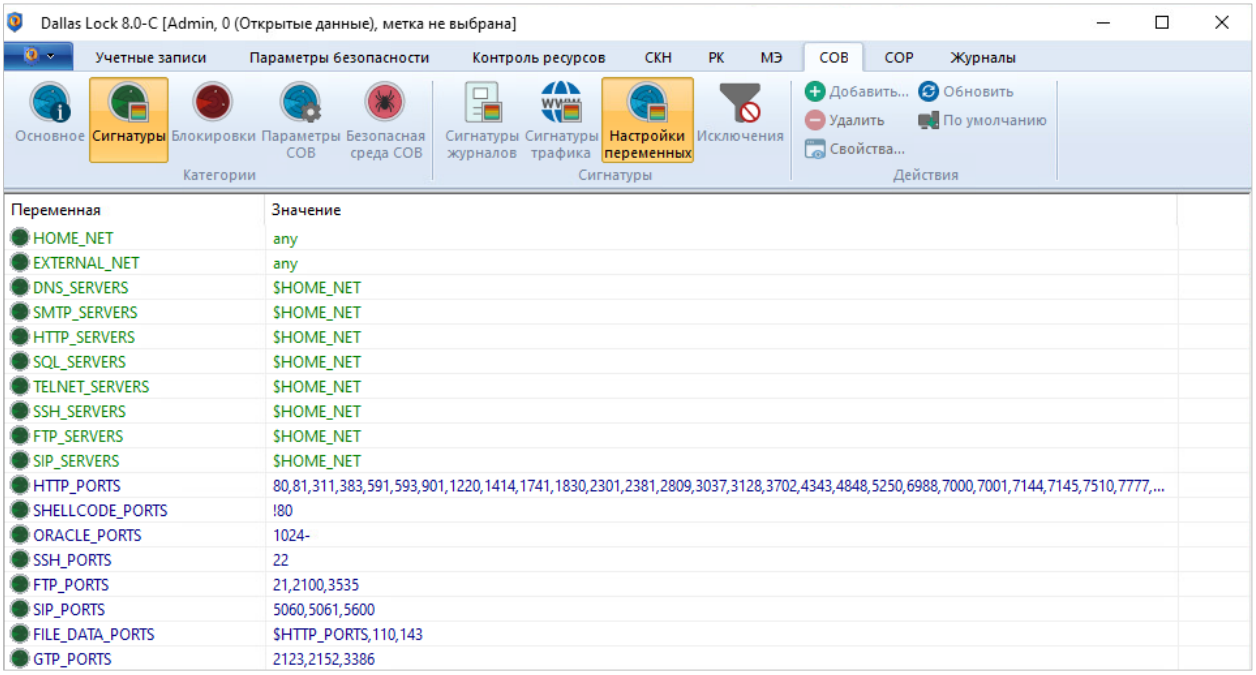


Рис. 304. Информационная панель настройки переменных трафика

HOME_NET

В данной переменной требуется задать диапазон внутренних IP-адресов. По умолчанию переменная HOME_NET содержит значение «any», что относится к любому IP-адресу.

Для того, чтобы изменить переменную, нужно, выбрав ее на информационной панели, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие **Свойства**.

При настройке, возможно задать маску подсети и указать несколько IP-адресов включая их диапазон: «1.1.1.1, 1.1.2.1/24, 1.1.3.1-1.1.3.9»

EXTERNAL_NET

В переменной EXTERNAL_NET необходимо задать диапазон внешних IP-адресов. По умолчанию данная переменная содержит значение «any». СОВ будет реагировать на любой входящий или исходящий трафик.

Для уменьшения нагрузки на ЗАРМ, возможно воспользоваться логическим отрицанием, используя символ «!». Например, сеть не являющееся HOME_NET имеет значение «!$HOME_NET».
Переменные SERVERS
Настройка переменных _SERVERS ничем не отличается от настройки переменных HOME_NET или EXTERNAL_NET.
Переменные PORTS
При настройке портов, возможно назначить один или несколько портов, непрерывный диапазон, инвертировать, а также указать значение другой переменной: • «80,81,311»; • «1024-»; • «!80»; • «$HTTP_PORTS». При задании избыточно широкого диапазона портов в рамках одного правила МЭ количество используемых для перехвата портов будет ограничено, и в первую очередь будут заполнены порты из списка подозрительных и неиспользуемых служебных портов, подраздел 16.5.3 Настройки эвристики.

Действия по изменению переменных трафика фиксируются в журнале управления политиками.

16.3.4 Исключения

Исключения необходимы для работы с указанными хостами вне зависимости от настроек (Рис. 305).

Для создания правила исключения необходимо выбрать действие **Добавить**, после чего на информационной панели появится новое правило с пустым полем, где необходимо ввести IP-адрес или DNS-имя, с указанием порта.

Для поддержания актуальных адресов хостов исключений, адреса исключений периодически обновляются.

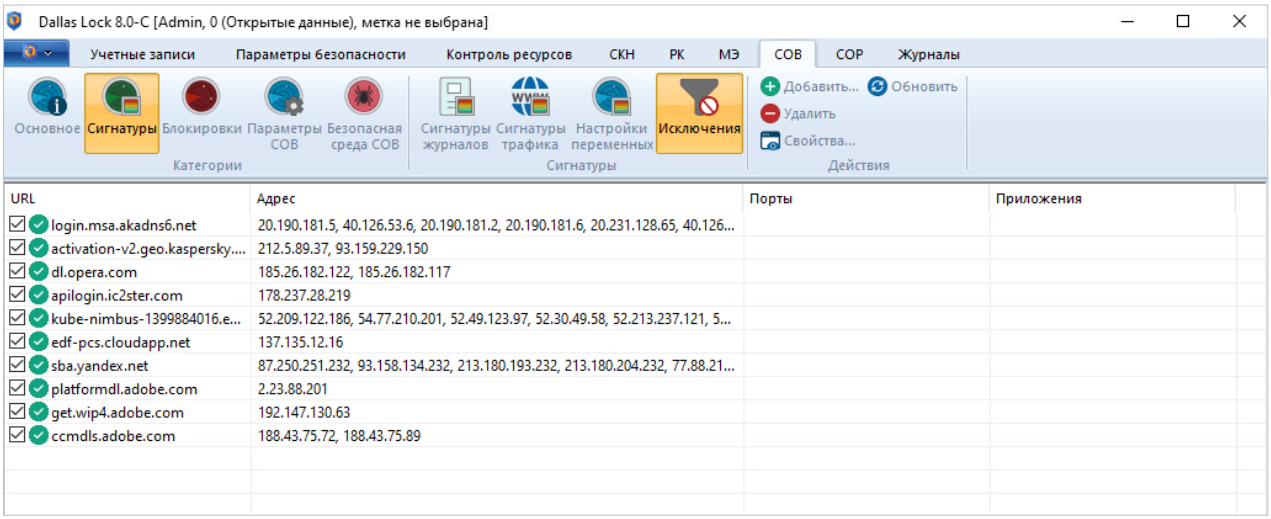


Рис. 305. Исключения сигнатур

Для того, чтобы удалить исключения нужно, выделив правило, нажать правой кнопкой мыши и выбрать в контекстном меню действие **Удалить**.

16.4 Блокировки

16.4.1 Заблокированные адреса

В подкатегории *Заблокированные адреса* отображаются заблокированные IP и MAC адреса, а также сведения о них: дата, адрес, DNS, правило, описание блокировки и т. д. (рис. 306).

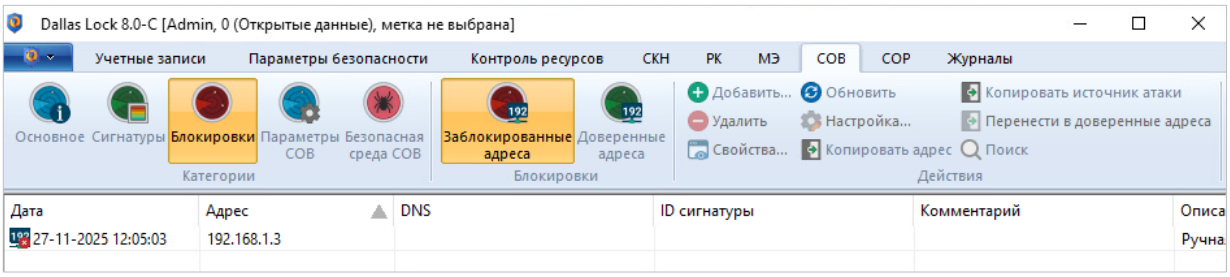


Рис. 306. Информационная панель заблокированных адресов

Существует возможность создания ручной блокировки адреса. Для этого необходимо выбрать действие **Добавить**. Появится окно **Добавление блокировки СОВ**, в котором необходимо указать IP или MAC и задать период блокировки (рис. 307).

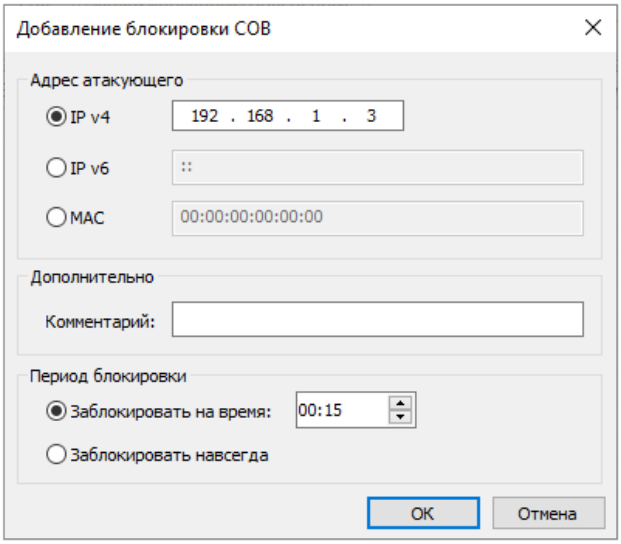


Рис. 307. Добавление блокировки СОВ

Для того, чтобы снять блокировку, нужно, выбрав один или несколько заблокированных адресов, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие **Удалить**. Далее появится окно с просьбой подтвердить операцию.

Для копирования адреса или источника атаки необходимо выбрать заблокированный адрес и нажать соответствующую кнопку на панели **Действия** или воспользоваться контекстным меню.

Для упрощения администрирования доступен поиск по ключевым словам, с учетом регистра и поиск по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку **Поиск** на панели **Действия**.

Если необходимо изменить время уже заблокированного адреса, необходимо нажать правой кнопкой мыши на адрес (или выделить группу адресов), выбрать пункт **Настройка…**(Рис. 308) и в окне (Рис. 307) в подразделе *Период блокировки* настроить время блокировки или заблокировать адрес навсегда.

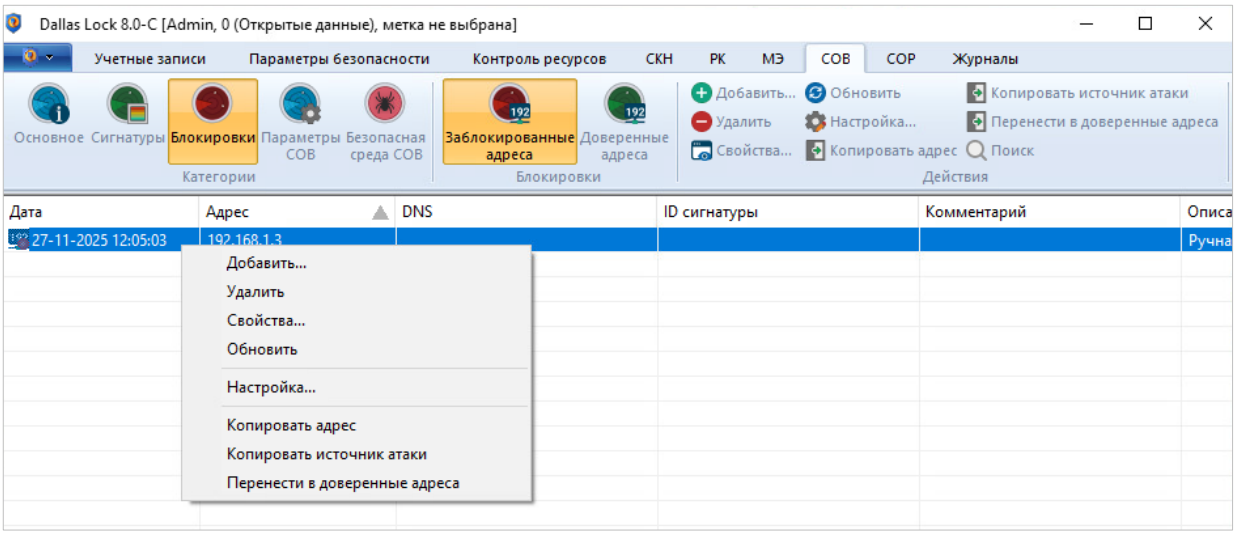


Рис. 308. Настройка блокировки

Действия по изменению списка заблокированных адресов фиксируются в журнале управления политиками.

16.4.2 Доверенные адреса

В подкатегории *Доверенные адреса* отображаются доверенные IP и MAC адреса, а также сведения о них: адрес, комментарий, отметка в журнале (рис. 309).

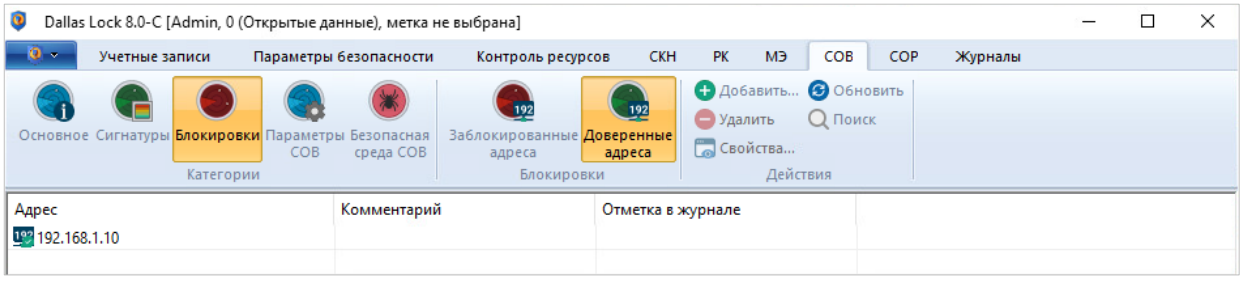


Рис. 309. Информационная панель доверенных адресов

Для того, чтобы добавить доверенный адрес, необходимо выбрать действие **Добавить**. Дополнительно возможно написать комментарий и включить опцию *Фиксировать в журнале обнаруженные атаки* (рис. 310).

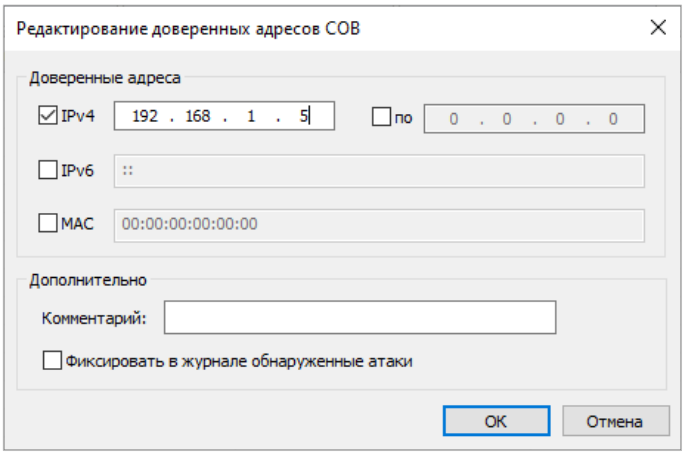


Рис. 310. Редактирование доверенных адресов СОВ

В некоторых случаях может понадобиться занесение в белые адреса и IP и MAC доверенного узла, так как в одних случаях может срабатывать блокировка по IP-адресу, а в других случаях — по MAC.

Для того, чтобы удалить доверенный адрес, нужно, выбрав один или несколько доверенных адресов, щелкнуть правой кнопкой мыши и выбрать в контекстном меню действие **Удалить**. Далее необходимо подтвердить операцию.

Для упрощения администрирования доступен поиск по ключевым словам с учетом регистра и поиск по всем столбцам таблицы на информационной панели. Для этого необходимо нажать на кнопку **Поиск** на панели **Действия**.

Действия по изменению списка доверенных адресов фиксируются в журнале управления политиками.

16.5 Параметры СОВ

16.5.1 Контроль приложений

Обнаружение аномалий в поведении приложений и ОС, может являться сигналом об осуществлении попытки вторжения. Для выявления таких попыток **СОВ** перехватывает вызовы функций от приложений к ОС и отслеживает следующие события:

- Обращения ПО к системному реестру и критическим объектам ОС. Критическими являются объекты, удаление, блокирование или модификация которых оказывает влияние на функционирование или безопасность ОС Windows — системные библиотеки, драйверы, файл hosts и т. п.
- Попытки модификации или удаления объектов ПО **СЗИ**.
- Обращения ПО к объектам ФС, в том числе прямой доступ к диску.
- Попытки внедрения компонент — подмена и установка сторонних библиотек, установка системных перехватчиков, через которые посторонний код может быть внедрен в другой процесс, оконные перехватчики.
- Внедрение в память процесса.
- DDE- и OLE- взаимодействие.
- Запросы на завершение и запуск процессов.
- Низкоуровневый сетевой доступ.
- Вызов DNS API.
- Попытки снятия скриншота экрана, НСД к буферу обмена или перехват нажатия клавиш приложениями.



При помощи правила **Получение контекста десктопа или активного окна (возможность снятия скриншота)** можно заблокировать попытки снятия снимка экрана приложениями, использующими для этого возможности GDI API, например, «Ножницы», Shift+Win+S и т. д.

Попытки получения контекста десктопа с помощью других методов, таких как Windows.Graphics.Capture, не блокируются.

Если требуется исключить возможность снятия скриншота для конкретного приложения, например, «Ножницы», необходимо создать соответствующее правило Контроля приложений в соответствии с примером, приведенным в данном разделе.



Если **Получение контекста десктопа или активного окна (возможность снятия скриншота)** заблокировано в правилах по умолчанию, то это может повлиять на работоспособность и быстродействие безопасных приложений, использующих те же возможности GDI API, но в иных, не связанных со снятием снимка экрана целях (например, Microsoft Edge).

В этом случае для доверенных приложений, с которыми наблюдаются такие проблемы, рекомендуется создать правило Контроля приложений, разрешающее получение контекста десктопа или активного окна.



Если в **СОВ** созданы запрещающие правила для контроля приложений и реестра, и при этом была создана новая учетная запись пользователя, то для работы данного пользователя необходимо временно отключить **СОВ** и выполнить вход под новой учетной записью пользователя. При этом входе в системной папке ОС формируется профиль пользователя, необходимый для корректной работы с **СОВ**.



Исполняемые модули ОС, входящие в состав внутреннего каталога Windows, считаются доверительными и проходят проверку подписи.

В системе не контролируются системные процессы и защищенные процессы.

Некоторые разрешающие и запрещающие правила Контроля приложений применяются к процессу в момент его запуска и действуют до момента его завершения. Поэтому если правила Контроля приложений были изменены, то для того, чтобы обновленные правила применились ко всем процессам, рекомендуется выполнить выход и повторный вход в ОС либо перезагрузить ЗАРМ.

На информационной панели находится список правил контроля приложений и сведения о них (рис. 311).

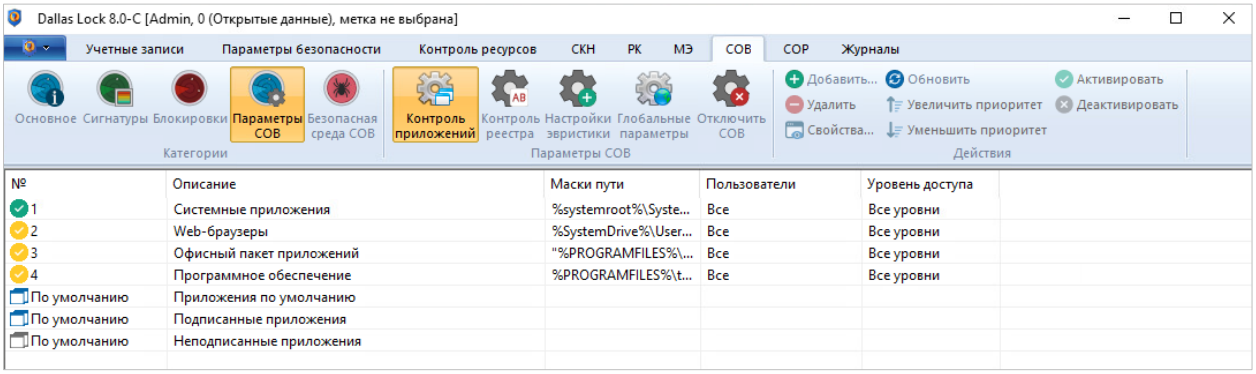


Рис. 311. Информационная панель контроля приложения

При запуске любого приложения **СОВ** производит его анализ (определяет, подписано приложение или нет) и ищет данное приложение в пользовательских правилах контроля приложений **СОВ**. При обнаружении приложения, **СОВ** выполняет проверку на наличие ограничений для системных функций приложения. В правиле для каждой функции возможно установить следующие значения:

- разрешить,
- запретить,
- наследуется.

Пользовательские правила могут наследовать настройки правил по умолчанию для подписанных и неподписанных приложений.

Если приложение не было найдено в пользовательских правилах, то **СОВ** проверяет доступ в правилах по умолчанию для подписанных и неподписанных приложений. Для системных функций возможно установить аналогичные значения, что и в пользовательских правилах.

Правила по умолчанию для подписанных приложений и неподписанных приложений, могут наследовать настройки у глобальных правил для приложений по умолчанию.

Поэтому приоритеты правил контроля приложений представляют собой следующую иерархию:

Таблица 13. Приоритеты правил контроля приложений СОВ

Правила	Приоритет
Пользовательские правила	Самый высокий
Правила по умолчанию для подписанных и неподписанных приложений	Средний
Глобальное правило для приложений по умолчанию	Самый низкий

Предустановленные наборы правил необходимы для корректной работы операционной системы и прикладного программного обеспечения.

Таблица 14. Предустановленные правила контроля приложений

№	Описание	Приложения
1.	**Системные приложения**	-

№	Описание	Приложения
2.	**Web-браузеры**	Opera Яндекс браузер Mozilla Firefox Google Chrome Microsoft Edge Internet Explorer
3.	**Офисный пакет приложений**	Microsoft Excel Microsoft Word
4.	**Программное обеспечение**	Microsoft Pdf Reader Total Commander Acrobat Reader DC

Набор правил «Системные приложения» не доступен для редактирования и всегда активирован. Для данного набора правил не доступны действия **Удалить** и **Деактивировать**.

Для того, чтобы изменить правило, нужно выбрать его на информационной панели и нажать кнопку **Свойства** на панели **Действия**.

Существуют возможность удаления пользовательского правила, добавление нового и обновления, а также назначения приоритета. Эти действия становятся доступны как в контекстном меню при нажатии правой кнопки мыши, так и на панели **Действия**.

При изменении или добавлении правила появится меню **Настройка правила контроля приложений**, где можно осуществить несколько уровней настроек.

В разделе *Информация* отображается сводная информация всех параметров правила. Вносить какие-либо изменения в работу правила на данном этапе нельзя (рис. 312).

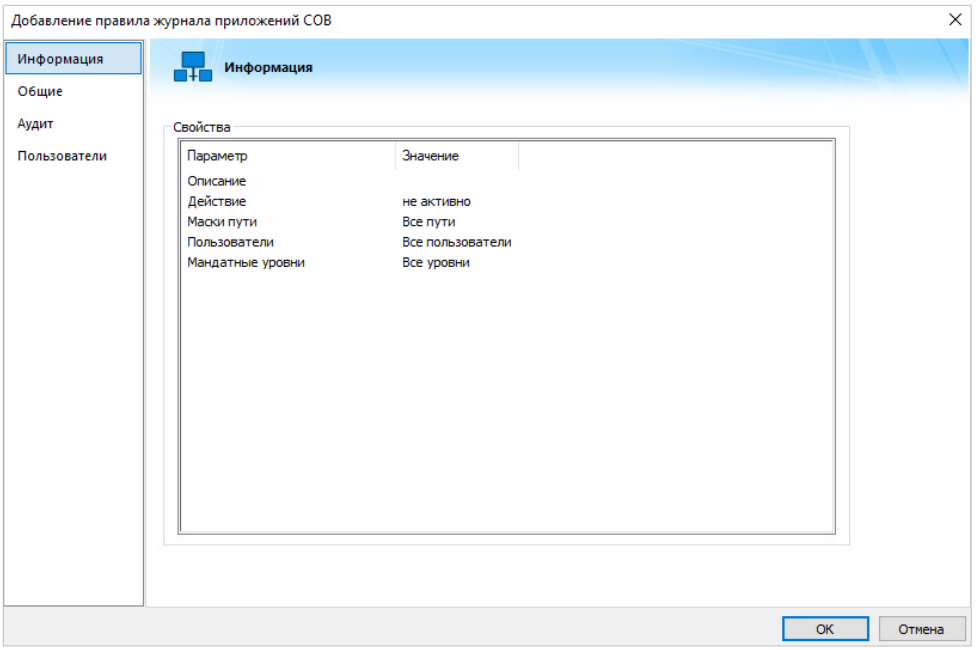


Рис. 312. Информация

В разделе *Общие* представлены основные настройки правила (рис. 313). Есть возможность наследовать настройки у правила по умолчанию для подписанных и неподписанных приложений. Для перечисленных системных функций приложения возможно разрешить или запретить доступ, или наследовать значения у правила выше приоритетом.

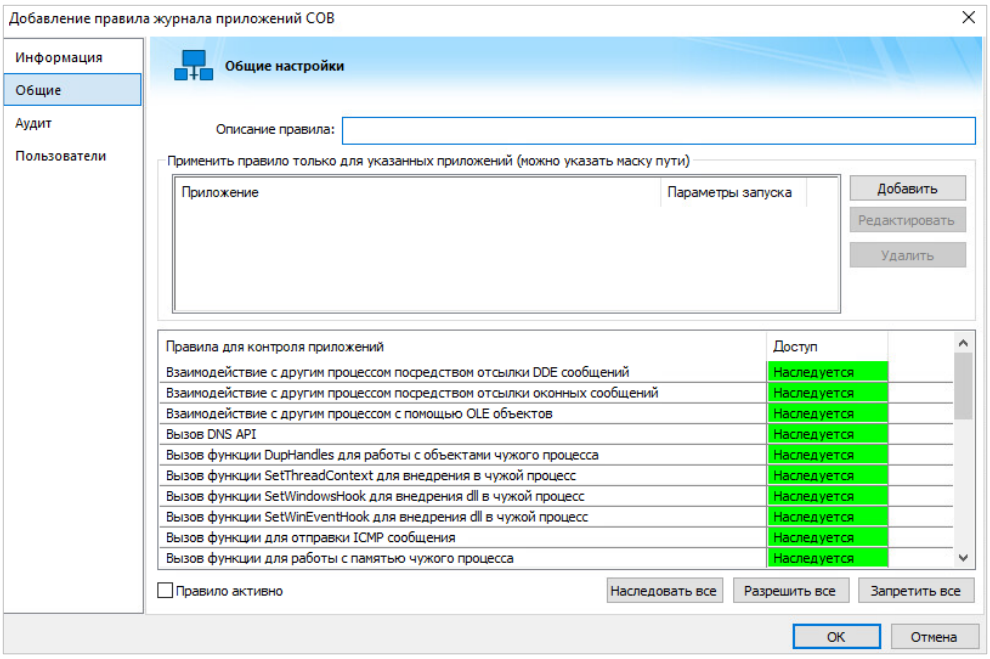


Рис. 313. Общие

В разделе *Аудит* есть возможность установить уровень журналирования событий успеха и отказа (рис. 314). Есть возможность наследовать значение параметров у правила выше приоритетом.

Уровень журналирования правил контроля приложений должен быть равен глобальному уровню журналирования **СОВ** или быть выше, подраздел 16.5.3 Настройки эвристики.

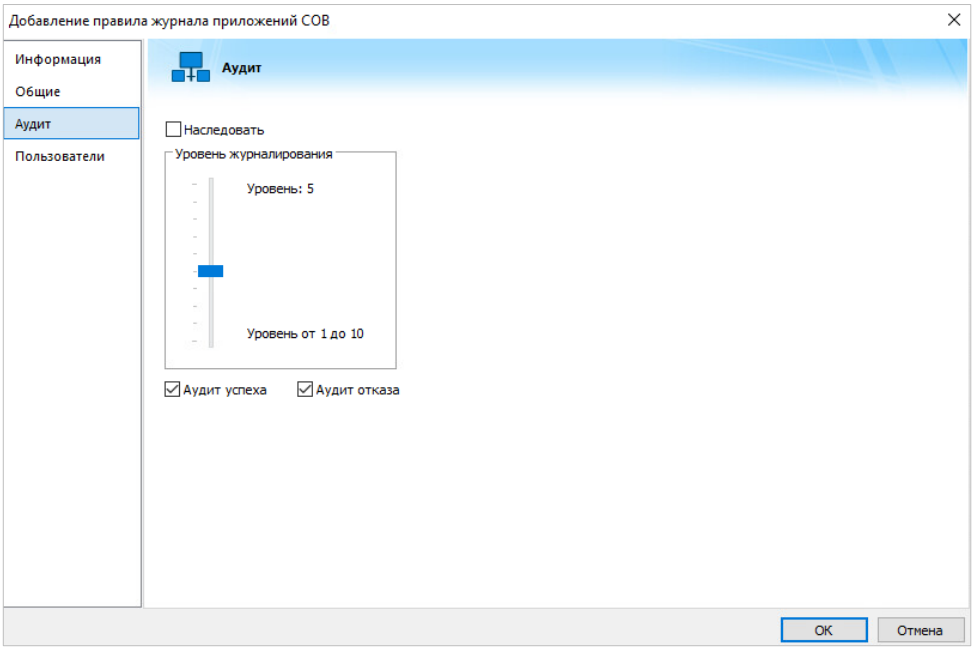


Рис. 314. Аудит

В разделе *Пользователи* отображается список пользователей, к которым будет применяться созданное правило.

Отметив пункт *Автоматический поиск пользователей/групп* при последующем нажатии кнопок **Пользователи** и **Группы** будет показан список всех возможных пользователей для последующего назначения прав.

При нажатии кнопки **Все** все пользователи и группы получают права доступа согласно создаваемому правилу. Удалить назначенные группы можно нажатием кнопки **Удалить** (рис. 315).

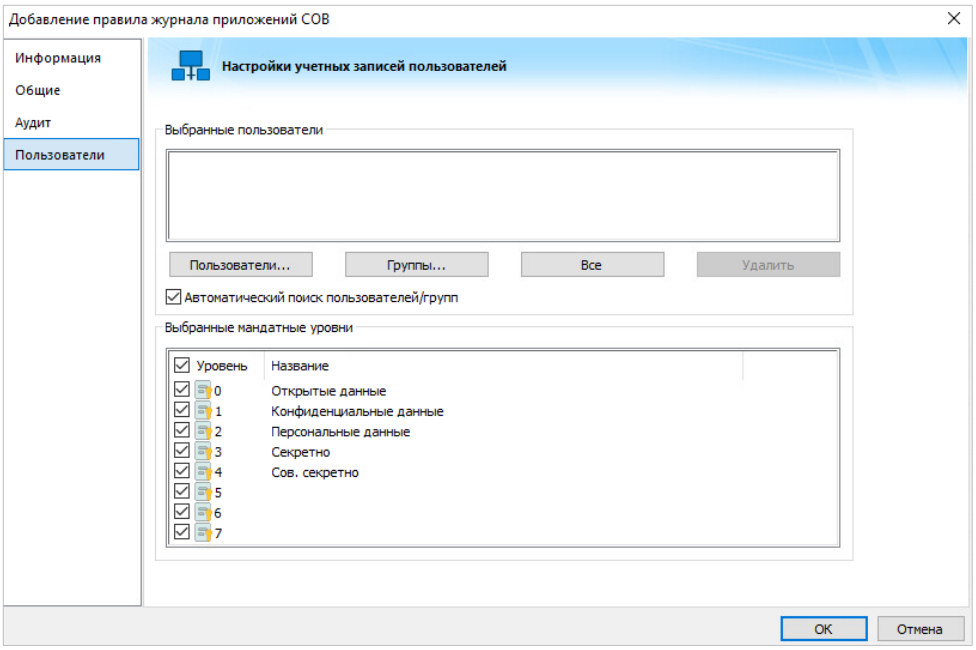


Рис. 315. Пользователи

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

Реализована возможность выбора мандатных уровней доступа пользователей, для которых будет применено правило (рис. 316).

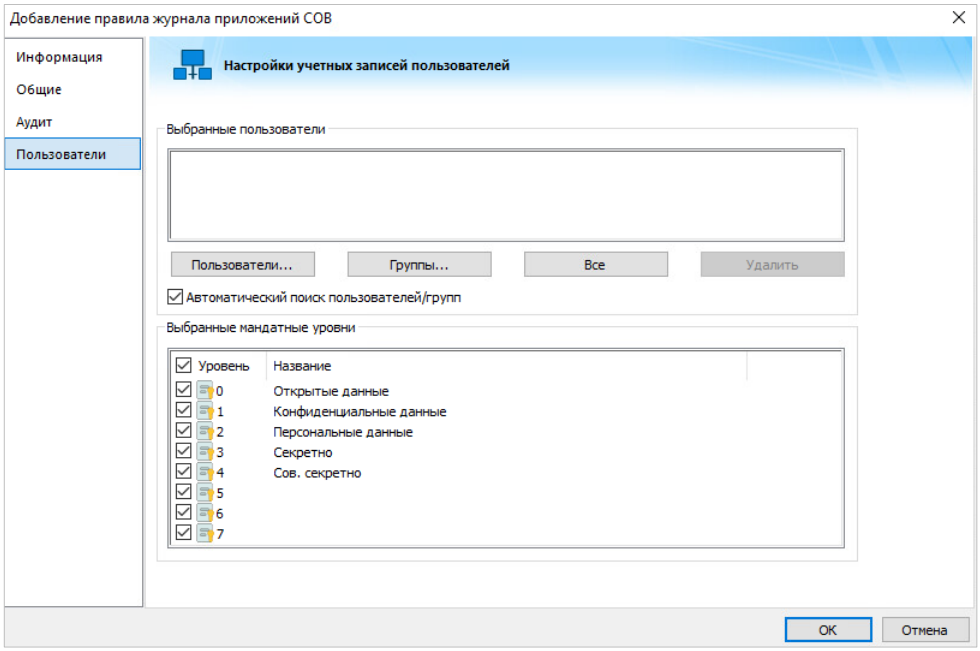


Рис. 316. Пользователи в редакции «С»

Рассмотрим пример создания нового правила.

Необходимо исключить возможность снятия снимка экрана приложением «Ножницы» для пользователя *user*. Для этого нужно перейти в категорию *Настройки СОВ* и нажать кнопку **Контроль приложений**. Затем необходимо щелкнуть правой кнопкой мыши на информационной панели и выбрать контекстном меню действие **Добавить**.

Далее в разделе *Общие* следует нажать кнопку **Обзор** и выбрать файл, расположенный по пути «C:\Windows\System32\SnippingTool.exe», после чего нажать кнопку **Добавить**.

В нижнем окне требуется выбрать все события, кроме **Получение контекста десктопа или активного окна (возможность снятие скриншота)** (рис. 317).

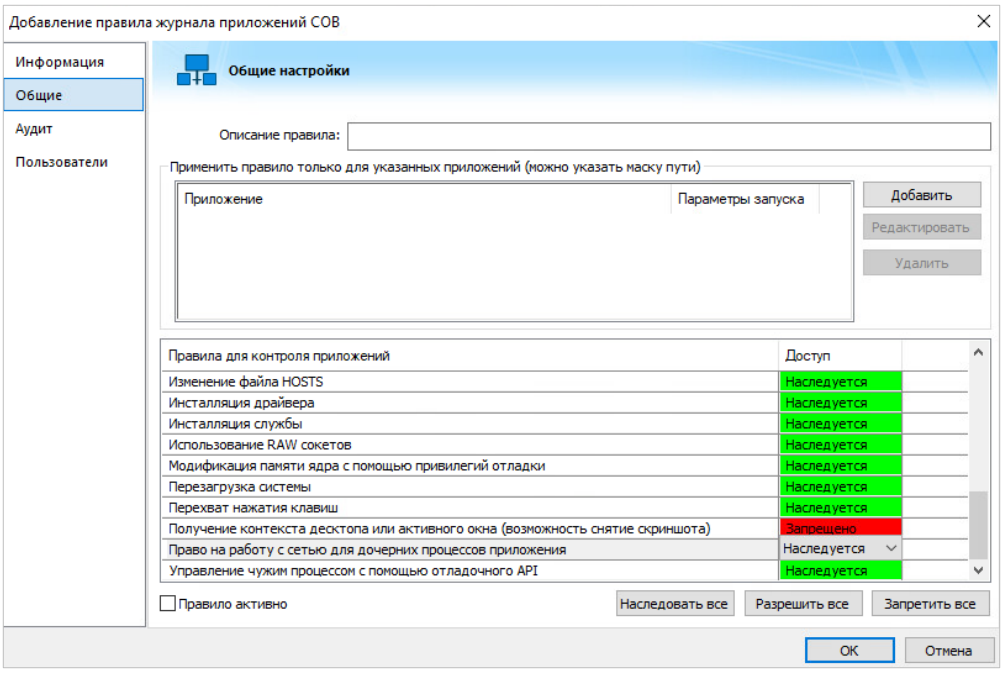


Рис. 317. Создание правила контроля приложений

В разделе пользователи можно выбрать пользователей, для которых будет применимо данное правило. По умолчанию все пользователи и группы получают права доступа согласно создаваемому правилу.

После необходимо активировать правило, это возможно сделать как в свойствах правила, так и на информационной панели действием **Активировать**.

Действия по изменению правил контроля приложений фиксируется в журнале управления политиками.

16.5.2 Контроль реестра

Подкатегория *Контроль реестра* позволяет ограничивать попытки ПО изменять в системном реестре настройки критических объектов ОС, такие как: автоматический запуск приложений, автоматический запуск системных приложений, правила обработки расширений файлов, ветка автоматически запускаемых **DLL** и т. д.

На информационной панели находится список групп и контролируемых ключей реестра (рис. 318).

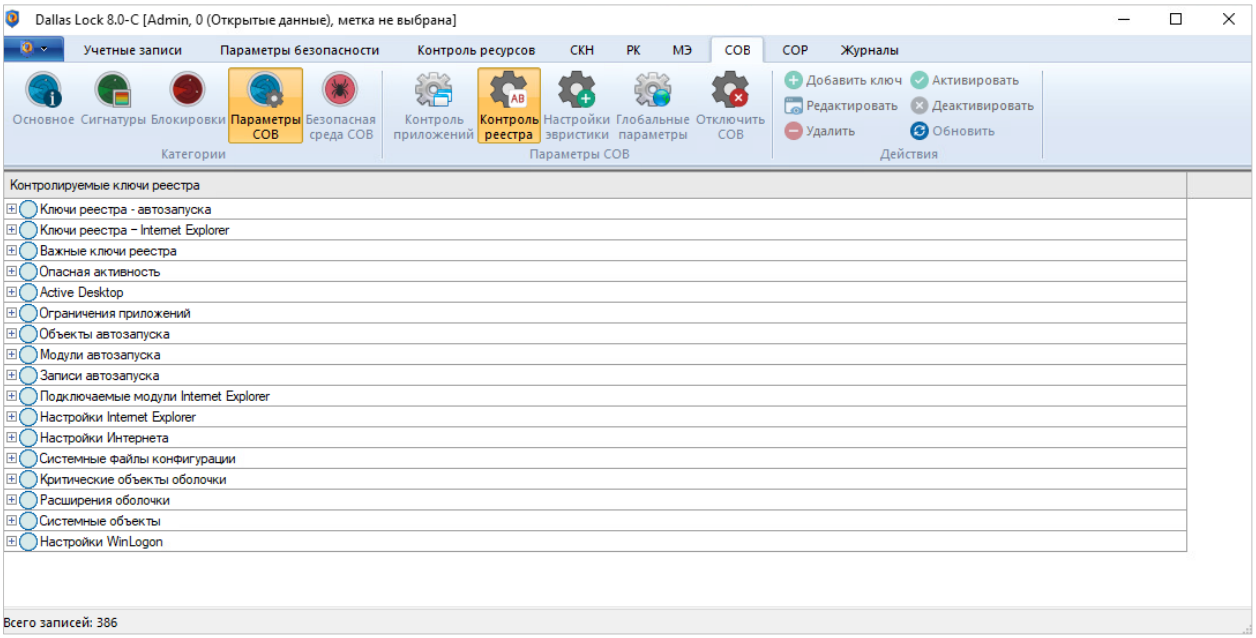


Рис. 318. Информационная панель контроля реестра

В настройках контроля реестра можно изменять ключи в фиксированном списке групп настроек, но

нельзя добавлять или удалять произвольные группы. Возможна активация и деактивация как отдельных ключей, так и групп целиком. Редактирование осуществляется аналогично редактированию других настроек **СОВ**.

Действия по изменению настроек контроля реестра фиксируются в журнале управления политиками.

16.5.3 Настройки эвристики

Данная подкатегория позволяет произвести настройку эвристического анализа, с целью обнаружения аномалий сетевого трафика.

Информационная панель содержит следующие рабочие области (рис. 319):

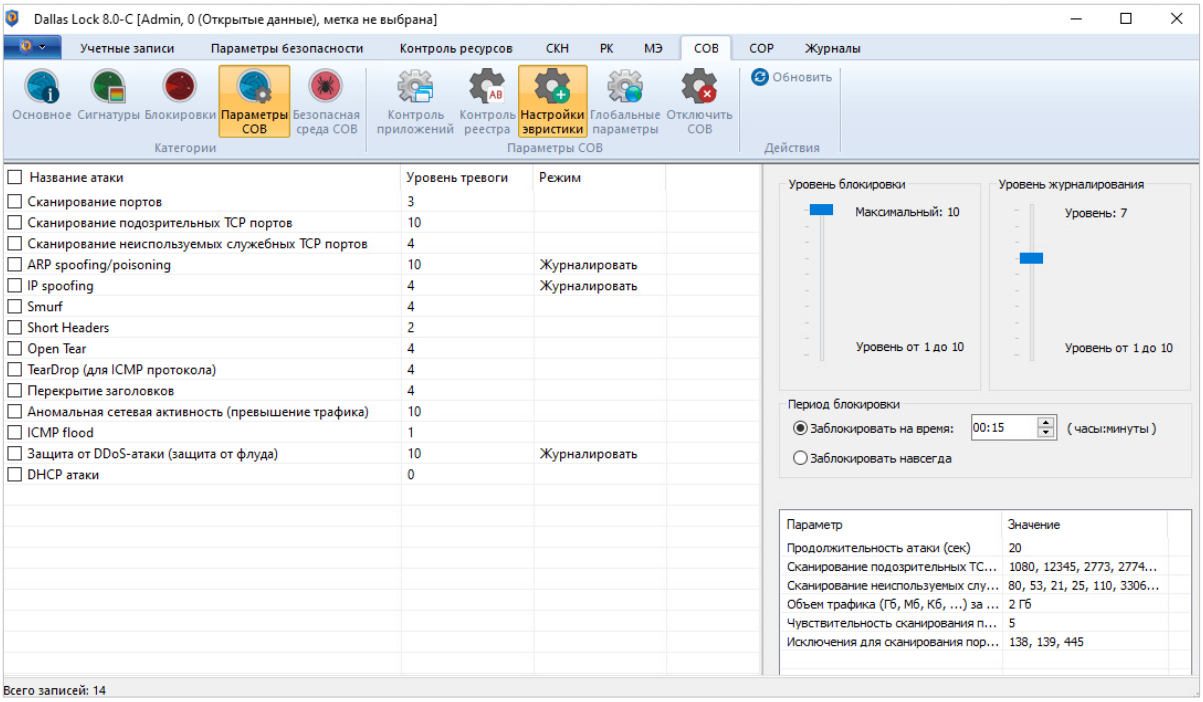


Рис. 319. Настройки эвристики

1. Список атак и их уровень тревоги. Для изменения уровня тревоги определенной атаки нужно щелкнуть два раза левой кнопкой мыши по значению и задать необходимое новое значение. Для того чтобы полностью отключить обнаружение отдельной атаки необходимо снять галочку у данной атаки.

Сканирование портов
Действие, предшествующее сетевой атаке, когда TCP и UDP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
Сканирование подозрительных TCP портов
Действие, предшествующее сетевой атаке, когда TCP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
Сканирование неиспользуемых служебных TCP портов
Действие, предшествующее сетевой атаке, когда TCP порты защищаемой системы опрашиваются с целью определения потенциальных уязвимостей.
ARP spoofing/poisoning
Техника сетевой атаки, основанная на использовании недостатков протокола ARP и позволяющая перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена.
IP spoofing
Атака, в процессе реализации, которой в значении поля IP-пакета «адрес отправителя» адрес атакующего подменяется на адрес доверенного хоста, после чего данный IP-пакет отправляется жертве.

Smurf
Атака заключается в передаче в сеть широковещательных ICMP запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к существенному снижению пропускной способности канала связи или к полной изоляции атакуемой сети.
Short Headers
Атака, направленная на выход из строя программы обработчика (заголовок датаграммы содержит менее 8 байт).
Open Tear
Атака использует случайно измененный исходный адрес и отправляет случайным образом фрагментированные UDP-пакеты на случайные порты.
TearDrop (для ICMP протокола)
Атака, заключающаяся в отправке на атакуемый узел не всех фрагментов пересылаемого пакета, что приводит к ошибкам при сборке полученной датаграммы.
Перекрытие заголовков
Атака, заключающаяся в отправке на атакуемый узел датаграммы с некорректно установленными параметрами, начала и длины фрагментов. Параметры фрагментов пересекаются при сборке полученной датаграммы в памяти компьютера, что приводит к ошибкам.
Аномальная сетевая активность (превышение трафика)
Неожиданно большой объем трафика, свидетельствующий об атаке на защищаемую систему.
ICMP (flood)
Атака на сетевое оборудование, ставящая своей целью отказ в обслуживании. Заключается в отправке большого количества ICMP Echo запросов жертве с разных IP-адресов.
Защита от DDoS-атаки (защита от флуда)
Атака типа «Отказ в обслуживании», то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднен.
DHCP-атаки
DHCP-атаки, направленные на эксплуатацию уязвимостей протокола DHCP для перехвата трафика, отказа в обслуживании или перенаправления сетевых запросов: DHCP флуд клиента, DHCP флуд сервера, истощение DHCP аренды IP адресов, поддельный DHCP сервер. К активностям относятся: появление нового DHCP-сервера в сети и несанкционированное изменение IP-адреса существующего DHCP-сервера.

2. Глобальные **Уровень блокировки** и **Уровень журналирования**, применимые к сигнатурам трафика и правилам контроля приложений. Данные уровни отвечают за количество баллов, при наборе которых произойдет реагирование на атаку. Для того, чтобы изменить уровень, необходимо передвинуть ползунок вверх или вниз. При срабатывании уровня журналирования — событие занесется в соответствующий журнал, при срабатывании уровня блокировки — произойдет блокировка атакующего (там, где это применимо).
3. Дополнительные настройки эвристики. Данные настройки позволяют настроить общие глобальные настройки эвристики, общие для всех атак.
   - Продолжительность атаки (сек) — время, в течение которого учитываются атаки с одного источника для набора баллов тревоги и журналирования.
   - Сканирование подозрительных TCP портов — перечисляется список TCP портов, сканирование которых является атакой с высокой степенью вероятности.
   - Сканирование неиспользуемых служебных TCP портов — перечисляется список TCP портов, сканирование которых (в случае, если данные порты «закрыты») является атакой со значительной степенью вероятности.
   - Время блокировки (мин) — время блокировки обнаруженного источника атаки.
   - Объем трафика (Гб, Мб, Кб) за 10 мин., для определения аномальной сетевой активности — указывается объем трафика для определения аномальной сетевой активности.

- Чувствительность сканирования портов — в данном параметре указывается количество сканируемых портов, для реагирования на атаки «Сканирования портов и «Сканирования неиспользуемых служебных TCP портов».
- Исключения для сканирования портов — перечисляется список TCP портов, сканирование которых не является атакой.

Процесс настройки параметров эвристики для разных типов атак.

1. **«Сканирование портов»** и **«Сканирование неиспользуемых служебных TCP портов»**.

   Для атак на TCP-порты существует формула подсчета баллов:

$$W = \frac{a*b}{c},$$

   где a — «Уровень тревоги», b — количество просканированных портов, c — «Чувствительность сканирования портов».

Пример

Предположим, что «Уровень блокировки» равен 10, а «Уровень журналирования» 7.

Атакующий произвел сканирование 15 портов в течение 20 секунд. Уровень тревоги для атаки «Сканирование портов» равняется 3, а «Чувствительность сканирования портов» 5. Исходя из этих данных, набрано 9 баллов:

$$W = \frac{3 * 15}{5}$$

Данная атака не заблокируется, но при этом будет зафиксирована в журнале трафика. Иначе говоря, если при условиях, представленных выше:

- набрано 16 баллов — атака блокируется и журналируется;
- набрано 7 баллов — атака не блокируется, но журналируется;
- набрано 5 баллов — атака не блокируется и не журналируется.

Чтобы избежать ложных срабатываний **СОВ**, для атак на UDP-порты, значение параметра «Чувствительность сканирования портов» увеличивается в 3 раза.

2. **Остальные атаки.**

   Для всех остальных атак также существует формула подсчета баллов:

$$K = a * b,$$

   где a — «Уровень тревоги» атаки, b — количество атак или просканированных портов.

   При срабатывании блокировки атаки, в области уведомлений Windows на панели задач появится сообщение с информацией о блокировке (рис. 320).

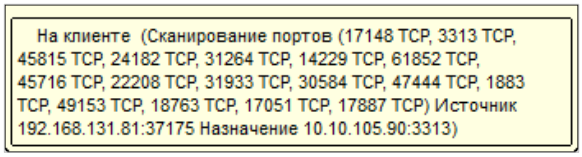


Рис. 320. Уведомление о блокировке источника атаки

Действия по изменению настроек эвристики фиксируются в журнале управления политиками.

16.5.4 Глобальные параметры

В подкатегории *Глобальные параметры* предусмотрена настройка обновления базы решающих правил (далее — БРП), в частности сигнатур, и других параметров (рис. 321):

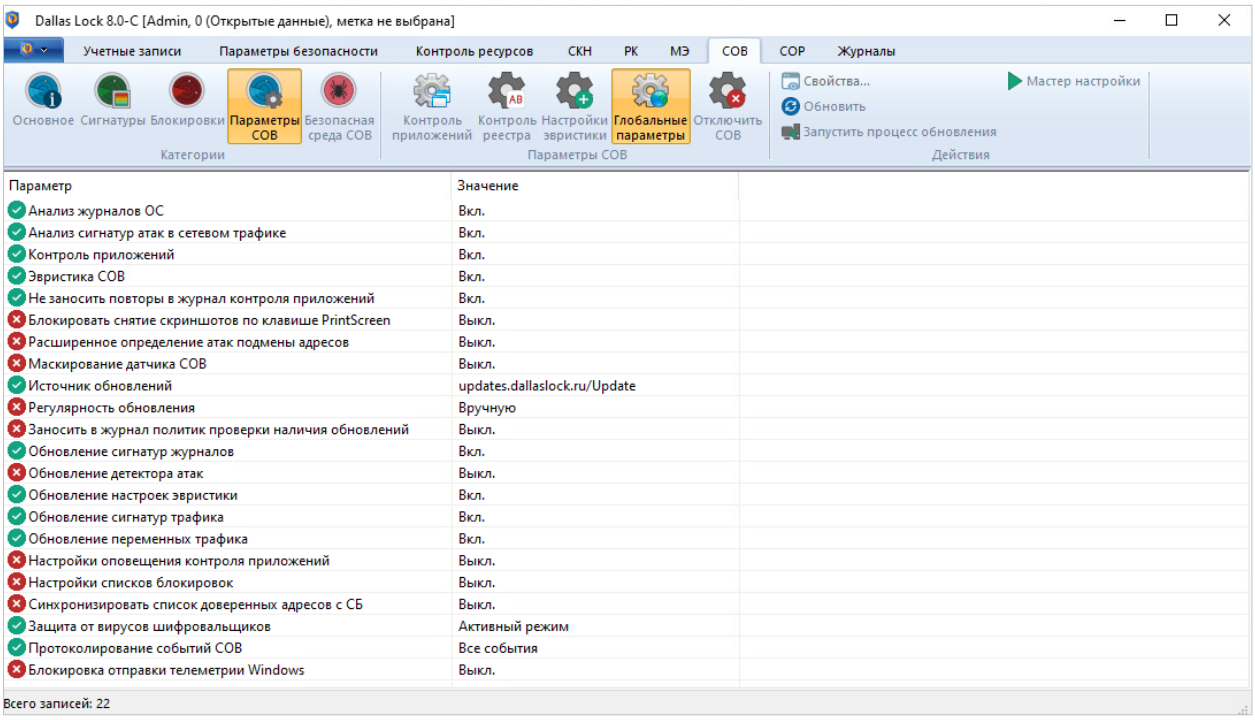


Рис. 321. Список глобальных параметров

Анализ журналов ОС

Данный параметр позволяет включать/отключать сигнатурный эвристический анализ, использующий журналы ОС и приложений.

Анализ сигнатур атак в сетевом трафике

Данный параметр позволяет включать/отключать сигнатурный эвристический анализ, использующий **Журнал трафика** (независимо от блокировки атак на протоколы).

Контроль приложений

Данный параметр позволяет включать/отключать функционирование контроля приложений.

Эвристика СОВ

Данный параметр позволяет включать/отключать блокировку атак на протоколы и сканирование портов (независимо от анализа сигнатур сетевого трафика).

Не заносить повторы в журнал контроля приложений

Включение данного параметра позволяет фильтровать повторяющиеся однотипные события в журнале контроля приложений.

Блокировать снятие скриншотов по клавиатуре PrintScreen

Включение данного параметра позволяет блокировать процесс копирования изображения текущего состояния экрана в буфер обмена при нажатии клавиши Print Screen.

Расширенное определение атак подмены адресов

Включение данного параметра позволяет минимизировать ложные срабатывания обнаружения некоторых атак при получении сетевым адаптером пакетов, адресованных не только непосредственно данному адаптеру (это актуально, например, при использовании виртуальных машин VMware в сетевом режиме Bridged).

Маскирование датчика СОВ

Данный параметр позволяет скрыть наличие датчика **СОВ** для пользователей, не имеющих прав на просмотр и изменение настроек **СОВ**. Для таких пользователей не будут появляться уведомления **СОВ**, а также в меню значка блокировки скроется пункт **СОВ**.

Источник обновлений

Данный параметр позволяет задать источник обновления БРП.

По умолчанию параметры подключения к интернету определяются автоматически. Если используется прокси-сервер, необходимо настроить параметры прокси-сервера в свойствах обозревателя или браузера в зависимости от версии Windows.

Регулярность обновления

Данный параметр отвечает за регулярность обновления БРП.

При выполнении обновления Измененные пользователем значения параметров настроек сохраняются, при использовании мастера настройки защищенных механизмов СОВ данные изменения могут быть отменены обновлением СОВ.

Существует 3 режима обновлений: вручную, раз в час и раз в сутки. При выборе обновления вручную обновление не произойдет до тех пор, пока не будет нажата кнопка **Запустить процесс обновления** на панели **Действия** или в контекстном меню значка блокировки (рис. 322).

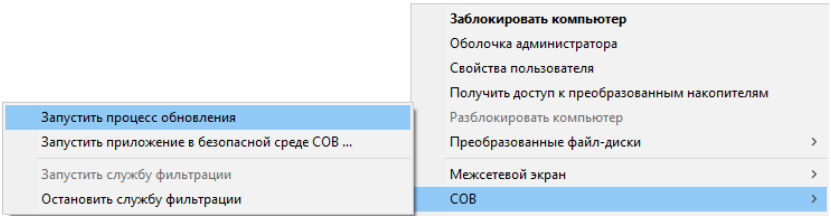


Рис. 322. Запуск процесса обновления БРП

После применения обновления, в журнал управления политик производится соответствующая запись.

Заносить в журнал политик проверки наличия обновлений

Включение данного параметра позволяет вести учет проверок на наличие обновлений в журнале управления политиками.

Обновление сигнатур журналов

Включение/отключение обновления сигнатур журналов при ручном или автоматическом обновлении.

Обновление детектора атак

Включение/отключение обновления детектора атак при ручном или автоматическом обновлении.

Обновление настроек эвристики

Включение/отключение обновления настроек эвристики при ручном или автоматическом обновлении.

Обновление сигнатур трафика

Включение/отключение обновления сигнатур трафика при ручном или автоматическом обновлении.

Обновление переменных трафика

Включение/отключение обновления переменных трафика при ручном или автоматическом обновлении.

Настройки оповещения контроля приложений

Данный параметр позволяет произвести настройку оповещений для контроля приложений. Для каждой системной функции возможно указать следующее:

- максимальное количество событий в день для информационного оповещения;
- максимальное количество событий в день для оповещения об опасной активности;
- максимальное количество событий в неделю для информационного оповещения;
- максимальное количество событий в неделю для оповещения об опасной активности.

При достижении порогового значения выводится соответствующее всплывающее сообщение на

панели задач.

После превышения порогового значения подсчет количества событий прекращается.

Настройки списков блокировок

Данный параметр позволяет включать/отключать использование файлов блокировки, управлять составом файлов блокировки и частотой их опроса. По умолчанию параметр имеет значение «*Выкл.*».

В диалоговом окне свойств параметра «Настройка списка блокировок» можно добавлять следующие типы адресов файлов:

- для файлов на сервере в сети Интернет http(s)://<Site>/<fileName>.txt;
- для файлов на жестком диске <Drive>:\<Path>\<fileName>.txt;

для файлов на сетевом диске \\<Server>\<Path>\<fileName>.txt, причем эти файлы должны быть доступны без ввода логина и пароля, то есть должен быть установлен общий доступ к этим файлам на чтение.

Не функционирует опрос файла с блокировками, расположенный в сетевом каталоге из-за отсутствия доступа к нему у учетной записи System, под которой работает служба фильтрации DllpsService на защищенном АРМ.

Синхронизировать список адресов с СБ

Данный параметр позволяет включать/отключать синхронизацию списка доверенных адресов с **СБ**. По умолчанию параметр имеет значение «*Выкл.*».

Защита от вирусов шифровальщиков

Данный параметр позволяет осуществлять настройку механизма защиты от вирусов-шифровальщиков, который нацелен на обнаружение неизвестных антивирусным базам вредоносных программ по их поведению.

Допустимые значения:

- «Не используется» — осуществляется отключение механизма защиты от вирусов-шифровальщиков;
- «Режим аудита» — осуществляется обнаружение работы вируса-шифровальщика и информирование об этом администратора безопасности;
- «Активный режим» — реализуется обнаружение вируса-шифровальщика и минимизация ущерба от его действий;
- «Активный режим с очисткой» — реализуется обнаружение вируса-шифровальщика и минимизация ущерба от его действий, а также осуществляется удаление созданных в процессе работы вируса-шифровальщика исполняемых файлов, что позволяет избежать повторного запуска вредоносной программы;
- «Активный режим с восстановлением» — реализуется обнаружение вируса-шифровальщика и остановка вредоносных процессов, а затем осуществляется восстановление данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

По результатам работы механизма создается лог-файл, в котором содержится информация о принудительно завершенных процессах, о действиях в системе, которые они совершали и которые были классифицированы как вредоносные, список безвозвратно утерянных файлов и т. д.

При обнаружении ложноположительного срабатывания приложение можно добавить в исключения.

По умолчанию параметр имеет значение «*Активный режим*».

Поскольку обнаружение вредоносной активности происходит не моментально, к моменту начала работы подсистемы реагирования часть файлов будет безвозвратно зашифрована. Важно отметить, что это не относится к режиму «Активный режим с восстановлением».

Эффективность защиты зависит от количества потенциальных целей для вируса в системе — в «чистых» системах и системах с небольшим количеством пользовательских файлов возможности механизма по обнаружению шифровальщиков могут быть ограничены.

Протоколирование событий СОВ
Данный параметр позволяет выбрать регистрируемые события об изменении конфигурации **СОВ**.
Блокировка отправки телеметрии Windows
Данный параметр предназначен для ограничения сбора диагностических данных и их отправки на серверы Microsoft, с выбором периодичности автоматического обновления файлов (частота опроса 7, 10 или 30 суток). По умолчанию параметр имеет значение «*Выкл*». Установка контроля целостности на определенные ветки реестра может вызвать конфликт в работе политики «Блокировка отправки телеметрии Windows». Рекомендуется производить установку контроля целостности после включения политики.

Для удобства настройки глобальные параметры имеют всплывающие подсказки с кратким описанием функциональных возможностей.

Действия по изменению глобальных параметров фиксируются в журнале управления политиками.

Мастер настройки

Назначением мастера настройки **СОВ** является снижение трудоемкости для эффективной настройки **СОВ**, позволяя в упрощенном интерфейсе определить требуемые уровни защищенности системы без проведения индивидуальных и точных настроек.

Для того, чтобы задать уровни защищенности с помощью мастера настроек, необходимо:

1. В блоке **Параметры СОВ → Глобальные параметры** нажать кнопку **Мастер настройки** на панели **Действия** или в контекстном меню рабочей области.
2. В появившемся окне **Мастер настройки защитных механизмов СОВ** (рис. 323) выбрать уровень защиты компонетов **СОВ**.
   - Для **защиты от сетевых атак** доступны следующие уровни защиты:
     - **«Высокий»** уровень защиты активирует набор настроек, включающий максимальное количество детектируемых атак, высокую чувствительность датчиков **СОВ**, расширенный набор сигнатур, используемых при анализе сетевого трафика. Данный уровень также включает в себя настройки «среднего» и «низкого» уровней защиты.
     - **«Средний»** уровень защиты активирует набор настроек, включающий рекомендуемый перечень детектируемых атак, наиболее часто применяемых или оказывающих критическое влияние на ЗАРМ, набор сигнатур трафика для наиболее распространенных (опасных) сетевых атак. Характеризуется оптимальным соотношением чувствительности датчиков СОВ и возможных ложных срабатываний. Средний уровень включает в себя настройки «низкого» уровня защищенности.
     - **«Низкий»** уровень защиты активирует набор настроек, обеспечивающий обнаружение (предотвращение) вторжений только наиболее опасных (для обеспечения конфиденциальности, целостности и доступности информации) атак, критически влияющих на защищенность системы, и характеризуется малым процентом ложных срабатываний.
     - **«Выкл»** — отключает защиту от сетевых атак **СОВ**. Переводит параметр «Анализ сигнатур атак в сетевом трафике» в состояние «*Выкл*.».

     При необходимости возможно включить **Расширенное определение атак подмены адресов**, а также задать время блокировки атакующего компьютера.
   - Для **защиты реестра** доступны следующие уровни защиты:
     - **«Высокий»** уровень защиты активирует набор правил, обеспечивающий контроль всех важных ключей реестра, критически влияющих на защищенность системы.
     - **«Средний»** уровень защиты активирует набор правил, обеспечивающих контроль большинства ключей реестра, критически влияющих на защищенность системы, за исключением групп правил «Active Desktop», «Ограничения приложений» и «Системные файлы конфигурации».
     - **«Низкий»** уровень защиты активирует набор правил, обеспечивающий контроль наиболее важных ключей реестра, критически влияющих на защищенность системы.

- **«Выкл»** — отключает контроль реестра. Деактивирует все правила контролируемых ключей реестра (вкладка *Контроль реестра*).

- Для **контроля приложений** доступны следующие уровни защиты:
  - **«Высокий»** уровень защиты задает ограничения для подписанных приложений, запрещая использовать сетевые небезопасные функции и отладочные функции управления потоками, вызывать DNS API, запускать службы и неподписанные дочерние процессы. Для неподписанных приложений ограничивается вызов DNS API, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Данный уровень также включает в себя настройки «среднего» и «низкого» уровней защиты.
  - **«Средний»** уровень защиты задает ограничения для подписанных приложений, запрещая использовать небезопасные сетевые функции, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Для неподписанных приложений ограничивается вызов DNS API, использование функций межпроцессного взаимодействия и расширенного списка отладочных функций. Средний уровень включает в себя настройки «низкого» уровня защищенности.
  - **«Низкий»** уровень защиты задает минимальные ограничения для подписанных приложений, запрещая использовать отладочные API и RAW сокеты. Для неподписанных приложений запрещается все, кроме использования функций межпроцессного взаимодействия, запуска подписанных и неподписанных процессов.
  - **«Выкл»** — отключает контроль приложений. Переводит параметр **Контроль приложений** в состояние «*Выкл.*».

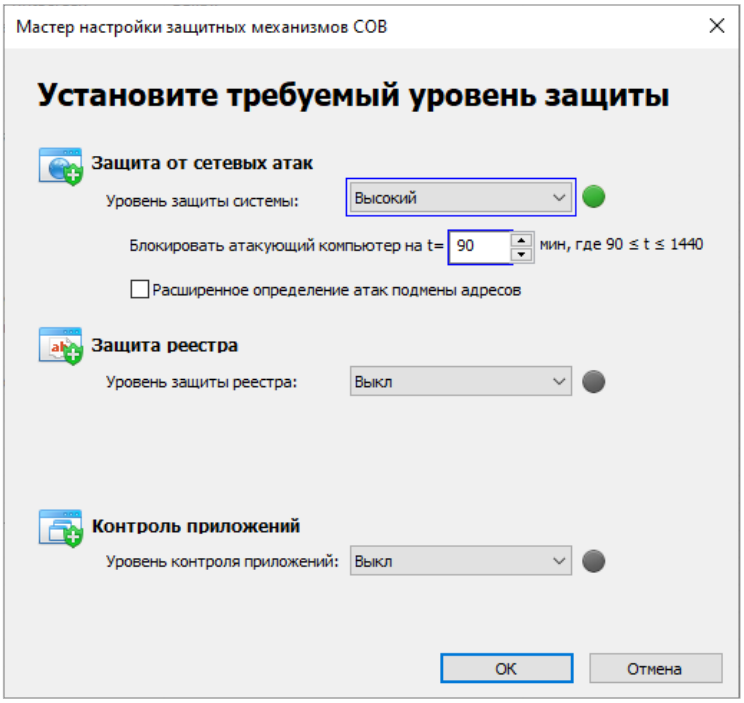


Рис. 323. Мастер настройки защитных механизмов СОВ

16.5.5 Отключить СОВ

Для временного прекращения работы **СОВ** необходимо нажать кнопку **Отключить СОВ** на панели **Параметры СОВ** и в появившемся окне подтвердить действие (рис. 324).

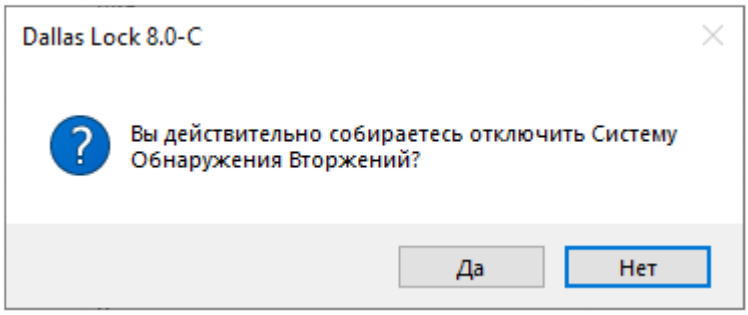


Рис. 324. Отключение СОВ

16.6 Безопасная среда СОВ (песочница)

В **СЗИ** реализована возможность запускать стороннее ПО в изолированной, безопасной среде — песочнице. В результате запуска стороннего ПО, в песочнице проводится анализ поведения такого приложения в изолированной среде. По результатам анализа реализована возможность автоматического закрытия приложения, в случае обнаружения угроз безопасности и информирование пользователя (администратора) о результатах проверки.

16.6.1 Настройки

Уполномоченному пользователю предоставляется возможность на вкладке **СОВ** оболочки администрирования **СЗИ** выбрать категорию **Безопасная среда СОВ**, после чего пользователь может произвести настройку безопасной среды в подкатегории *Настройки* (рис. 325).

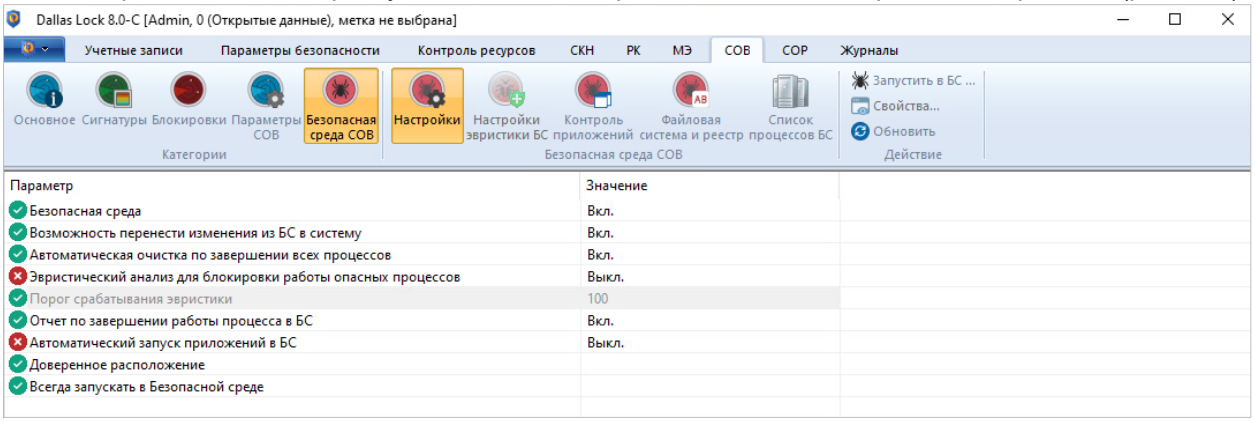


Рис. 325. Панель настройки безопасной среды СОВ

Доступны следующие параметры:

Безопасная среда
Параметр позволяет включать и отключать **БС**. По умолчанию имеет значение «*Вкл.*».
Возможность перенести изменения из БС в систему
Параметр позволяет пользователю отключить сохранение результатов работы процесса, запущенного в БС. Если данный параметр включен, перед сохранением пользователю будет выведено диалоговое окно с вопросом на сохранение изменений, выполненных завершенным процессом. По умолчанию имеет значение «*Вкл.*».
Автоматическая очистка по завершению всех процессов
Данный параметр позволяет пользователю определить будет ли производиться автоматическая очистка временных каталогов от содержимого, созданного процессом или процессами, запущенными в безопасной среде. По умолчанию имеет значение «*Вкл.*».
Эвристический анализ для блокировки работы опасных процессов
Параметр позволяет разрешить безопасной среде применять эвристический анализ для принудительного завершения работы опасных процессов согласно настройкам эвристического анализа, указанным в категории **Безопасная среда СОВ → Настройки эвристики БС**, раздел 16.6.2 Настройки эвристики безопасной среды. Параметру задается значение **Режим ручной настройки**, при котором пользователь самостоятельно определяет весовые коэффициенты и

значение параметра **Порог срабатывания эвристики**, которые в этом режиме доступны для редактирования. При переключении с **Режима ручной настройки** на **Режим с настройками по умолчанию** будет выведено сообщение сбросе настроек на значения по, раздел 16.6.2 Настройки эвристики безопасной среды.

Параметру может быть задано значение **Режим с настройками по умолчанию** для автоматического определения и завершения потенциально опасных приложений, запущенных в режиме БС, с учетом настроек весов правил эвристического анализа по умолчанию. При этом параметр **Порог срабатывания эвристики** не активен, кнопка **Настройка эвристики БС** активна, но настройки весов недоступны для редактирования. При нажатии на кнопку **Настройки эвристики БС** и при двойном клике на параметре **Порог срабатывания эвристики** выводится сообщение: «*Для разрешения редактирования настроек включите «Режим ручной настройки» в «Эвристическом анализе для блокировки работы опасных процессов*».

При заданном значении параметра «*Выключен*» (по умолчанию) параметр **Порог срабатывания эвристики** и кнопка **Настройки эвристики БС** не активны и действия по принудительному завершению процесса со стороны БС предприниматься не будут. Уполномоченный пользователь может запустить приложение в БС и самостоятельно принять решение о его завершении.

Порог срабатывания эвристики

Параметр является накопительным счетчиком весов срабатываний правил эвристики, расположенных в подкатегории *Настройки эвристики БС*, по достижению значения (по умолчанию равного «100») которого приложение, запущенное в БС, будет принудительно завершено.

Параметр может принимать значения в диапазоне от 0 до 1000 единиц. Если при включенной эвристике значение порога срабатывания указано «0», то любое приложение, выполнившее любое действие из списка правил настройки эвристического анализа, будет немедленно закрыто. Таким образом возможно блокировать любые потенциально опасные действия подозрительного ПО в БС. При значении от 1 до 1000 происходит накопление счетчиком всех срабатываний указанных настроек эвристического анализа в виде последовательного сложения значений веса первого параметра, если данное действие было выявлено в первый раз, и значения веса последующих срабатываний, если действие было выявлено во второй и последующий разы. Данное действие происходит при срабатывании каждого правила эвристики.

При каждом увеличении счетчика происходит сравнение его значения со значением параметра. В случае, если значение параметра больше значения счетчика, то БС продолжает фиксацию действий приложения с увеличением счетчика согласно значениям весов, указанным в настройках. В случае, если значение порога срабатывания эвристики равно или меньше значения счетчика, то БС завершает работу приложения и предлагает пользователю открыть отчет, а также сохранить данные из БС. При завершении работы приложения в БС по достижению значения параметра в журнале контроля приложений фиксируется последнее действие, добавление веса которого привело к завершению процесса в БС по порогу эвристики. Все остальные действия подлежат записи в отчет.

Отчет по завершению работы процесса в БС

Параметр разрешает **СЗИ** формировать отчет с результатами контроля ПО, запущенного в БС с уведомлением пользователя. По умолчанию имеет значение «*Вкл.*».

Автоматический запуск приложений в БС

Параметр позволяет автоматически запускать в безопасной среде исполняемые файлы и приложения, ассоциированные с неисполняемыми файлами, а также файлы, запускаемые из недоверенных источников. Доверенные источники указываются в параметре **Доверенное расположение**.

По умолчанию параметр имеет значение «*Выкл.*».

Доверенное расположение

Параметр содержит пути к доверенным директориям, имеющим сетевое расположение, либо находящимся на съемном носителе. Запуск программ и файлов из этих директорий в автоматическом режиме не производится.

Для добавления и удаления доверенных директорий и носителей информации необходимо открыть окно редактирования свойств параметра, воспользовавшись соответствующей кнопкой в панели **Действия** или в контекстном меню, либо вызвать данное окном двойным кликом мыши на выбранном параметре.

Затем необходимо перейти на соответствующую вкладку и в случае добавления директории

указать соответствующий путь, в случае добавления носителя информации — выбрать подключенный носитель из выпадающего списка, затем нажать кнопку **Добавить** (Рис. 326).

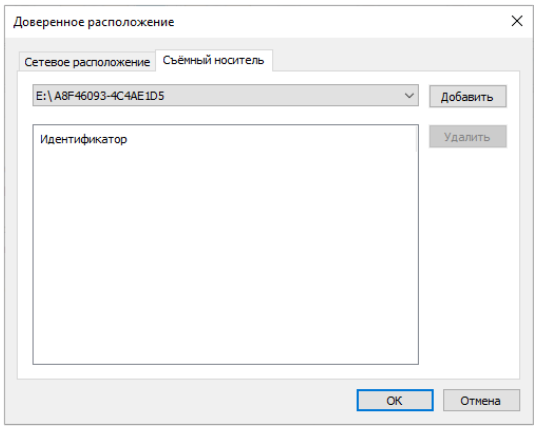


Рис. 326. Добавление доверенного носителя информации

Для удаления директории или съемного носителя из списка доверенных необходимо выбрать их в списке и нажать кнопку **Удалить**.

Всегда запускать в Безопасной среде

Параметр **Всегда запускать в Безопасной среде** обеспечивает запуск программы или скрипта в контролируемой и ограниченной среде, чтобы минимизировать потенциальные угрозы безопасности для системы. В безопасной среде могут быть применены различные механизмы, такие как изоляция ресурсов, ограничение доступа к файлам и сети, контроль прав доступа и прочее.

Чтобы добавить или удалить элементы, нужно открыть окно редактирования свойств параметра. Это выполняется нажатием на соответствующую кнопку в панели **Действия** или в контекстном меню, либо двойным щелчком мыши по выбранному параметру. Затем необходимо перейти на соответствующую вкладку. Для добавления директории указывается путь и необходимо нажать кнопку **Добавить**. Для удаления элементов из списка доверенных нужно выбрать их и нажать кнопку **Удалить**.

Для корректной работы ОС не рекомендуется добавлять системные или затрагивающие критические системные функции приложения в список **Всегда запускать в Безопасной среде**. Принудительный запуск таких приложений в БС приведет ОС к неработоспособности.

16.6.2 Настройки эвристики безопасной среды

Настройки эвристического анализа в *Безопасной среде* расположены на вкладке *СОВ* оболочки администрирования **СЗИ** в категории **Безопасная среда СОВ** в подкатегории *Настройки эвристики БС* и доступны, если для параметра **Эвристический анализ для блокировки работы опасных процессов** установлено значение *Режим ручной настройки*. Для удобства пользователя параметр **Порог срабатывания эвристики** вынесен в подкатегорию *Настройки*.

Настройки содержат поля *Правило эвристики*, *Вес первого срабатывания*, *Вес последующих срабатываний* (рис. 327):

- «Правило эвристики» содержит наименование настраиваемого правила;
- «Вес первого срабатывания» определяет то количество единиц, которое прибавляется к значению счетчика в случае первого обнаружения действия из списка настроек, может задаваться в диапазоне от 0 до 1000;
- «Вес последующих срабатываний» определяет то количество единиц, которое прибавляется к значению счетчика в случае второго и последующих обнаружений действия из списка настроек, может задаваться в диапазоне от 0 до 1000.

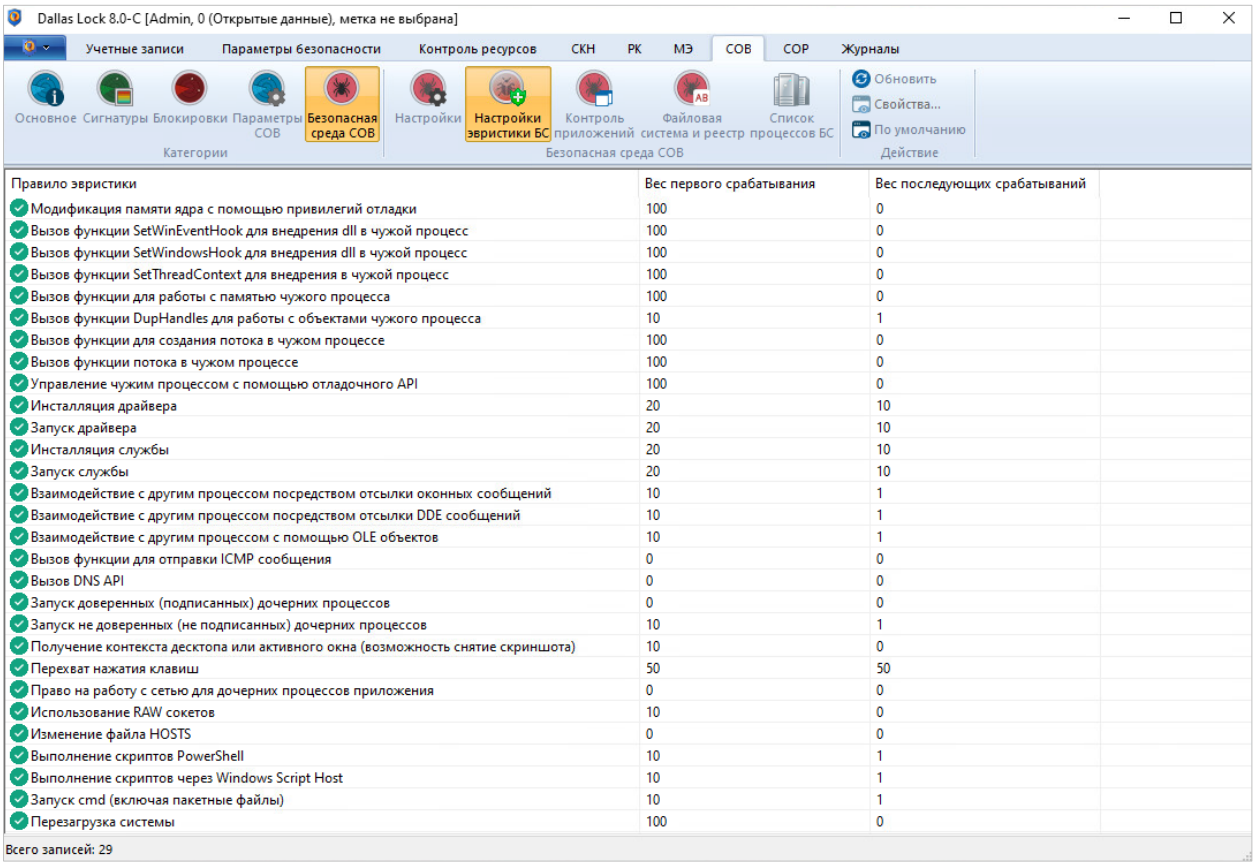


Рис. 327. Панель «Настройки эвристики БС»

Применение двух весов срабатывания позволяет максимально гибко настроить БС для более безопасного и удобного использования. Настройки эвристики БС имеют предустановленные параметры весов, указанные по умолчанию. Эти правила используются для пользователей, не имеющих прав на настройку параметров **СОВ** и БС. Для возврата всех настроек к значениям по умолчанию необходимо нажать кнопку **По умолчанию** в блоке **Действие**.

При включении блокировки межпроцессорного взаимодействия в БС завершаются процессы межпроцессорного взаимодействия в том случае, если превышен порог срабатывания по эвристике для операций, выходящих за рамки БС. При проверке на превышение порога срабатывания по эвристике берется разность между общим счетчиком весов срабатываний и счетчиком весов для процессов внутри БС (не учитывается взаимодействие с процессами, которые находятся внутри БС). В отчет вносится общее число срабатываний.

Доступны следующие настройки эвристики БС:

Модификация памяти ядра с помощью привилегий отладки
Позволяет определять попытки потенциально зловредного ПО проводить модификацию памяти ядра через получения привилегий отладки. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetWinEventHook для внедрения dll в чужой процесс
Позволяет определять функцию системного перехватчика SetWinEventHook для внедрения динамических библиотек в процесс другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetWindowsHook для внедрения dll в чужой процесс
Позволяет определять функцию системного перехватчика SetWindowsHook для внедрения динамических библиотек в процесс другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции SetThreadContext для внедрения в чужой процесс
Позволяет определять функцию SetThreadContext для внедрения исполняемого кода в процесс

другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции для работы с памятью чужого процесса
Позволяет определять функции, с помощью которых потенциально зловредное ПО может произвести внедрение постороннего кода в адресное пространство другого приложения. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции DupHandles для работы с объектами чужого процесса
Позволяет определять функцию DupHandles, используемую для работы с объектами чужого процесса. Значения по умолчанию: вес первого срабатывания — 10; вес последующих срабатываний — 1.
Вызов функции для создания потока в чужом процессе
Позволяет определять функции, создающие поток в чужом процессе. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Вызов функции потока в чужом процессе
Позволяет определять вызов функции потока в чужом процессе. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Управление чужим процессом с помощью отладочного API
Позволяет определять попытки потенциально зловредного ПО управлять чужим процессом с помощью отладочного API. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.
Инсталляция драйвера
Позволяет определять инсталляцию драйвера потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Запуск драйвера
Позволяет определять запуск драйвера потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Инсталляция службы
Позволяет определять инсталляцию службы потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Запуск службы
Позволяет определять запуск службы потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 20, вес последующих срабатываний — 10.
Взаимодействие с другим процессом посредством отсылки оконных сообщений
Позволяет определять попытки взаимодействия (внедрение динамических библиотек или компонент) потенциально зловредного ПО с другим процессом путем отправки информации в его окно. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Взаимодействие с другим процессом посредством отсылки DDE сообщений
Позволяет отслеживать взаимодействие потенциально опасного ПО с другими приложениями посредством DDE сообщений. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.

Взаимодействие с другим процессом с помощью OLE объектов
Позволяет отслеживать взаимодействие потенциально опасного ПО с другими приложениями посредством OLE объектов. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Вызов функции для отправки ICMP сообщения
Позволяет контролировать вызов функции, через которую происходит отправка сообщений по протоколу ICMP. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Вызов DNS API
Позволяет отследить создание ПО DNS-запросов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Запуск доверенных (подписанных) дочерних процессов
Позволяет определять запуск потенциально зловредным ПО доверенных (подписанных) дочерних процессов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Запуск не доверенных (не подписанных) дочерних процессов
Позволяет определять запуск потенциально зловредным ПО не доверенных (не подписанных) дочерних процессов. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Получение контекста десктопа или активного окна (возможность снятия скриншота)
Позволяет определять попытки потенциально зловредным ПО получения контекста рабочего стола пользователя или активного окна в целях получения снимка. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 0.
Перехват нажатия клавиш
Позволяет отследить попытки вредоносного ПО перехватить доступ к нажатию клавиш. Значения по умолчанию: вес первого срабатывания — 50, вес последующих срабатываний — 50.
Право на работу с сетью для дочерних процессов приложения
Позволяет определить попытку получения потенциально зловредным ПО права на работу с сетью для своих дочерних процессов. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.
Использование RAW сокетов
Позволяет определить попытку получения низкоуровневого сетевого доступа потенциально зловредным ПО. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 0.
Изменение файла HOSTS
Позволяет определить попытку потенциально зловредного ПО произвести изменения в файле HOSTS, содержащий базу данных доменных имен. Значения по умолчанию: вес первого срабатывания — 0, вес последующих срабатываний — 0.

Выполнение скриптов PowerShell
Позволяет определить попытку выполнения последовательности действий (сценариев) в оболочке с интерфейсом командной строки PowerShell. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Выполнение скриптов через Windows Script Host
Позволяет определить попытку выполнения последовательности действий (сценариев), реализованных на языках JScript и VBScript в среде сервера сценариев Windows. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Запуск cmd (включая пакетные файлы)
Данная настройка позволяет отслеживать запуск консоли, в том числе пакетные файлы. Значения по умолчанию: вес первого срабатывания — 10, вес последующих срабатываний — 1.
Перезагрузка системы
Позволяет отслеживать перезагрузку системы. Значения по умолчанию: вес первого срабатывания — 100, вес последующих срабатываний — 0.

16.6.3 Контроль приложений

Подкатегория *Контроль приложений* предназначена для управления правилами безопасной среды **СОВ** (рис. 328).

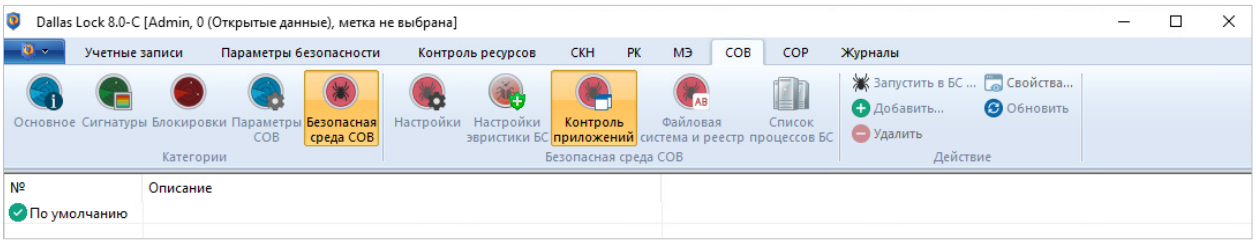


Рис. 328. Панель «Контроль приложений»

По умолчанию *Контроль приложений* содержит настройку безопасной среды *По умолчанию*, которая содержит в себе набор правил для контроля приложений, запускаемых в *Безопасной среде*.

Доступно создание новых и изменение созданных правил. Во вкладке *Общие* для правила безопасности **СОВ** устанавливается его описание и настраивается список *Правил контроля приложений*. Для правила по умолчанию устанавливается вариант доступа *Запрещено* или *Разрешено*. При новом правиле устанавливается один из вариантов доступа: *Запрещено*, *Разрешено* или *Наследуется* (рис. 329).

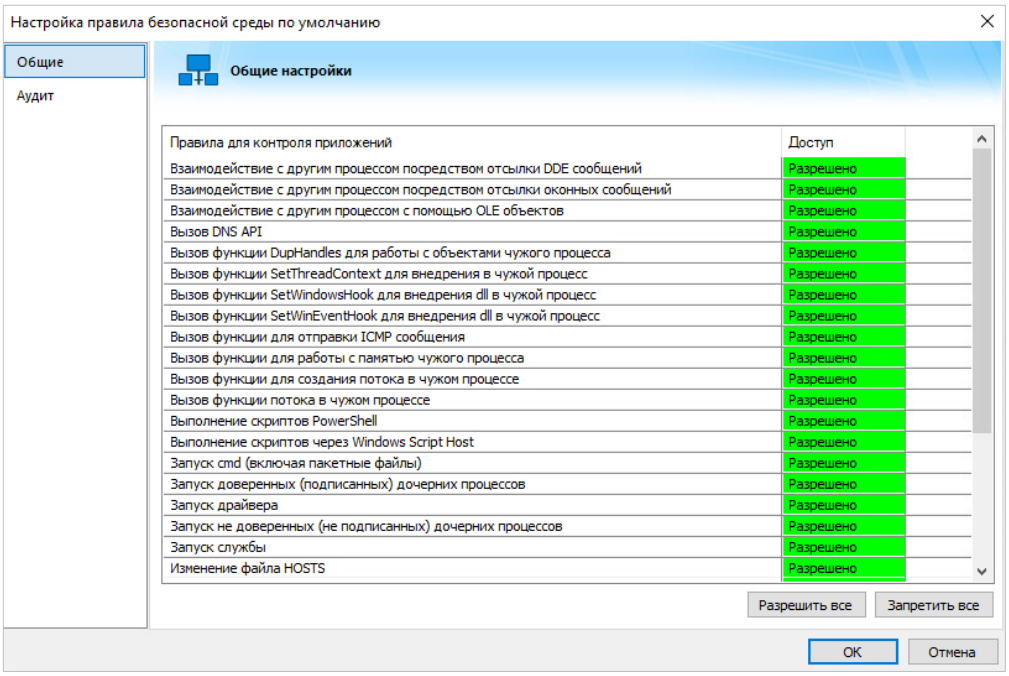


Рис. 329. Общие настройки правила безопасности СОВ

Необходимо отметить, что если правило **СОВ Контроль приложений** отмечено как *Запрещено*, то общее правило с **Контролем приложений** БС будет так же запрещено и изменению не подлежит. Если в правиле **СОВ Контроль приложений** отмечено как *Разрешено*, а в **Контроле приложений** БС запрещено, то будет действовать запрещение этого правила.

Некоторые разрешающие и запрещающие правила Контроля приложений применяются к процессу в момент его запуска и действуют до момента его завершения. Поэтому если правила Контроля приложений были изменены, то для того, чтобы обновленные правила применились ко всем процессам, рекомендуется выполнить выход и повторный вход в ОС либо перезагрузить АРМ.

На вкладке *Аудит* предлагается настройка уровня журналирования (рис. 330).

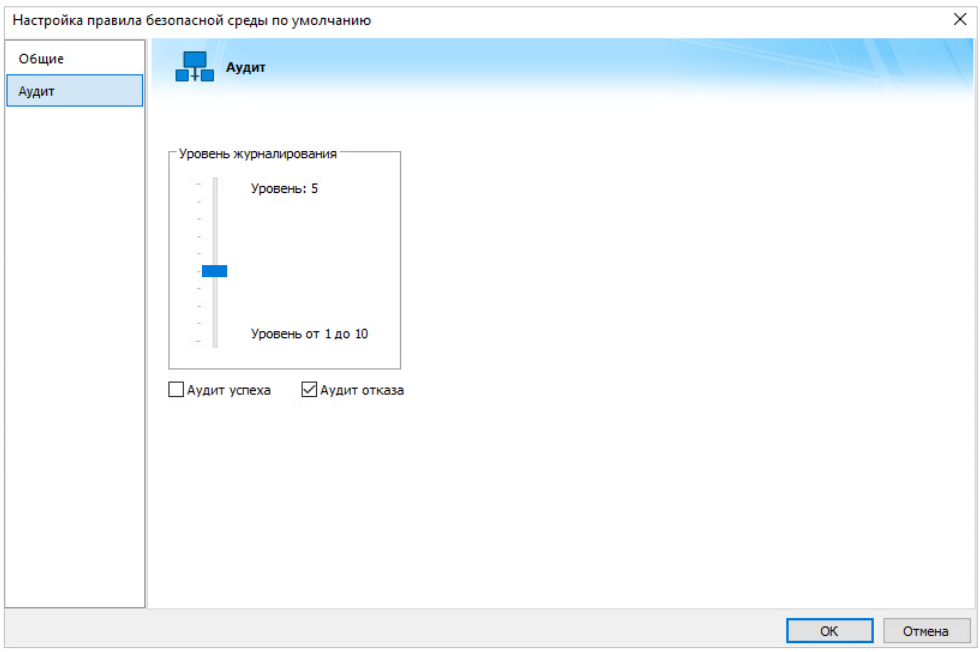


Рис. 330. Настройка аудита правила безопасной среды СОВ

16.6.4 Файловая система и реестр

Подкатегория *Файловая система и реестр* категории **Безопасная среда СОВ** предназначена для указания пользователем тех областей ФС и реестра, которые могут содержать в себе критически важные данные, к которым нельзя предоставлять доступ недоверенным приложениям. При запуске приложения в безопасной среде **СЗИ** перехватывает вызовы функций от приложения к ОС и отслеживает обращения ПО к системному реестру и критическим объектам операционной системы.

По умолчанию доступ ко всем областям разрешен.

Настройка позволяет указать пути к каталогам и веткам реестра, которые недоступны для чтения и записи, и к каталогам и веткам реестра, к которым разрешен полный доступ (рис. 331).

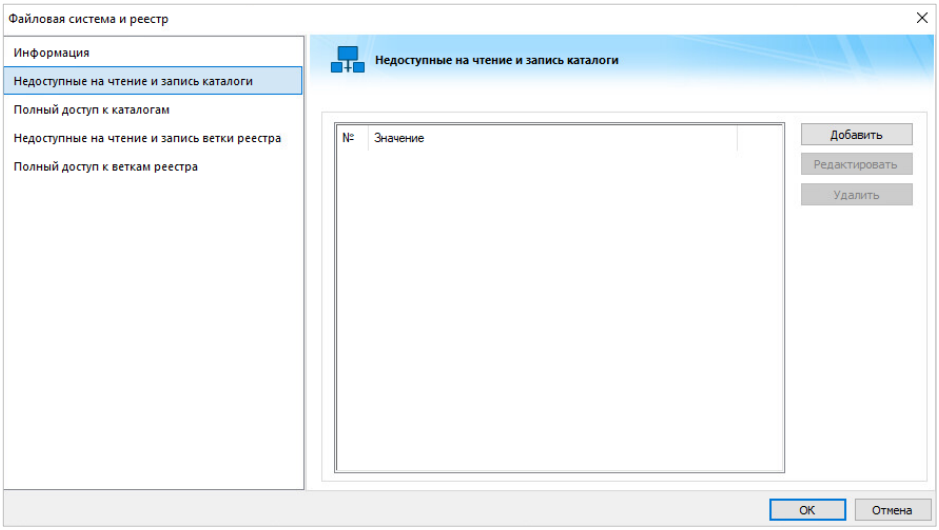


Рис. 331. Настройка доступа приложений к ФС и реестру в режиме БС

16.6.5 Режим безопасной среды

Необходимо отметить, что при попытке запуска в БС приложений с расширением .msi такие процессы не запускаются в БС, выводится соответствующее сообщение о невозможности запуска приложения .msi в БС и отмене запуска.

Приложения, запускаемые в безопасной среде системы обнаружения вторжений, поддерживают работу как с локальным хранилищем, так и с сетевыми папками и дисками.

Приложения, которые автоматически запускаются при старте ОС, необходимо убирать из автозапуска для их корректной работы в Безопасной среде.

Произвести запуск приложения в безопасной среде системы обнаружения вторжений можно следующими способами:

- в консоли администрирования **СЗИ** перейти на вкладку **СОВ** → **Безопасная среда СОВ** → нажать кнопку **Запустить в БС** на панели **Действия**;
- через пункт **DL8.0: Запустить в безопасной среде …** контекстного меню, отображаемого при нажатии на нужном файле правой кнопкой мыши;
- через пункт **СОВ** → **Запустить приложение в безопасной среде СОВ** контекстного меню, отображаемого при нажатии на значок на **Панели задач** Windows (рис. 332).

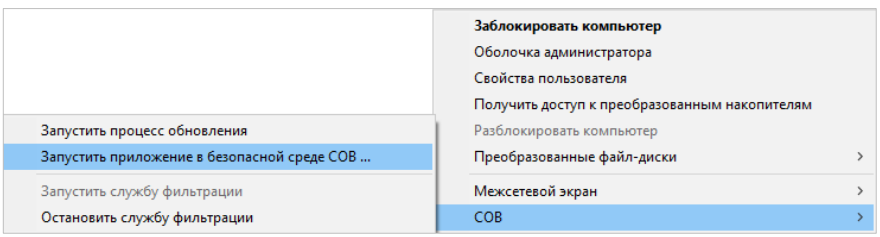


Рис. 332. Запуск приложения в безопасной среде через «Панель задач»

После выполнения одного из этих действий, на экране возникнет диалоговое окно, в котором необходимо в поле *Файл* указать путь к запускаемому приложению, указать параметры, правило и права для запуска приложения (рис. 333).

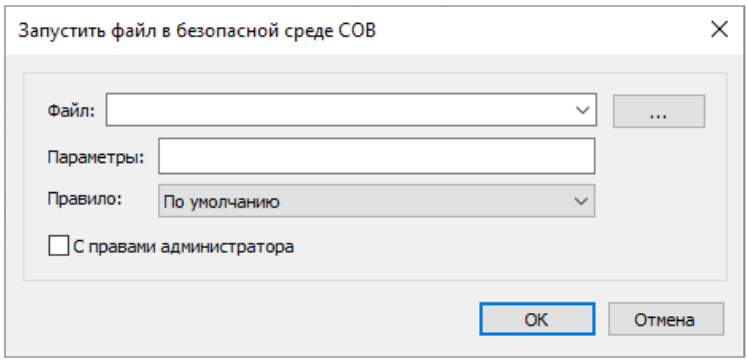


Рис. 333. Запуск приложения в режиме БС

Графическая форма приложения, запущенного в безопасной среде, выделяется цветовой рамкой и подписывается (рис. 334).

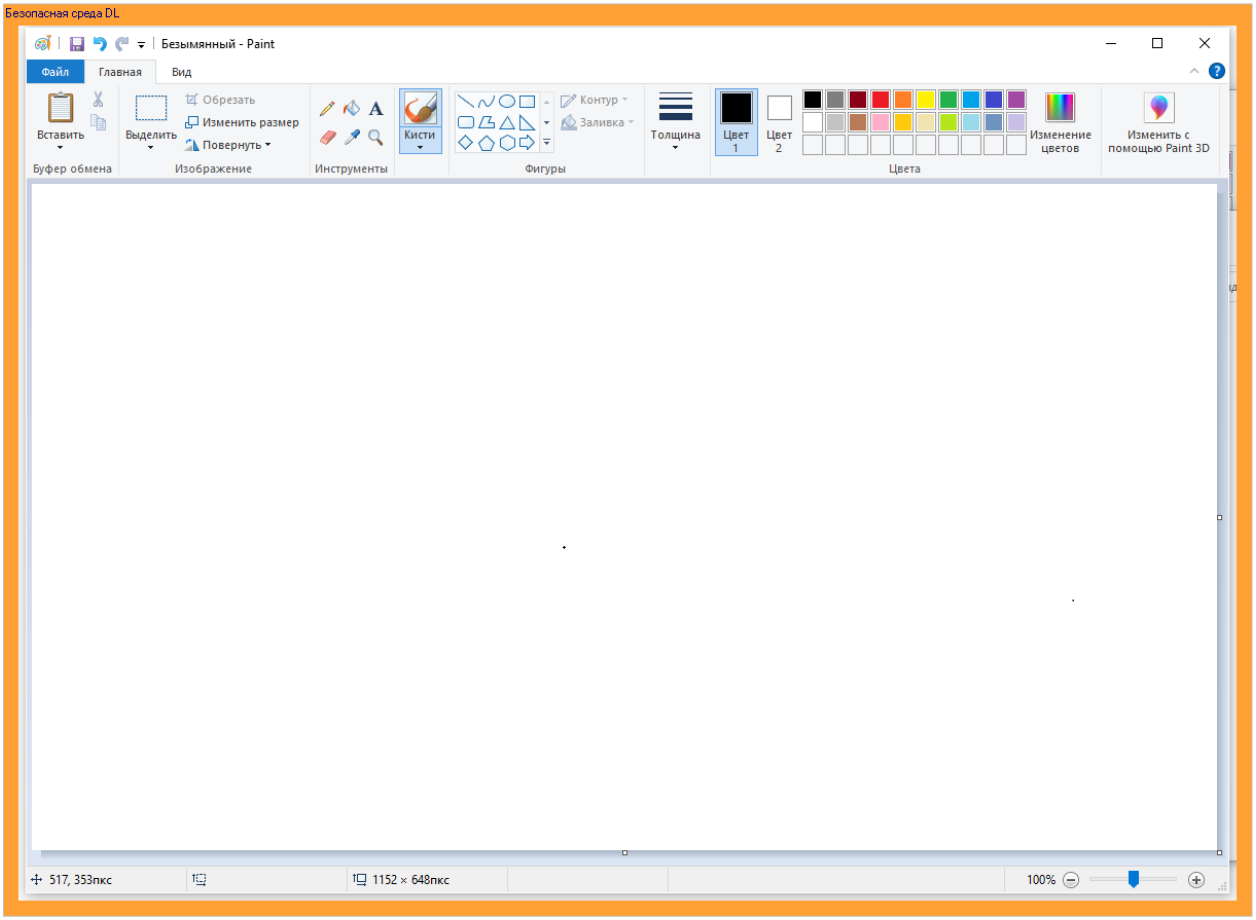


Рис. 334. Безопасная среда

Для формирования отчета безопасной среды СОВ необходимо запустить приложение в БС с включенным параметром **Отчет по завершении работы процесса в БС** во вкладке **СОВ** → категория **Безопасная среда СОВ** → подкатегория **Настройки**. В разделе настроек активировать параметр **Эвристический анализ** для блокировки работы опасных процессов и установить порог срабатывания в параметре **Порог срабатывания эвристики**. При закрытии запущенного приложения в БС будет сформирован отчет.

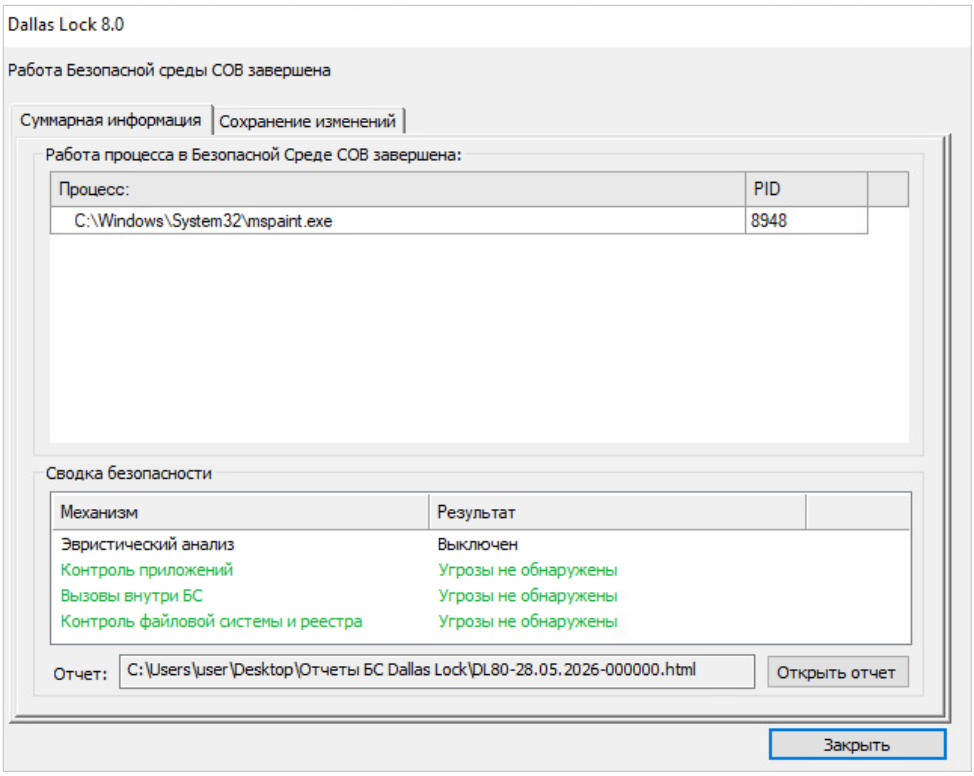


Рис. 335. Завершение работы приложения в безопасной среде

В появившемся окне на вкладке *Суммарная информация* содержится краткая информация о завершении работы процесса в безопасной среде. В строке *Отчет* указан путь, где сохранен отчет. Отчет безопасной среды откроется в браузере при нажатии на кнопку **Открыть отчет** (Рис. 336).

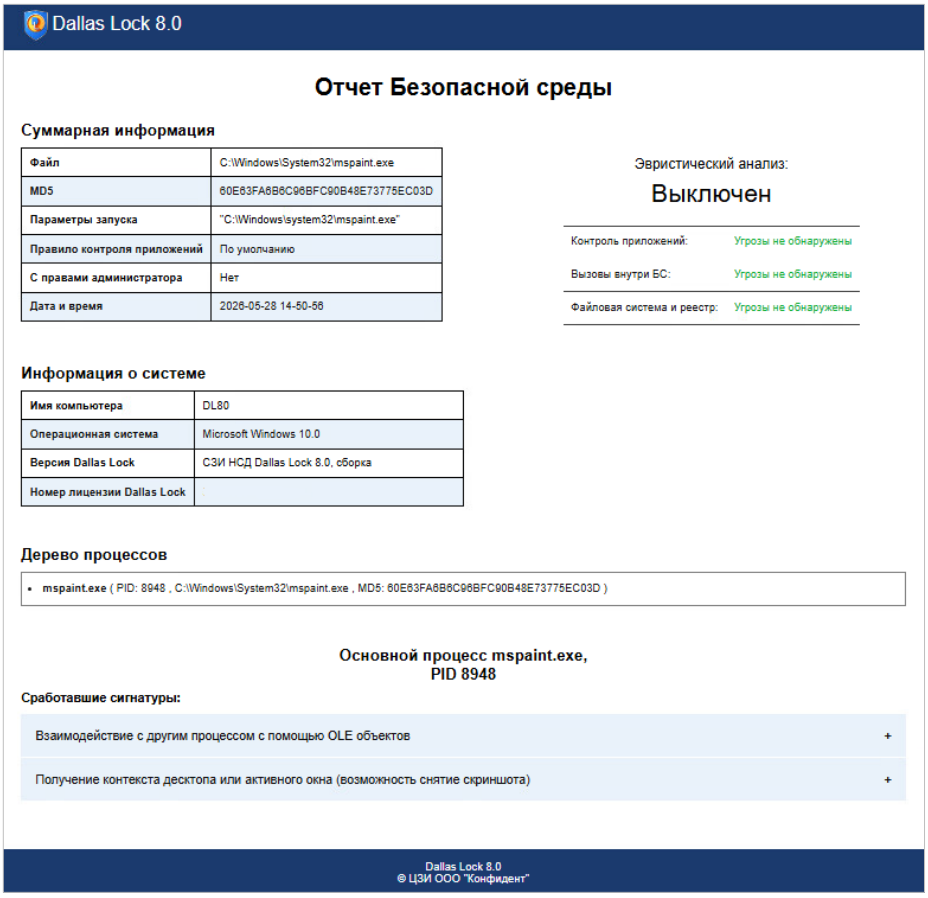


Рис. 336. Отчет безопасной среды

На вкладке *Сохранение изменений* отображены файлы, которые подлежат сохранению из безопасной среды в систему (рис. 337).

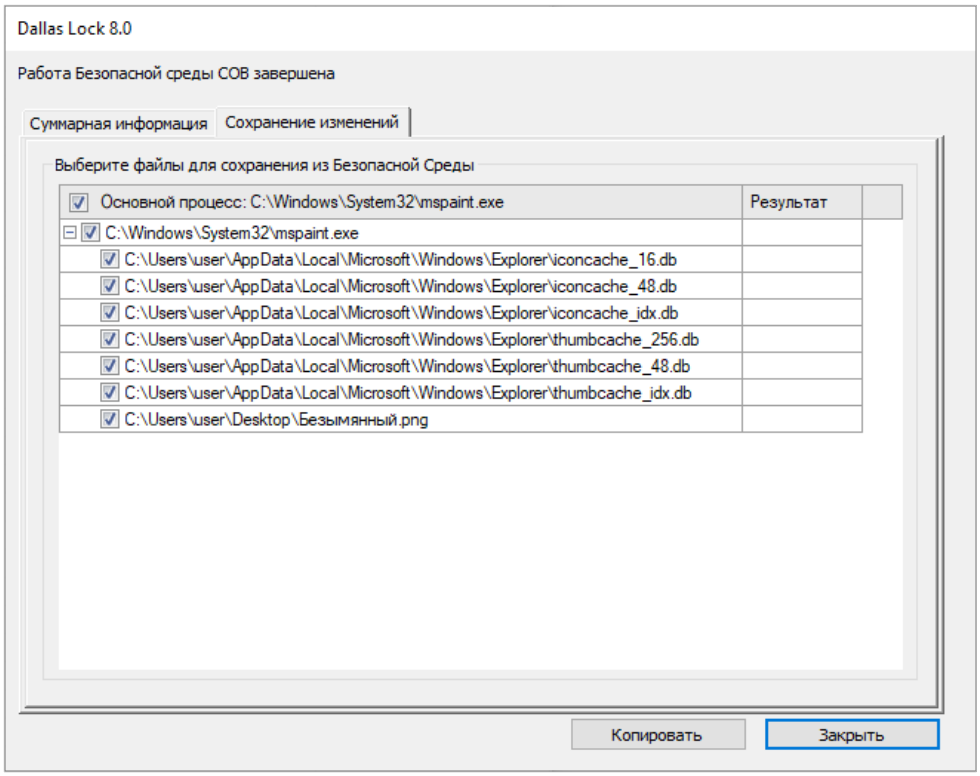


Рис. 337. Сохранение файлов из безопасной среды

Просмотр списка процессов, запущенных в БС доступен в подкатегории *Список процессов БС* (Рис. 338). Для получения списка запущенных процессов необходимо нажать кнопку **Обновить**.

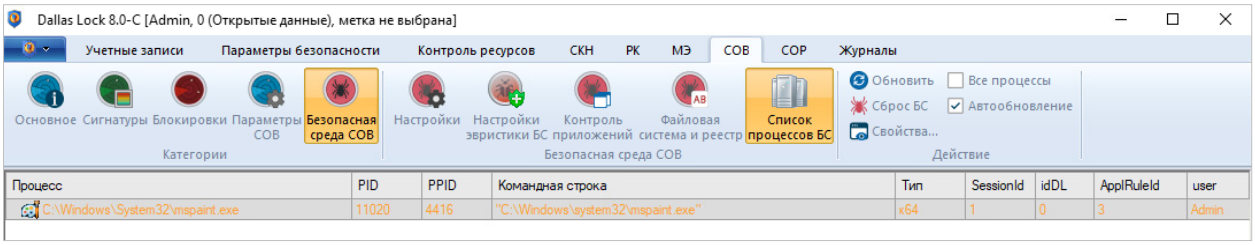


Рис. 338. Список процессов БС

В данной подкатегории есть возможность завершения работы всех процессов в БС и реализации полной очистки данных. Для этого нужно на панели **Действия** нажать кнопку **Сброс БС**.

При нажатии данной кнопки, пользователю показывается диалоговое окно для подтверждения завершения всех процессов и очистки данных в БС (рис. 339).

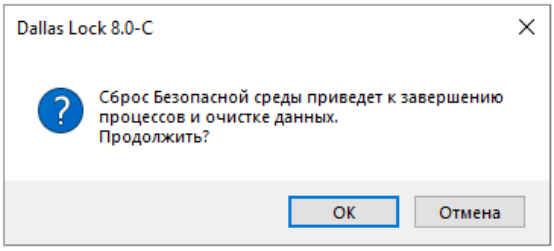


Рис. 339. Сброс БС

При завершении процесса сброса на экране появляется информационное сообщение об успехе выполнения команды (рис. 340).

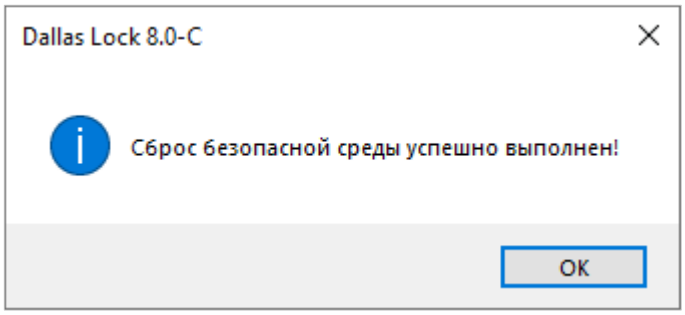


Рис. 340. Успешный сброс безопасной среды

16.7 Журналы СОВ

Основной информацией, фиксируемой в журналах **СОВ**, является информация о подозрительном сетевом трафике, блокировках сетевых атак, информация о поведении ОС и прикладного ПО.

Для того, чтобы ознакомиться с данной информацией, нужно открыть общую вкладку *Журналы* и выбрать один из трех журналов: **Системный журнал**, **Журнал трафика**, **Журнал контроля приложений**. По умолчанию журналы **СОВ** включены.

На панели **Действия** расположено три кнопки. При нажатии кнопки **Обновить** отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах СОВ, нужно нажать кнопку **Архивировать**. После этого в папке программы появится файл с архивом данных. Для открытия такого файла нужно использовать категорию **Журнал из файла** и в ее окне на панели действий нажать кнопку **Открыть журнал**, а затем, в открывшемся окне, выбрать файл журнала или задать путь к файлу. Кнопка **Экспорт** отвечает за сбор и конвертирование информации журналов межсетевого экрана в файлы с расширением txt (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку **Экспорт**, указать имя файла и выбрать место для его хранения.

При открытии **Журнала из файла**, в окне выбора файлов возможно выбрать несколько журналов одного типа. При выборе разных типов появится сообщение об ошибке.

В СОВ предусмотрено ведение следующих журналов:

1. Системный журнал — в журнал заносятся сведения о событиях безопасности, генерируемых ОС и прикладным ПО.
2. Журнал трафика — в журнал заносятся события, связанные с проходящим сетевым трафиком через контролируемые сетевые интерфейсы.
3. Журнал контроля приложений — в журнал заносятся сведения об активности приложений, при вызове ими функций, связанных с безопасностью ОС.

Настройки журналов **СОВ** находятся во вкладке **Параметры безопасности** → **Политики аудита** и задаются через три параметра (рис. 370).

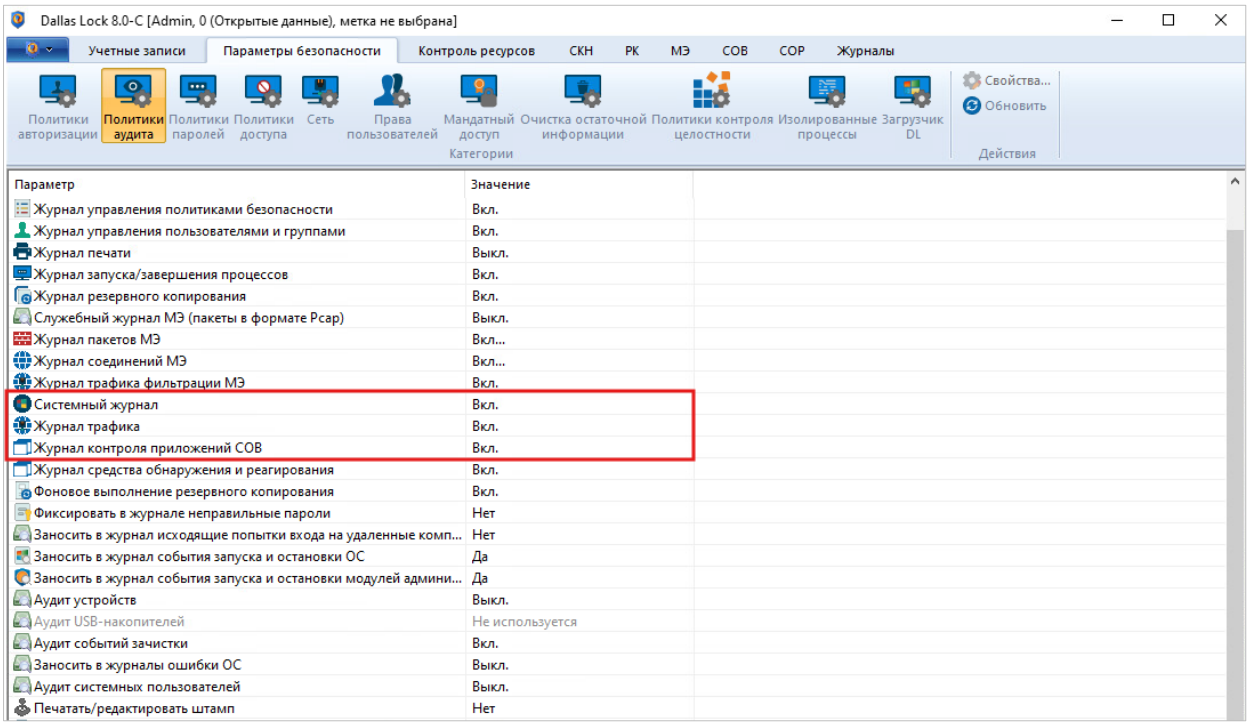


Рис. 341. Основные параметры работы журналов

Чтобы выключить системный журнал необходимо нажать правой кнопкой мыши на параметре **Системный журнал** и в появившемся окне выбрать пункт «*Выкл.*», после чего нажать кнопку **ОК** (рис. 371). Для остальных журналов **СОВ** настройка аналогична.

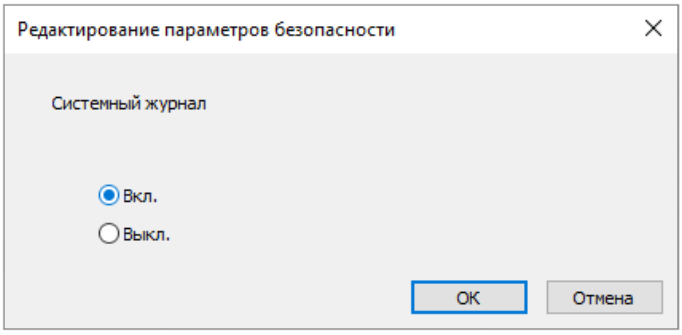


Рис. 342. Отключение ведения журнала событий ОС

В **Журнале управления политиками СЗИ** фиксирует события редактирования параметров и политик СОВ. По умолчанию журнал включен (рис. 343).

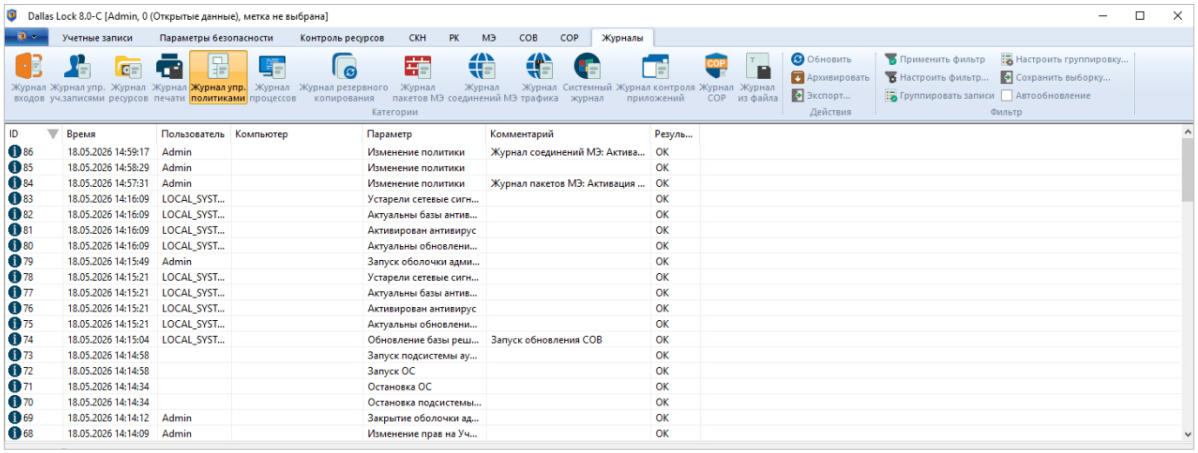


Рис. 343. Журнал управления политиками безопасности

Для просмотра и изменения политик и других параметров **Безопасной среды** пользователь должен быть указан в значении параметров **СОВ: Изменение настроек** и **СОВ: Просмотр настроек** категории **Права пользователей** либо состоять в группе, указанной в данном параметре (рис. 344).

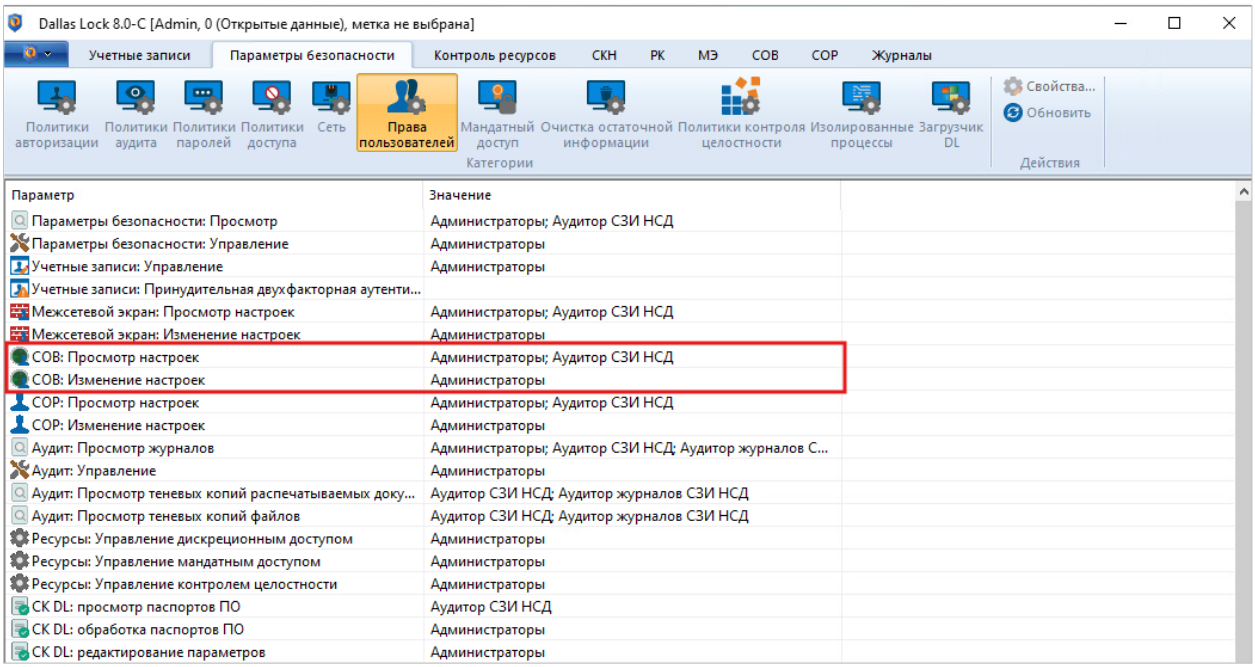


Рис. 344. Настройка аудита настроек СОВ

17 СРЕДСТВО ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ

На вкладке **COP** можно настроить средство обнаружения и реагирования, позволяющее на основе индикаторов компрометации выявлять уже совершенные попытки атаки и настраивать реакцию **COP** при их обнаружении. Настройка **COP** доступна пользователям, которым назначена возможность изменения настроек **COP**, — администраторам ЗАРМ **Dallas Lock** (по умолчанию членам группы *Администраторы*) и происходит из оболочки администратора во вкладке *COP*.

Для просмотра и изменения политик и других параметров **COP** пользователь должен быть указан в значении параметров **COP: Изменение настроек** и **COP: Просмотр настроек** категории **Права пользователей** либо состоять в группе, указанной в данном параметре.

Индикаторы компрометации (IoC) — цифровые артефакты, которые с большой долей вероятности указывают на несанкционированный доступ к системе (то есть ее компрометацию). Сканирование системы на IoC осуществляется на основании IoC-объектов (JSON-объекты в формате STIX, которые содержат описание индикатора компрометации).

17.1 Параметры COP

В категории **Параметры COP** предусмотрена настройка обновления базы решающих правил (далее — БРП), в частности индикаторов компрометации (Рис. 345).

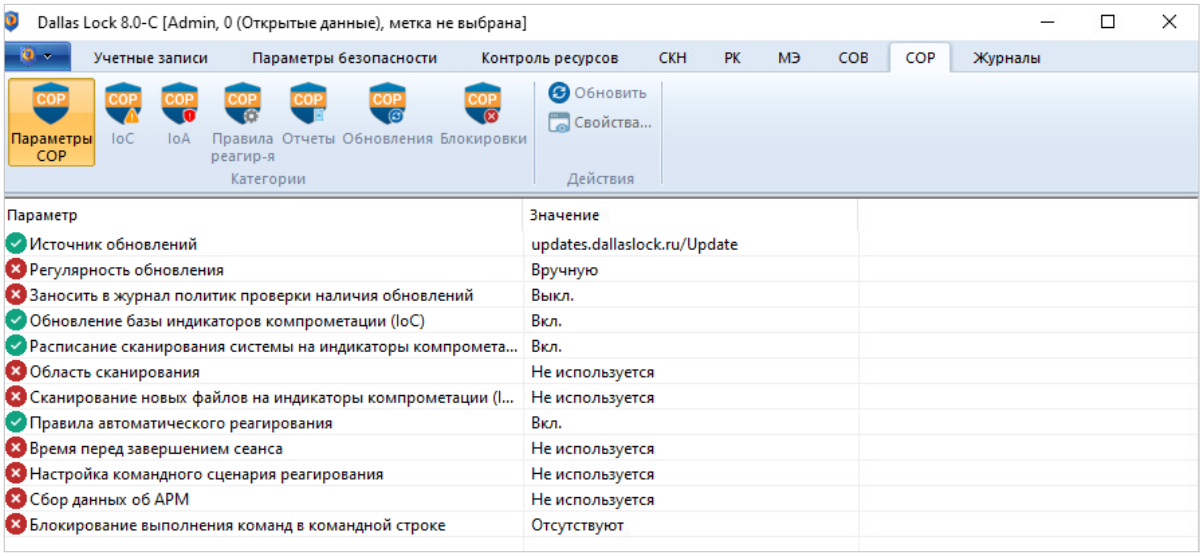


Рис. 345. Параметры COP

Источник обновлений

Данный параметр позволяет задать источник обновления БРП.

По умолчанию параметры подключения к интернету определяются автоматически. Если используется прокси-сервер, необходимо настроить параметры прокси-сервера в свойствах обозревателя или браузера в зависимости от версии Windows.

Регулярность обновления

Данный параметр отвечает за регулярность обновления БРП.

Существует 4 режима обновлений: вручную, раз в час, раз в сутки и раз в две недели. При выборе обновления вручную обновление не произойдет до тех пор, пока не будет нажата кнопка **Обновить** на панели **Действия** или в контекстном меню значка блокировки.

После применения обновления, в журнал управления политик производится соответствующая запись.

Заносить в журнал политик проверки наличия обновлений

Включение данного параметра позволяет вести учет проверок на наличие обновлений в журнале управления политиками.

Обновление базы индикаторов компрометации (IoC)

Данный параметр позволяет включать/отключать синхронизацию списка доверенных адресов с **СБ**. По умолчанию параметр имеет значение «*Выкл.*».

Расписание сканирования системы на индикаторы компрометации (IoC)

Данный параметр отвечает за регулярность сканирования системы на индикаторы компрометации.

Область сканирования

Данный параметр отвечает за указание директории для быстрого сканирования системы на индикаторы компрометации. Для добавления директории необходимо нажать кнопку **Свойства** откроется окно, представленное ниже (рис. 346), убрать чекбокс **Не используется**, нажать кнопку ... и указать папку в системе. Нажать кнопку **Добавить**. После внесения изменений нажать кнопку **ОК**.

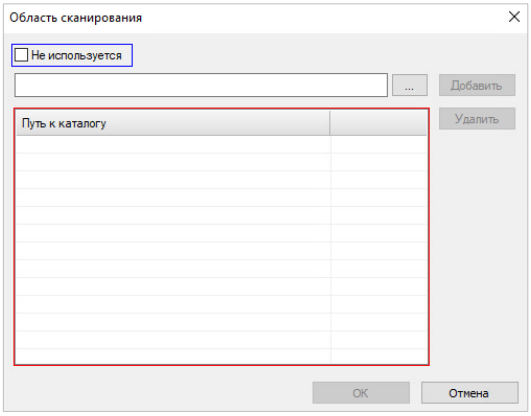


Рис. 346. Добавление области сканирования

Правила автоматического реагирования

Данный параметр отвечает за работу правил автоматического реагирования **СОР**.

Сканирование новых файлов на индикаторы компрометации (IoC)

Данный параметр отвечает за автоматическое сканирование новых файлов в системе на индикаторы компрометации. Для добавления директории необходимо нажать кнопку **Свойства** откроется окно, представленное ниже (рис. 347), убрать чекбокс **Не используется**, нажать кнопку ... и указать папку в системе. Нажать кнопку **Добавить**. Для сканирования подпапки активировать чебокс **Сканировать вложенные директории**. После внесения изменений нажать кнопку **ОК**.

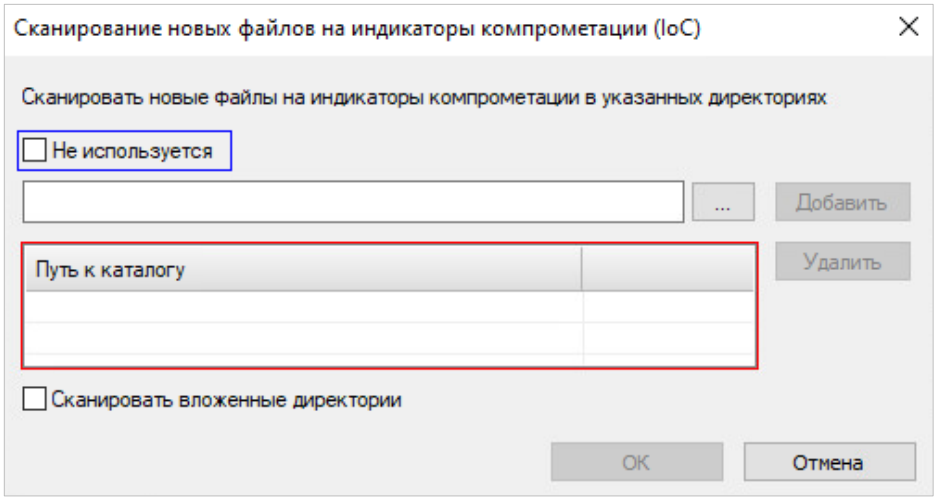


Рис. 347. Сканирование новых файлов на индикаторы компрометации

В случае, если в процессе сканирования произошло обновление базы, автоматическое сканирование осуществляется на основании той базы, которая была актуальной на момент запуска сканирования.

В связи с особенностью некоторых вирусов видоизменять и/или создавать новый файл, при первом сканировании такой зловред может быть не обнаружен, однако при полном сканировании модифицированный файл будет обнаружен.

При создании пустого файла сканирование не происходит.

В случае, если созданный файл был переименован, такой файл не подлежит сканированию, однако при полном сканировании такой файл будет просканирован.

Время перед завершением сеанса

Данный параметр отвечает за время, которое дается пользователю для сохранения обрабатываемых данных перед завершением сеанса. По умолчанию параметр имеет значение «Не используется». Возможные принимаемые значения: 1 мин., 2 мин., 5 мин. При включённой политике перед завершением пользовательского сеанса отображается информационное сообщение.

Причины, при которых появляется информационное сообщение:

- Блокировка АРМ;
- Блокировка учетной записи;
- Выключение АРМ.

Блокирование выполнения команд в командной строке

Данный параметр отвечает за блокирование выполнения команд, определенных администратором средства обнаружения и реагирования на уровне узла, в командной строке на заданный промежуток времени. Для настройки необходимо нажать кнопку **Свойства** откроется окно, представленное ниже (Рис. 348), выключить чекбокс **Не используется**, нажать кнопку **Добавить** и ввести команду, которую необходимо заблокировать. В выпадающем списке **Время блокировки** выбрать значение времени, на которое необходима блокировка. Для редактирования или удаления добавленных команд нажать кнопки **Редактировать** и **Удалить** соответственно.

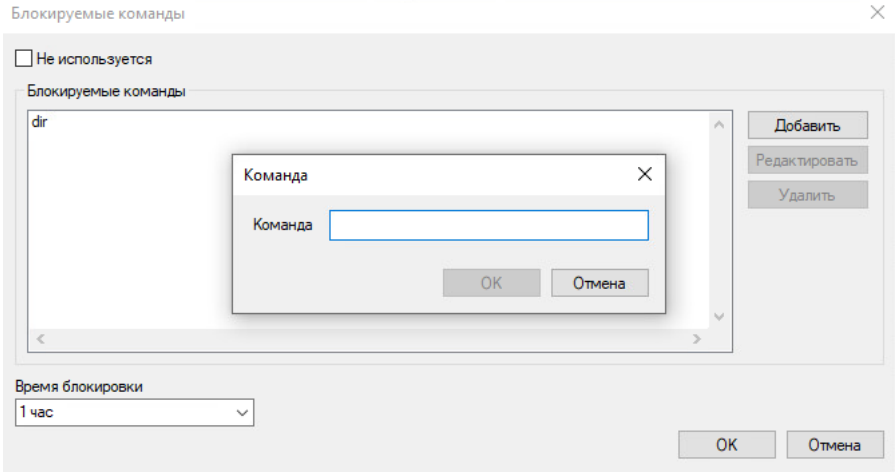


Рис. 348. Блокируемые команды

Настройка командного сценария реагирования

Данный параметр отвечает за настройку командного сценария реагирования. По умолчанию значение политики «*Не используется*». Для настройки нажать кнопку **Свойства** откроется окно, представленное ниже (Рис. 349), выбрать тип **CMD** или **ПО**. При выборе **CMD** откроется окно, в которое необходимо ввести параметры. Если выборать тип **ПО** откроется окно выбора ФС. При установке чекбокса у соответствующего поля, активируется тот или иной сценарий. Если активированы оба чекбокса, сценарии выполняются последовательно.

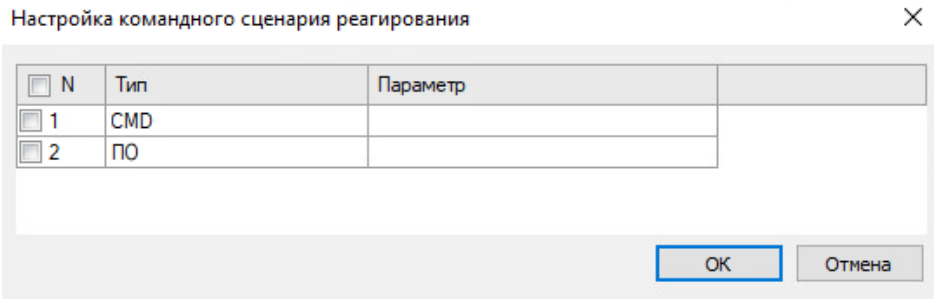


Рис. 349. Настройка командного сценария реагирования

Сбор данных об АРМ

Данный параметр позволяет включить и настроить получение дополнительных данных об узле. По умолчанию значение политики «*Не используется*». Данные, которые можно собрать:

- запущенные процессы операционной системы;
- активные сетевые соединения;
- авторизованные учетные записи;
- список автозапуска ПО;
- дамп памяти процесса;
- дамп оперативной памяти.

Для настройки необходимо нажать кнопку **Свойства** откроется окно, представленное ниже (Рис. 350), активировать чекбоксы напротив данных, которые необходимо собрать. При нажатии на кнопку "Собрать данные", отмеченные чекбоксом данные должны сохраниться в папке "C:\DLLOCK80\Data".

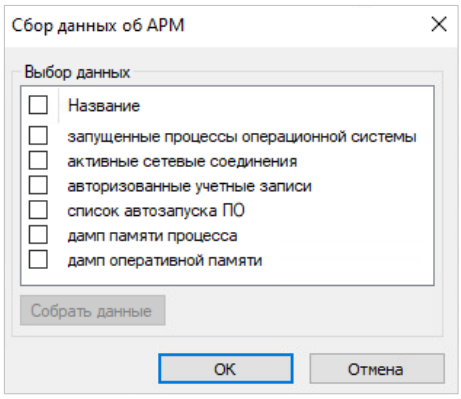


Рис. 350. Сбор данных об АРМ

Действия по изменению параметров СОР фиксируются в журнале управления политиками.

17.2 Индикаторы компрометации (IoC)

В данной категории уполномоченный пользователь может управлять списком индикаторов компрометации. Список индикаторов компрометации (рис. 351), разделен на две группы *Стандартные* и *Пользовательские*. Стандартными являются индикаторы компрометации, которые предварительно установлены в **СЗИ** или загружаются с серверов производителя при обновлении.

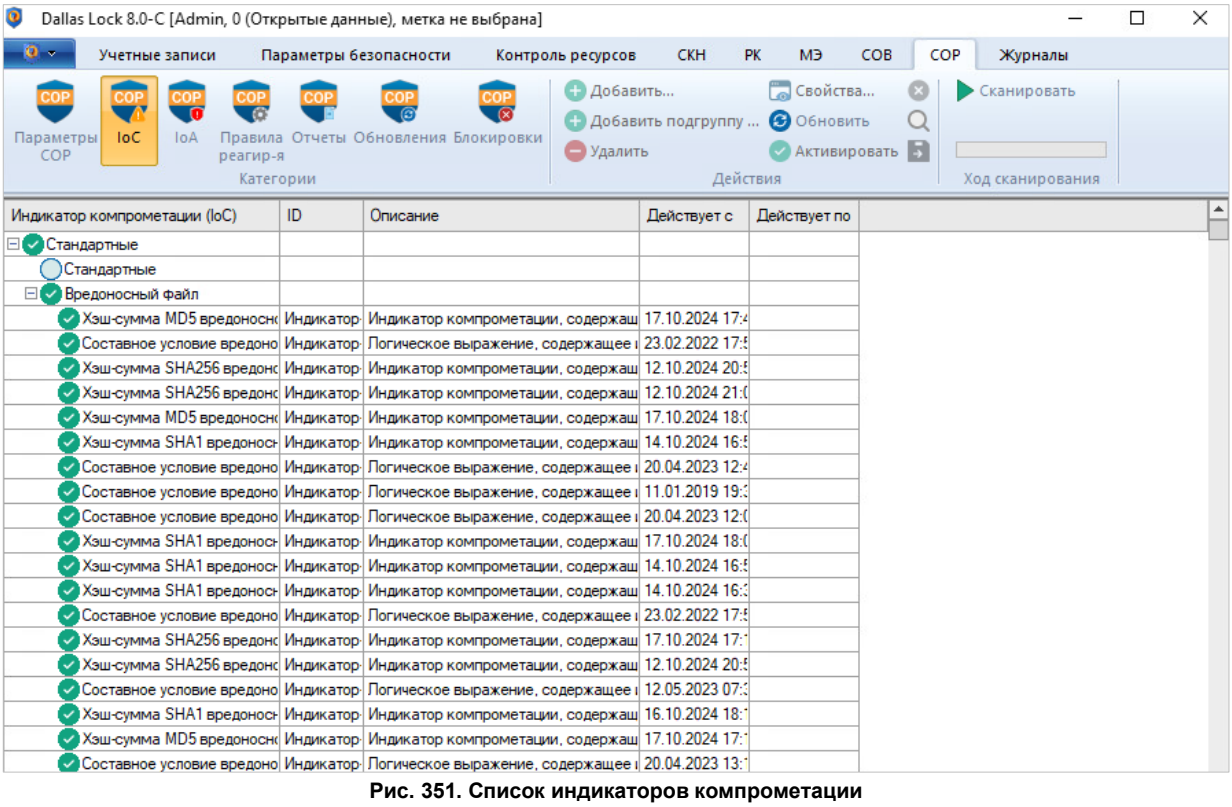


Рис. 351. Список индикаторов компрометации

В группе *Пользовательские* можно создавать подгруппы индикаторов компрометации. Для этого нажать кнопку **Добавить подгруппу** на панели *Действия* или с помощью контекстного меню (вызывается нажатием правой кнопкой мыши по группе *Пользовательские*). Откроется окно представленое ниже (Рис. 352). В поле *Имя подгруппы* ввести название и нажать кнопку **ОК**.

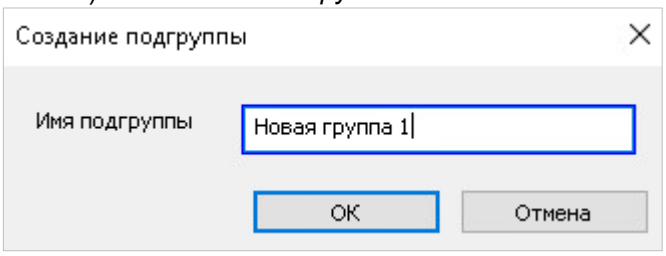


Рис. 352. Создание подгруппы IOC

Для добавления пользовательских индикаторов компрометации необходимо:

1. Выбрать группу *Пользовательские* и нажать кнопку **Добавить**, откроется окно **Добавление пользовательских индикаторов компрометации (IoC)**.
2. При включенном чекбоксе **Распределить по группам с учетом поля “pattern” формата IoC (если группа не существует она будет создана)** (рис. 353) все добавляемые пользовательские индикаторы компрометации будут разбиты на соответствующие полю 'pattern' подгруппы. Для добавления выбранных индикаторов компрометации в определенную группу выключить чекбокс.

> **!** В случае, если в группе «Пользовательские» нет никаких подгрупп и при добавлении индикатора в окне «Добавление пользовательских индикаторов компрометации (IoC)» выключен чекбокс, то автоматически создается подгруппа с именем «Новая подгруппа N» с данными индикаторами, где N – номер подгруппы в списке одноименных.

3. Для добавления дистрибутива нажать кнопку  и указать папку в системе, где расположены IoC-файлы в формате .json.
4. В списке установить чекбоксы напротив индикаторов компрометации, которые нужно добавить.
5. Нажать кнопку **ОК**.

Кнопка **Отмена** позволяет закрыть окно без сохранения любых изменений. Кнопка  запускает процесс повторного сканирования выбранного каталога на предмет наличия IoC-файлов и проверки содержащихся в них IoC-объектов на соответствие критериям **СЗИ**.

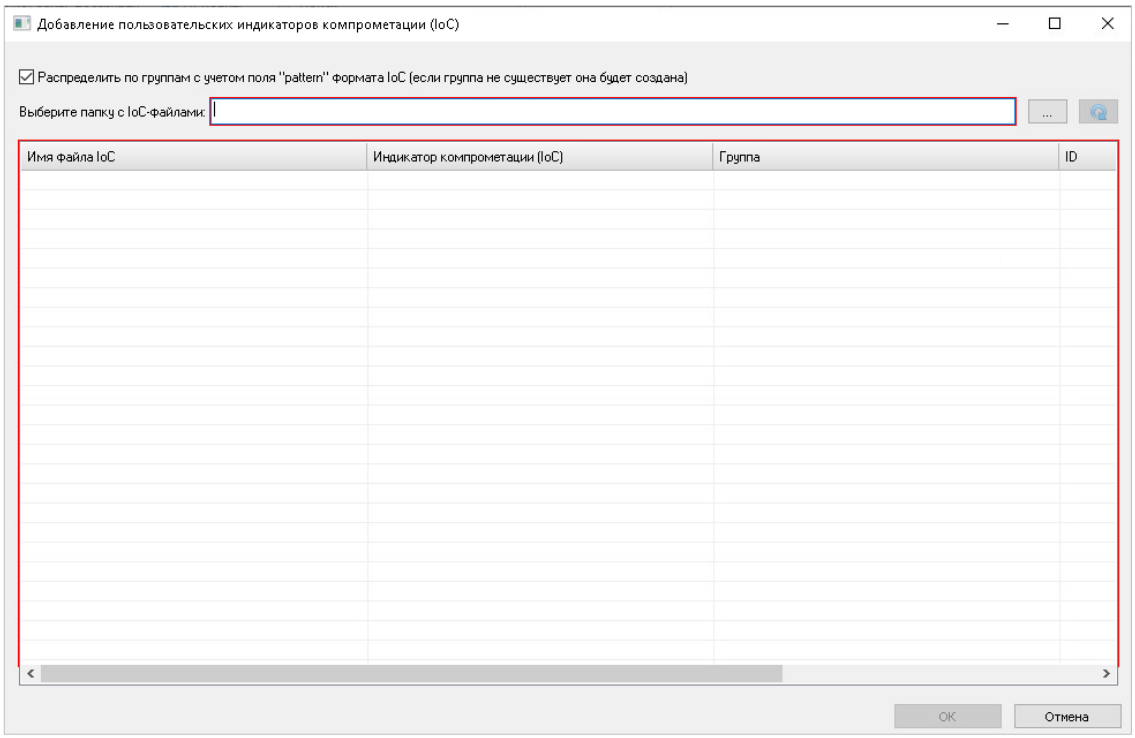


Рис. 353. Добавление пользовательских IoC-объектов

Ниже представлен перечень атрибутов IoC-объектов анализируемых СЗИ (Таблица 15).

Таблица 15. Перечень атрибутов IoC-объектов

№	Наименование атрибута	Описание атрибута
1	type	Определяет тип JSON-объекта. Значение «indicator» указывает на то, что этот JSON-объект является IoC-объектом
2	spec_version	Версия STIX
3	created	Дата и время создания IoC-объекта в формате RFC 3339
4	modified	Дата и время последнего изменения IoC-объекта в формате RFC 3339
5	id	Уникальный идентификатор IoC
6	name	Название IoC
7	description	Описание IoC
8	pattern	Информация, на которою осуществляется сканирование системы на индикаторы компрометации (IoC)
9	pattern_type	Язык, на котором описан паттерн IoC
10	valid_from	Дата и время в формате RFC 3339, когда IoC-объект начинает действовать
11	valid_until	Дата и время в формате RFC 3339, когда IoC-объект перестает действовать

Помимо описанных выше атрибутов, в IoC-объекте могут быть определены следующие атрибуты:

- indicator_types (массив);
- pattern_version (переменная);
- kill_chain_phases (массив);
- created_by_ref (переменная);
- revoked (переменная);
- labels (массив);
- confidence (переменная);
- lang (переменная);
- external_references (массив);
- object_marking_refs (массив);
- granular_markings (массив);
- extensions (json-объект).

Данные атрибуты не влияют на возможность добавления IoC-объекта в базу и не анализируются DL8.0, однако эти атрибуты (за исключением «extensions») сохраняются в базе IoC-объектов СЗИ наравне с другими атрибутами.

Все IoC-объекты в базе **СЗИ** должны иметь уникальные поля «id».

При сканировании каталога поиск IoC-файлов не осуществляется во вложенных каталогах.

Критерии того, что файл является IoC-файлом:

- файл имеет расширение .json;
- в файле есть хотя бы один JSON-объект, у которого «type» равен «indicator».

Возможны следующие ошибки при добавлении IoC-файлов:

- отсутствует один или несколько обязательных атрибутов STIX («type», «spec_version», «created», «modified», «id», «pattern», «pattern_type», «valid_from»);
- формат даты и времени не соответствует RFC 3339;
- дата создания IoC-объекта не может быть позже текущей даты;
- дата изменения IoC-объекта не может быть раньше даты создания;
- в базе уже есть IoC-объект с таким «id»;
- формат описания IoC («pattern_type») отличается от STIX;
- дата окончания действия не может быть раньше даты начала действия;
- «pattern» содержит неподдерживаемые объекты, свойства и операторы.

СЗИ поддерживает следующие типы данных, указанные в атрибуте «pattern»: string, timestamp, int, boolean, list, hashes. Ниже приведен список поддерживаемых объектов атрибута «pattern» и их свойств (см. Таблица 16).

Таблица 16. Перечень поддерживаемых объектов и их свойств

Свойства объекта	Тип данных	Описание	Источник данных
Свойства объекта directory (каталог)			
path	string	Полный путь к каталогу из корня раздела диска, на котором он находится, включая букву диска	Файловая система
ctime	timestamp	Дата и время создания каталога	
mtime	timestamp	Дата и время изменения каталога	
atime	timestamp	Дата и время последнего обращения к каталогу	
contains_refs	list (file, directory)	Файл или каталог, содержащийся в данном каталоге (один уровень вложенности)	
Свойства объекта file (файл)			
hashes	hashes	Хэш файла	Файловая система
size	int	Размер файла в байтах	
name	string	Имя файла с расширением	
ctime	timestamp	Дата и время создания файла	
mtime	timestamp	Дата и время изменения файла	
atime	timestamp	Дата и время последнего обращения к файлу	
parent_directory_ref	directory	Каталог, в котором находится файл	
Свойства объекта domain-name (доменное имя)			
value	string	Доменное имя ресурса	Таблица соединений,

Свойства объекта	Тип данных	Описание	Источник данных
resolves_to_refs	list (ipv4-addr, ipv6-addr)	IP-адрес, соответствующий этому имени	журнал соединений, журнал пакетов
Свойства объекта ipv4-addr (IPv4-адрес)			
value	string	IPv4-адрес и (опционально) маска подсети	Таблица соединений, журнал соединений, журнал пакетов
resolves_to_refs	list (mac-addr)	MAC-адрес, соответствующий этому IPv4-адресу	Журнал пакетов (поле «Информация»)
Свойства объекта ipv6-addr (IPv6-адрес)			
value	string	IPv6-адрес и (опционально) маска подсети	Таблица соединений, журнал соединений, журнал пакетов
resolves_to_refs	list (mac-addr)	MAC-адрес, соответствующий этому IPv6-адресу	Журнал пакетов (поле «Информация»)
Свойства объекта mac-addr (MAC-адрес)			
value	string	MAC-адрес	Журнал пакетов (поле «Информация»)
Свойства объекта network-traffic (сетевой трафик)			
src_ref	ipv4-addr, ipv6-addr, domain-name или mac-addr	Адрес источника	Таблица соединений, журнал соединений, журнал пакетов
dst_ref	ipv4-addr, ipv6-addr, domain-name или mac-addr	Адрес назначения	
src_port	int	Порт источника	
dst_port	int	Порт назначения	
protocols	list (string)	Протокол	
Свойства объекта url (ссылка)			
value	string	URL ресурса	Таблица соединений, журнал соединений, журнал пакетов
Свойства объекта process (процесс)			
pid	int	PID процесса	
created_time	timestamp	Дата и время старта процесса	
command_line	string	Полная командная строка запуска, включая имя процесса и аргументы	
opened_connection_refs	list (network-traffic)	Сетевые соединения, открытые процессом	

Свойства объекта	Тип данных	Описание	Источник данных
creator_user_ref	user-account	Учетная запись, от имени которой выполняется процесс	
image_ref	file	Исполняемый файл процесса	
parent_ref	process	Родительский процесс	
child_refs	list (process)	Дочерние процессы	
Свойства объекта software (программное обеспечение)			
name	string	Имя ПО	Get-WmiObject -Class Win32_Product
vendor	string	Вендор	
version	string	Версия ПО	
Свойства объекта user-account (учетная запись)			
user_id	string	SID учетной записи Windows	Список учетных записей операционной системы
account_login	string	Логин	
display_name	string	Полное имя	
account_type	string	Тип учетной записи. Может принимать значение 'windows-local' для локальных учетных записей и 'windows-domain' – для доменных	
is_service_account	boolean	Признак, описывающий является ли учетная запись служебной	
is_disabled	boolean	Признак, описывающий может ли учетная запись пользователя быть использована для входа в систему	
Свойства объекта windows-registry-key (раздел реестра)			
key	string	Путь к разделу (key) реестра (с hive)	Реестр Windows
values	list (windows-registry-value-type)	Список значений в разделе реестра	
modified_time	timestamp	Дата и время изменения раздела реестра	
creator_user_ref	user-account	Учетная запись, от имени которой был создан раздел реестра	
number_of_subkeys	int	Количество подразделов, содержащихся в разделе реестра	

Свойства объекта	Тип данных	Описание	Источник данных
Свойства объекта windows-registry-value-type (значение реестра)			
name	string	Имя значения реестра	Реестр Windows
data	string	Данные, содержащиеся в значении реестра	
data_type	string	Тип данных значения реестра (REG_*)	

СЗИ поддерживает следующие операторы в атрибуте «pattern» (см. Таблица 17).

Таблица 17. Перечень поддерживаемых операторов

Операторы	Описание
Булевы операторы	
A AND B	Логическое И (истина, если оба выражения являются истиной)
A OR B	Логическое ИЛИ (истина, если хотя бы одно выражение является истиной)
Операторы сравнения	
A = B	Истина, если A равно B
A != B	Истина, если A не равно B
A > B	Истина, если A больше B
A < B	Истина, если A меньше B
A >= B	Истина, если A больше либо равно B
A <= B	Истина, если A меньше либо равно B
A IN (B, C, D,...)	Истина, если A равно одному из значений, перечисленных в наборе (B, C, D,...)
A LIKE B	Истина, если A соответствует шаблону, указанному в B, где любой «%» представляет собой 0 или более символов, а «_» — любой один символ **Пример** "pattern": "[directory:path LIKE 'C:\\Windows\\%\\foo']"
Специальные операторы	
()	Оператор изменения приоритета



Учитывается следующий приоритет операторов: () → AND → OR.



A и B должны иметь один и тот же тип данных.

Для удаления необходимо выделить один или несколько индикаторов компрометации, нажать кнопку **Удалить** и в открывшемся окне нажать кнопку **Да** (рис. 354).



Удаление группы *Стандартные* и индикаторов компрометации, находящихся в этой группе, невозможно. Чтобы удалить группу *Пользовательские* или её подгруппу, следует выбрать ее и нажать кнопку **Удалить**. При удалении группы из неё удаляются все дочерние элементы, при этом сама группа сохраняется.

Если были одновременно выделены и пользовательские, и стандартные IoC-объекты, то при подтверждении удаления:

- выделенные пользовательские IoC-объекты будут удалены;
- выделенные стандартные IoC-объекты будут деактивированы.

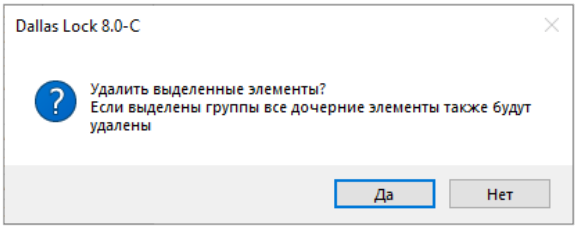


Рис. 354. Удаление IoC-объектов

Для просмотра свойств индикатора компрометации нажать кнопку **Свойства…** на панели *Действия* или с помощью контекстного меню, откроется окно просмотра информации о IoC-объекте (рис. 355).

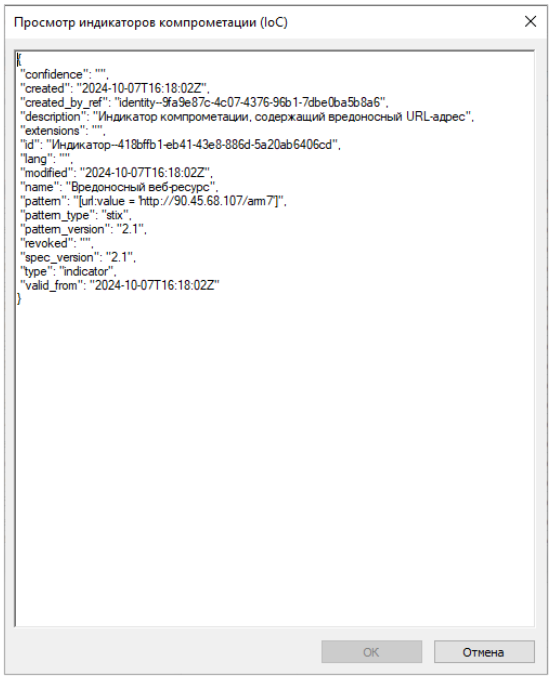


Рис. 355. Просмотр индикатора компрометации

Для обновления списка индикаторов компрометации (IoC) необходимо нажать кнопку **Обновить**.
При сканировании системы на индикаторы компрометации ведется сканирование только по активированным IoC (выделяются значком), деактивированные IoC (выделяются значком) при сканировании пропускаются**.** Для активации IoC необходимо выделить их на информационной панели и нажать кнопку **Активировать**, для деактивации нажать кнопку **Деактивировать**.
Для упрощения администрирования доступен поиск, по ключевым словам, с учетом регистра и поиск по всем столбцам таблицы на информационной панели (рис. 356). Для отображения поисковой строки необходимо нажать на кнопку **Поиск** на панели *Действия*.

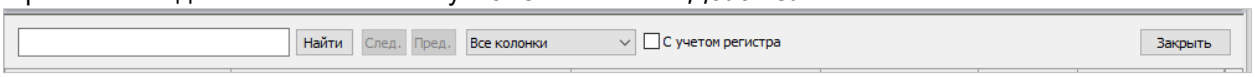


Рис. 356. Поиск по ключевым словам

Выбранные IoC-объекты можно сохранить, воспользовавшись кнопкой **Экспорт**, в выбранную папку в типе файла (JSON).
Для запуска сканирования системы на индикаторы компрометации необходимо нажать кнопку **Сканировать**, после чего начнется сканирование системы. Наблюдать за ходом процесса можно в категории *Отчеты*, раздел 18.1 Отчеты.

При сканировании системы на IoC имеются следующие ограничения:

- анализ объектов ФС сетевых дисков не производится;
- анализ объектов ФС и реестра осуществляется без учета регистра символов;
- если при сканировании ФС не удается получить доступ к объекту, то такой объект ФС пропускается;
- при анализе журналов **СЗИ** сканируются только текущие журналы, сканирование архивных журналов не производится.

Для остановки процесса сканирования необходимо нажать кнопку **Остановить** и в открывшемся окне нажать кнопку **Да** (рис. 357).

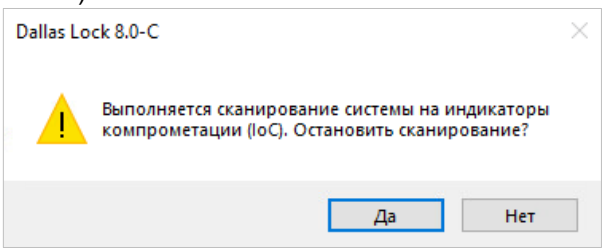


Рис. 357. Остановка поиска IoC

Сканирование системы на индикаторы компрометации (IoC) осуществляется путем проверки логических выражений, указанных в атрибуте «pattern» IoC-объектов. Если логическое выражение, указанное в «pattern» является истиной, то обнаружен IoC.

17.3 Индикаторы атаки (IoA)

В данной категории уполномоченный пользователь может управлять списком индикаторов атаки. Список (Рис. 358) состоит из индикаторов атаки, которые предварительно установлены в **СЗИ** или загружаются с серверов производителя при обновлении.

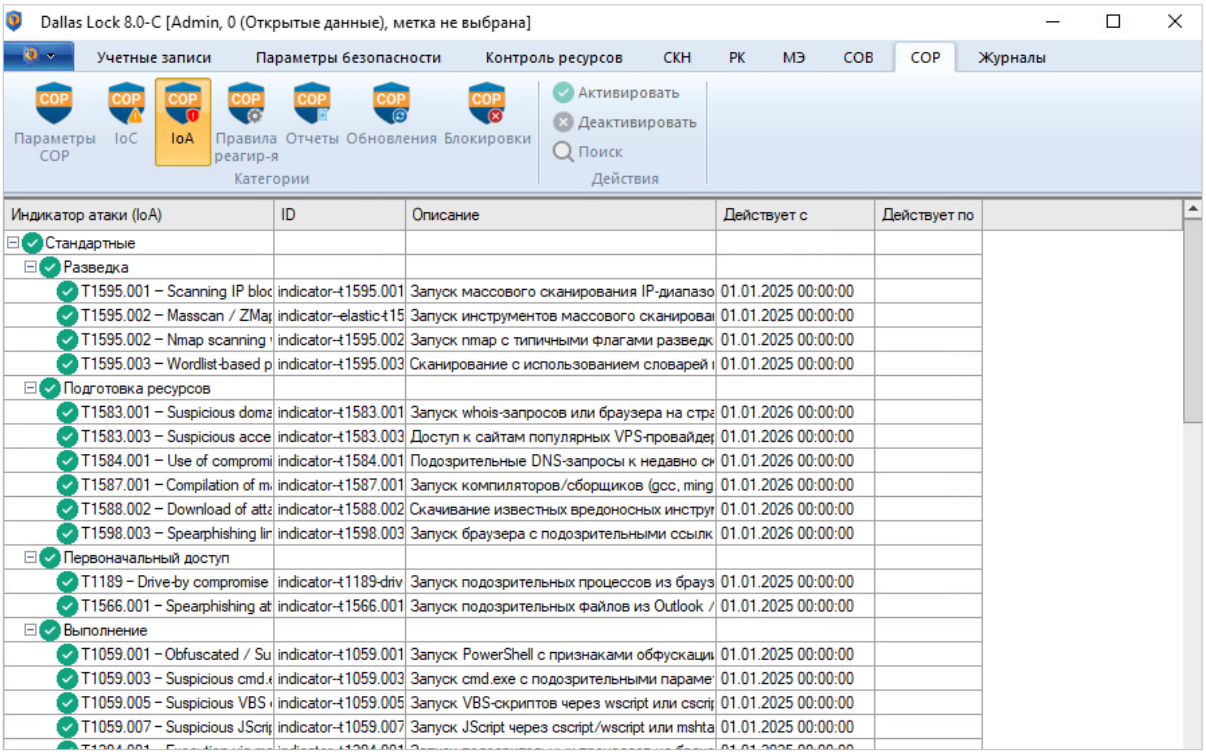


Рис. 358. Список индикаторов атаки

Реализована возможность активации, деактивации и поиска объектов в базе IoA-объектов.

17.4 Правила автоматического реагирования

СЗИ предоставляет возможность создания правил автоматического реагирования на обнаруженные индикаторы компрометации. Для создания, просмотра или редактирования правил автоматического реагирования **COP** необходимо во вкладке *COP* выбрать категорию **Правила реагирования** (рис. 359).

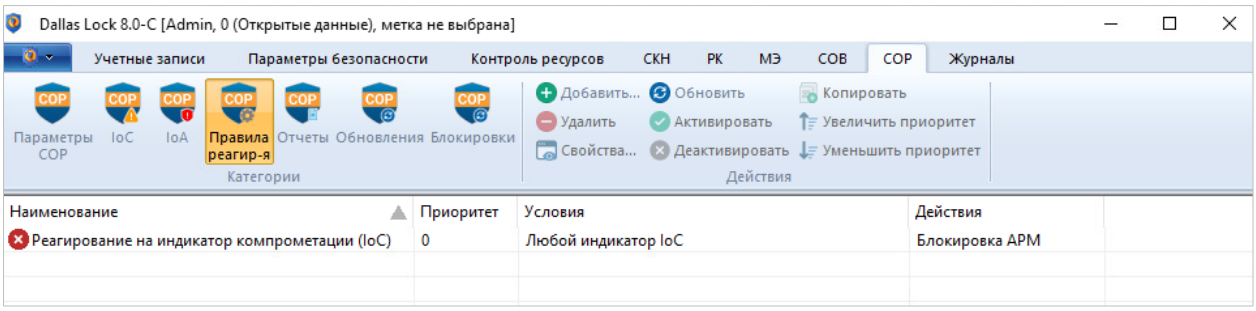


Рис. 359. Правила автоматического реагирования COP

Правила автоматического реагирования **COP** имеют следующие свойства:

1. Имя правила — уникальное имя правила длинной 1-255 символов;
2. Условия — индикатор или несколько индикаторов, разделенных операторами.
3. Действие — действие, выполняемое при срабатывании условия.
4. Активность — состояние правила: включено или выключено.

Для создания правила автоматического реагирования **COP** необходимо нажать кнопку **Добавить…** на панели *Действия*, откроется окно с выбором индикаторов (Рис. 360), после выбора откроется мастер создания правил автоматического реагирования, в котором необходимо задать параметры правила (рис. 361):

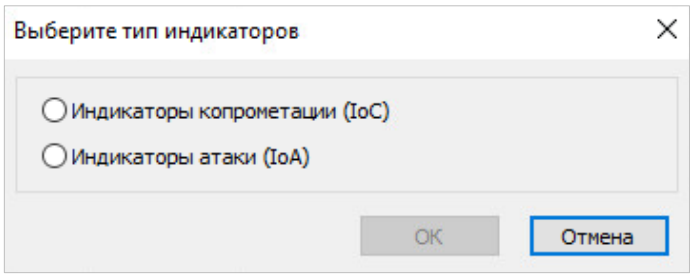


Рис. 360. Выбор типа индикаторов

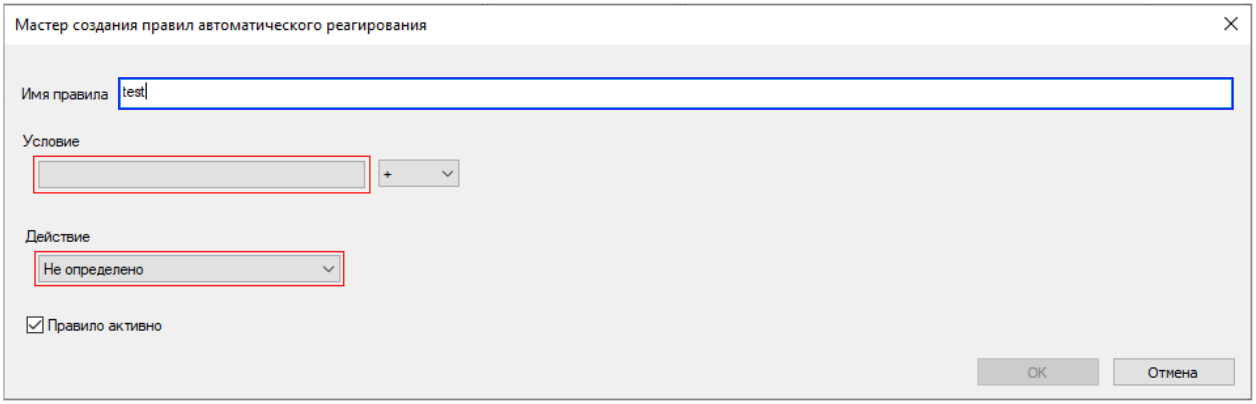


Рис. 361. Создание правила автоматического реагирования COP

1. Задать имя создаваемого правила, длинной 1-255 символов;
2. Настроить условие:
   - выбрать первый индикатор компрометации или отметить чекбокс *Любой индикатор* (рис. 362);

При активации чекбокса *Любой индикатор* выбор последующих индикаторов невозможен.

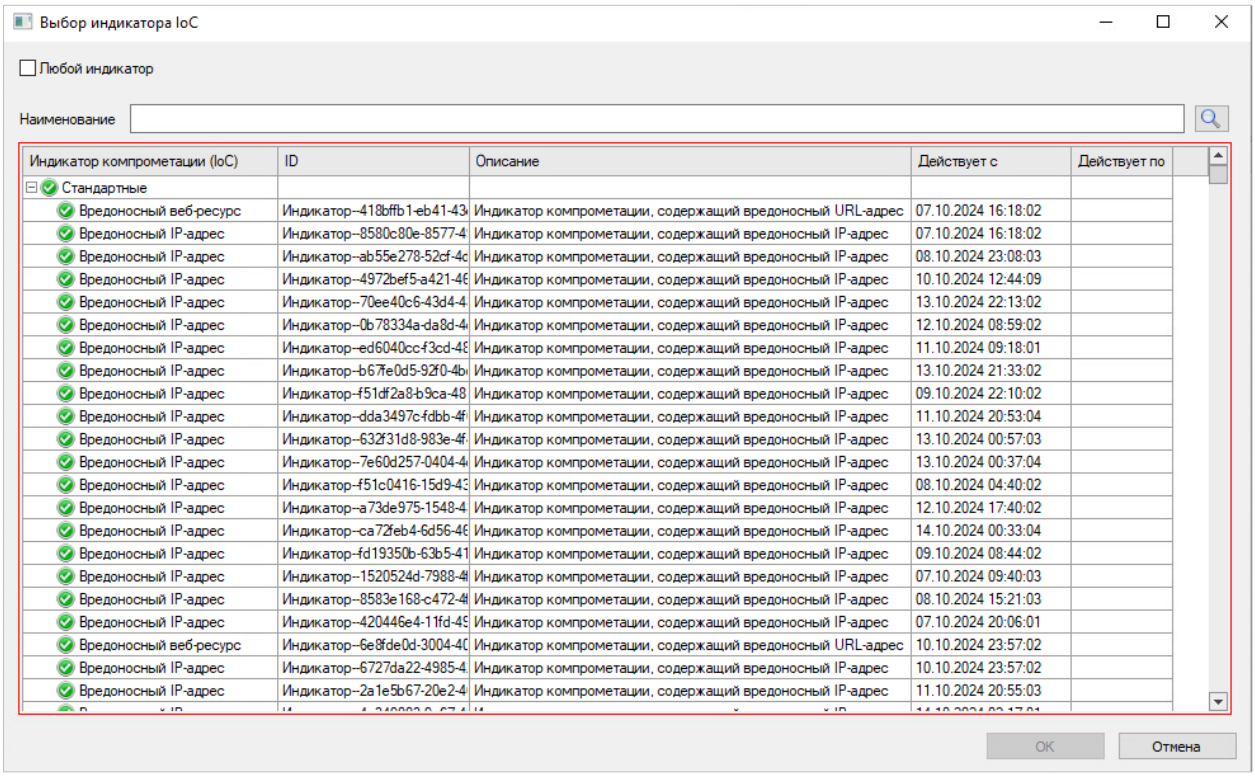


Рис. 362. Выбор индикатора компрометации

- при необходимости добавить дополнительный индикатор в выпадающем списке  выбрать логическое действие «И» или «ИЛИ» и выбрать следующий индикатор компрометации;

Максимальное количество индикаторов компрометации в правиле автоматического реагирования — 3.

- если индикатор компрометации необходимо удалить, то в выпадающем списке выбрать *Удалить*, удаляется тот индикатор компрометации, который находится справа от выпадающего списка;

В правиле автоматического реагирования **СОР** приоритетным является логический оператор «И».

Пример:

1. Пусть есть три индикатора: A, B и C.

2. Условия с логическим «И» означают, что все участвующие условия должны быть истинными. Например, A и B и C истинны.

3. Условия с логическим «ИЛИ» означают, что достаточно одного истинного условия из участвующих. Например, A или B или C истинно.

Если собрать условия по примеру:

- A и B или C: Истинно, если A и B оба истинны, или если C истинен.
- A или B и C: Истинно, если A истинен, или если B и C оба истинны.

Так используются комбинации логических операций «И» и «ИЛИ» для правил автоматического реагирования **СОР**.

3. Выбрать одно из действий **СОР**, представленных в таблице ниже.

Блокировка учетной записи
Блокируется активная УЗ (учетная запись с активной сессией в операционной системе) на АРМ, если в момент срабатывания правила активно несколько активных УЗ, то блокируются все. Если на момент срабатывания правила нет активной УЗ, то блокировка не происходит. Блокируется УЗ, относящаяся к найденному артефакту:

• файл – владелец файла (при невозможности определить владельца, действие не требуется); • процесс – пользователь (если процесс запущен не от системного пользователя). Выполнится блокировка АРМ (как при нажатии комбинации Win+L). При этом сессия пользователя не завершиться. В таблице «Заблокированные пользователи», в поле «Описание» для таких пользователей будет указано: «Заблокировано по причине срабатывания правила автоматического реагирования», в столбце «Время разблокировки» будет указано «Никогда».
Блокировка АРМ
Блокировка АРМ – режим работы компьютера, при котором вход любых пользователей, кроме администратора невозможен. Если в момент блокировки была активна сессия (сессии) пользователя, она не завершится.
Включение профиля «Изоляция узла»
Включается профиль МЭ «Изоляция узла».
Удалить файл
Удаление файла, соответствующего индикатору компрометации.
Завершение процесса
Завершение процессов, в том числе системных, а также блокирование их запуска.
Блокировка команд
Блокирование выполнения команд, определенных администратором средства обнаружения и реагирования на уровне узла, в командной строке на заданный промежуток времени.
Запуск сценария
Запуск программного обеспечения или командного сценария на узле для реагирования на вредоносное программное обеспечение или компьютерные атаки
Выключение АРМ
Завершение сеанса доступа в операционной системе на узле и выключение средства вычислительной техники.

4. Активировать или деактивировать правило, установив чекбокс *Правило активно* в соответствующее положение.
5. Нажать кнопку **ОК**.

Если не указано имя правила, не выбран хотя бы один индикатор компрометации или не выбрано действие, создание правила будет недоступно.

Для удаления правила автоматического реагирования **СОР** необходимо выбрать его в списке и нажать кнопку **Удалить**.

Редактирование правил автоматического реагирования **СОР** доступно при нажатии кнопки **Свойства…**, при этом редактирования правил аналогично процедуре их создания.

Для обновления списка и статуса заданий необходимо нажать кнопку **Обновить**.

При обнаружении индикаторов компрометации срабатывают только активированные правила (выделяются значком), деактивированные правила (выделяются значком) при обнаружении индикаторов не срабатывают**.** Для активации правил необходимо выделить их на информационной панели и нажать кнопку **Активировать**, для деактивации нажать кнопку **Деактивировать**.

Для упрощения создания правил можно воспользоваться механизмом копирования уже созданных правил автоматического реагирования **СОР**. Для этого необходимо:

1. Нажать кнопку **Копировать**.
2. В открывшемся окне задать имя для правила и нажать кнопку **ОК** (рис. 363).

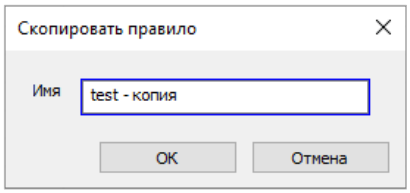


Рис. 363. Копирование правила автоматического реагирования СОР

Очередность срабатывания правил автоматического реагирования **СОР** определяет их приоритет, действия правила с приоритетом «0» считаются более приоритетными. Для редактирования приоритета правила необходимо выбрать его и нажать соответствующую кнопку **Увеличить приоритет** или **Уменьшить приоритет**.

Правило автоматического реагирования срабатывает только в том случае, если индикаторы компрометации обнаружены в ходе одного сканирования системы.

17.5 Отчеты

В категории **Отчеты** (рис. 364) располагается информация о сканированиях системы на индикаторы компрометации и срабатывании правил автоматического реагирования.
Рабочая область категории *Отчеты* содержит следующие столбцы:

1. Событие — поддерживает следующие типы событий: «Сканирование системы на индикаторы компрометации (IoC)», «Правило автоматического реагирования <наименование правила>», «Обновление базы индикаторов компрометации (IoC)».
2. Время — время события в формате: dd.MM.yyyy HH:mm:ss.
3. Статус — поддерживает следующие статусы событий «В процессе», «Выполнено», «Прервано».
4. Обнаруженные угрозы — количество обнаруженных угроз.

Количество записей в категории *Отчеты* ограничено 1000 шт. При архивации журнала **Журнал СОР** все события в категории *Отчеты* будут очищены.

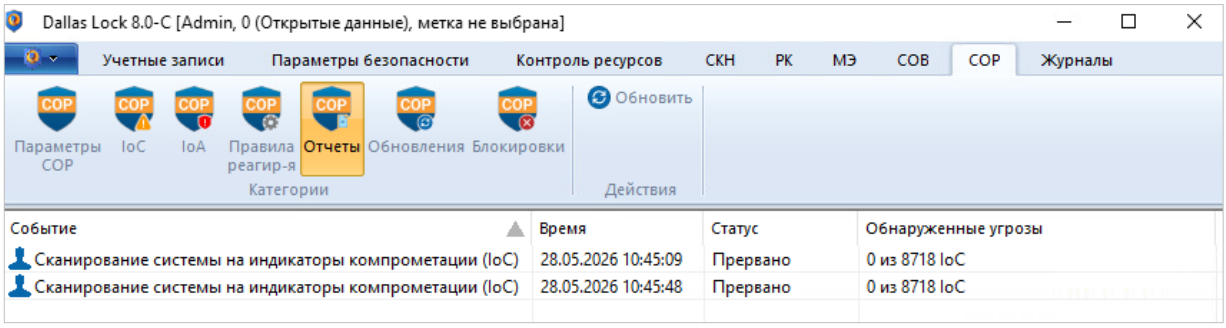


Рис. 364. Отчеты средства обнаружения и реагирования

При выборе записи в категории *Отчеты* откроется окно с подробной информацией о записи (рис. 365).

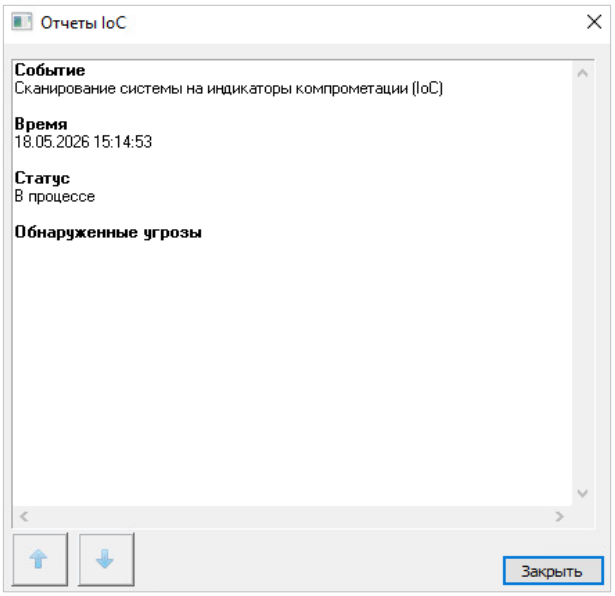


Рис. 365. Отчеты IoC

17.6 Обновления

В категории **Обновления** (Рис. 366) располагается информация об обновлениях базы индикаторов компрометации.
Рабочая область категории **Обновления** содержит следующие столбцы:

1. Название модуля — уникальное наименование модуля.
2. Время — время события в формате: dd.MM.yyyy HH:mm:ss.
3. Версия — версия обновления модуля.
4. Значение — поддерживает статусы «Вкл» и «Выкл».
5. Обновление — вид обновления.

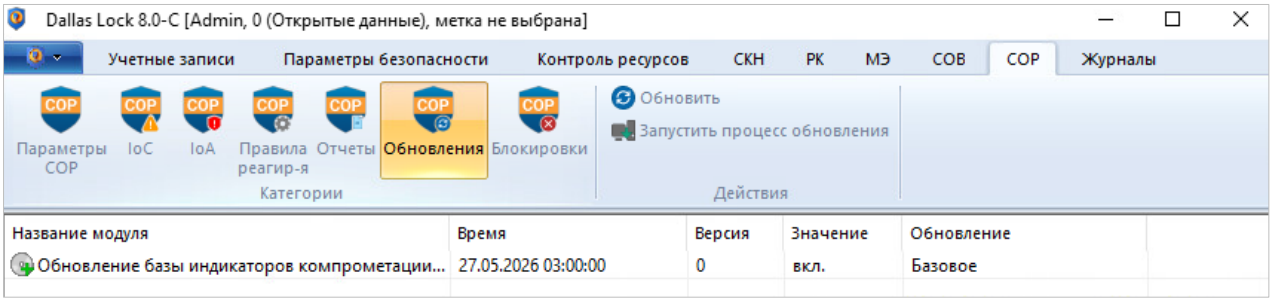


Рис. 366. Обновления средства обнаружения и реагирования

При двойном нажатии на запись в категории **Обновления** откроется окно с подробной информацией (рис. 367).

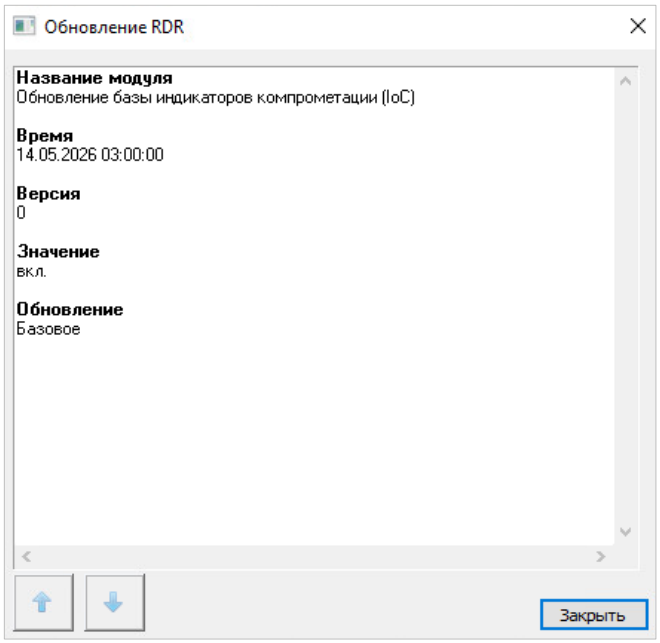


Рис. 367. Обновления RDR

17.7 Блокировки

В категории **Блокировки** располагается информация о заблокированных процессах.

Рабочая область категории **Блокировки** содержит следующие столбцы:

1. Процесс — уникальное наименование поцесса.
2. Исполняемый файл — расположение файла, который запускает соответствующий процесс.
3. Время блокировки — время начала события в формате: dd.MM.yyyy HH:mm:ss.

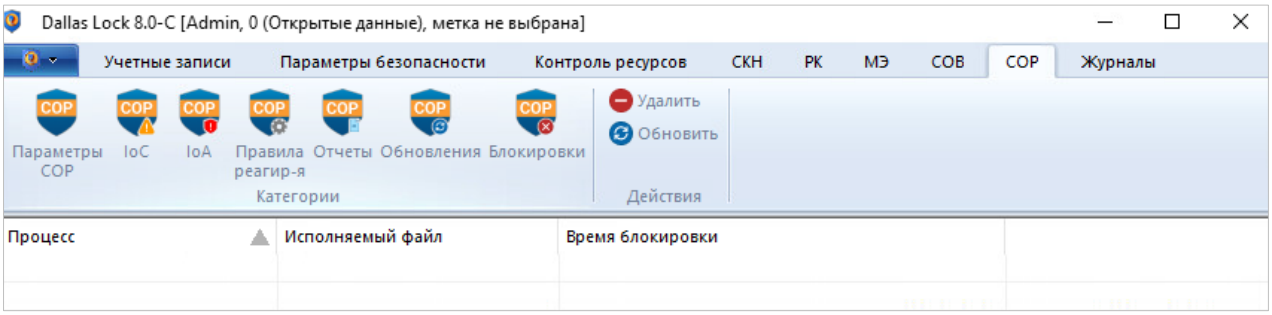


Рис. 368. Блокировки

Для разблокировки процесса необходимо выбрать его в списке и нажать кнопку **Удалить**. Для обновления текущей таблицы нажать кнопку **Обновить**.

17.8 Журнал СОР

В журнал средства обнаружения и реагирования заносятся события, связанные с индикаторами компрометации и правилами автоматического реагирования **СОР**.

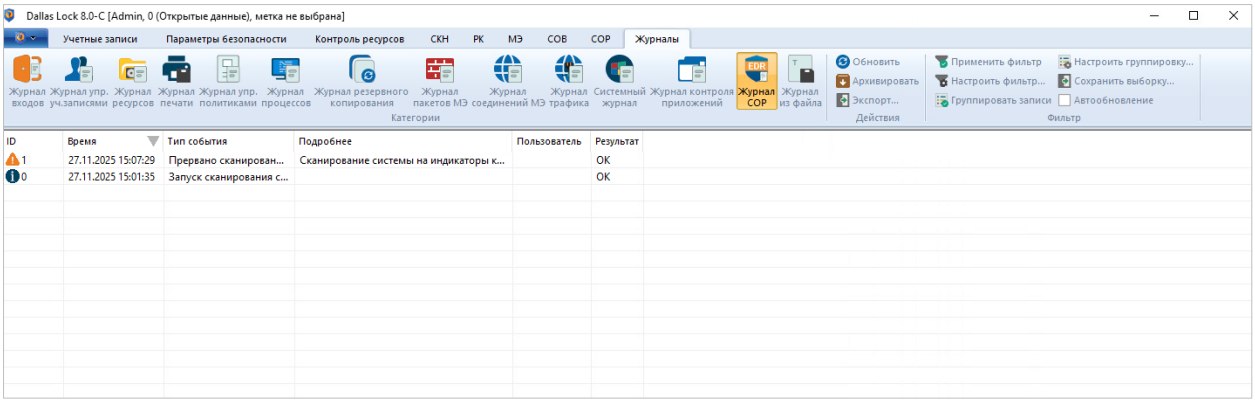


Рис. 369. Журнал СОР

Настройка журнала **СОР** находится во вкладке **Параметры безопасности → Политики аудита** (рис. 370).

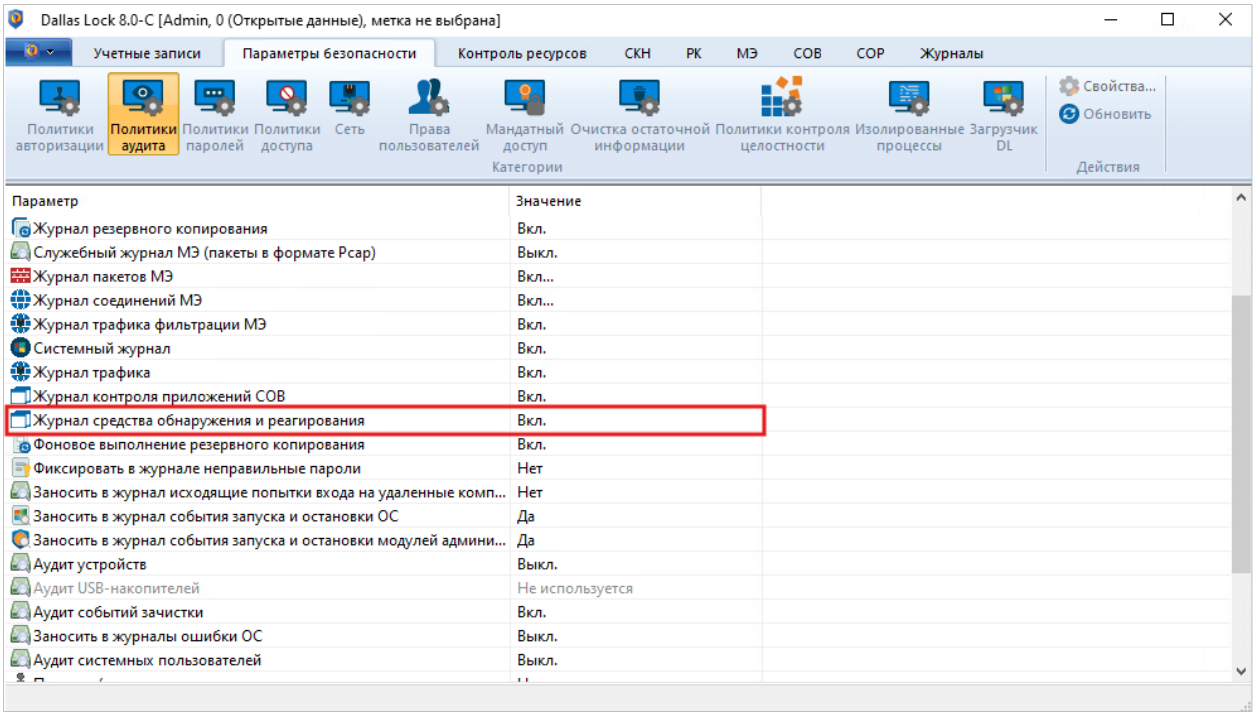


Рис. 370. Основные параметры работы журналов

Чтобы выключить журнал средства обнаружения и реагирования необходимо нажать правой кнопкой мыши на параметре **Журнал средства обнаружения и реагирования** и в появившемся окне выбрать пункт «*Выкл.*», после чего нажать кнопку **ОК** (рис. 371).

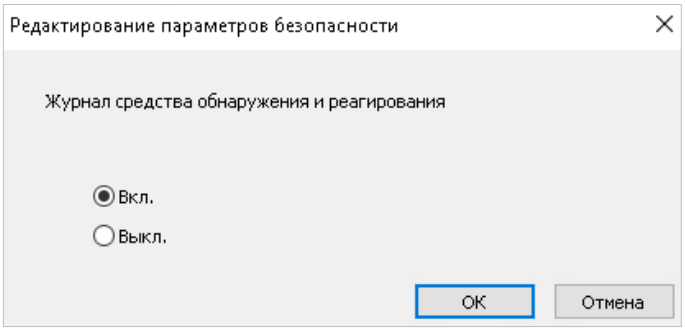


Рис. 371. Отключение ведения журнала СОР

В **Журнале управления политиками СЗИ** фиксирует события редактирования параметров и политик **СОР**. По умолчанию журнал включен (рис. 343).

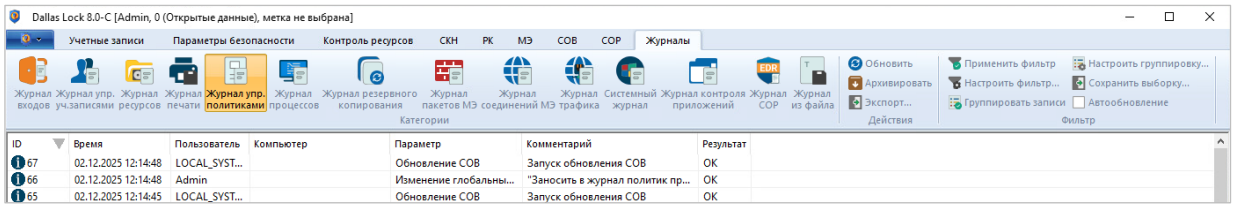


Рис. 372. Журнал управления политиками безопасности

Для просмотра и изменения политик и других параметров пользователь должен быть указан в значении параметров **СОР: Изменение настроек** и **СОР: Просмотр настроек** категории **Права пользователей** либо состоять в группе, указанной в данном параметре (Рис. 373).

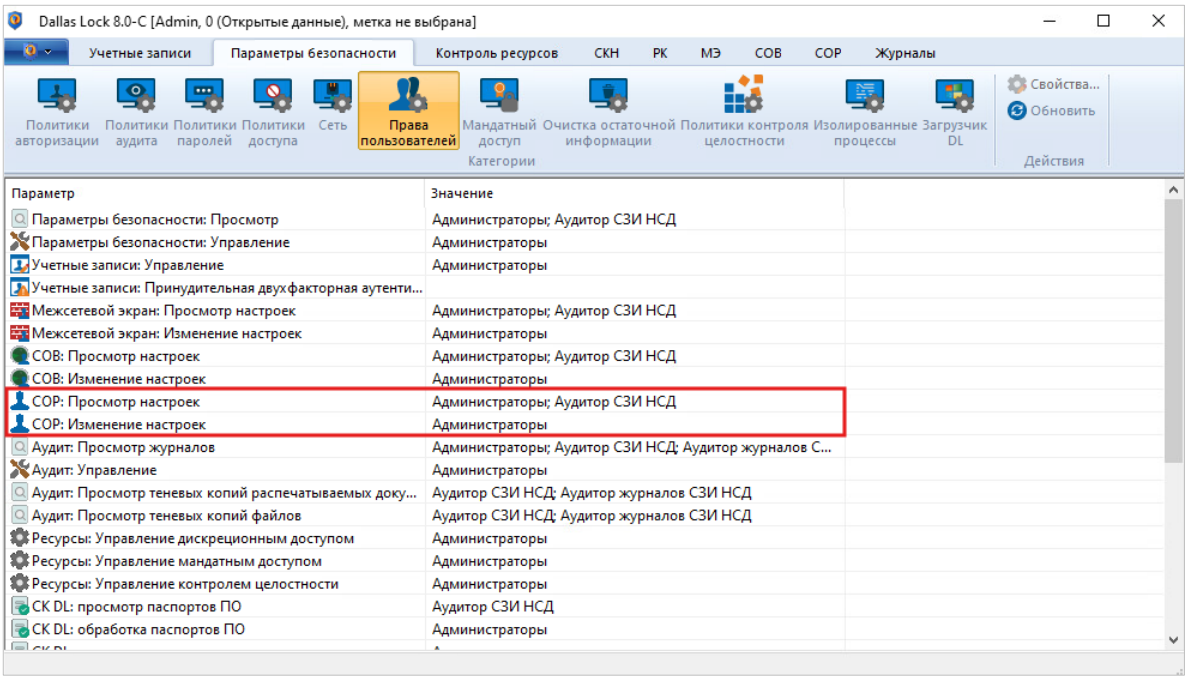


Рис. 373. Настройка аудита настроек СОР

18 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

18.1 Отчеты

18.1.1 Создание отчета о правах и конфигурации

В системе защиты **Dallas Lock 8.0** реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет по правам и конфигурации, который содержит упорядоченные списки пользователей с соответствующими правами на определенные ресурсы.

Для создания отчета по назначенным правам необходимо в оболочке администратора нажать кнопку основного меню и в появившемся меню выбрать *Отчеты → Отчет о правах и конфигурации* (рис. 374).

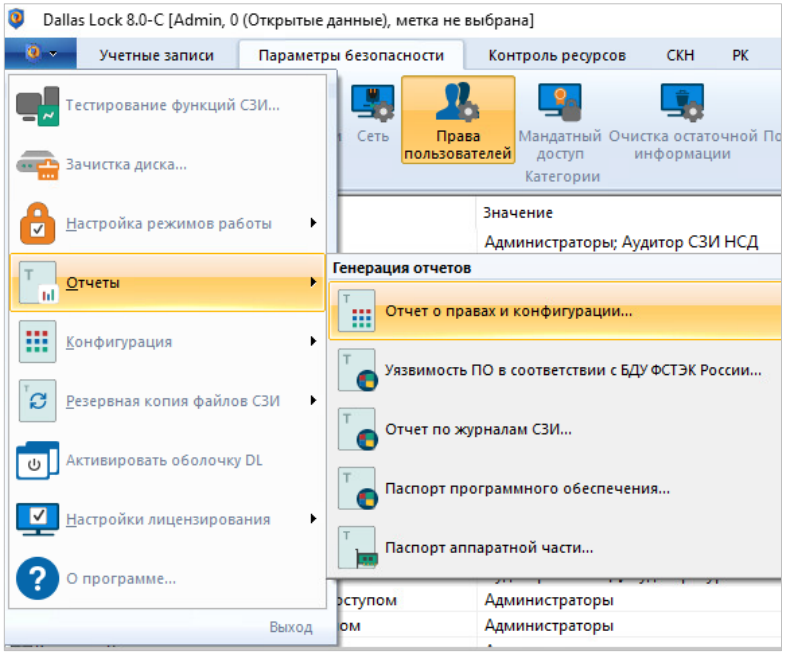


Рис. 374. Меню выбора дополнительных функций системы защиты

Появится окно с выбором параметров для формирования отчета (рис. 375):

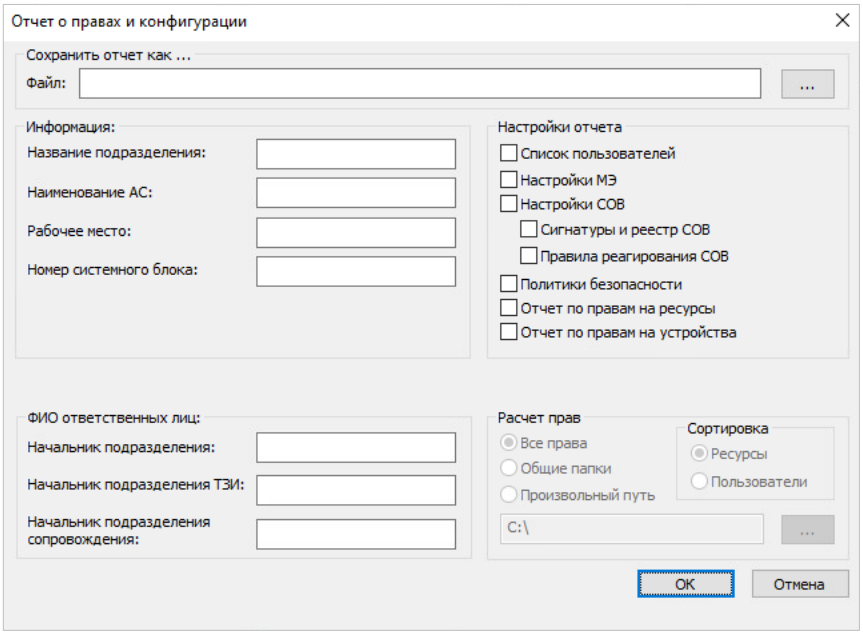


Рис. 375. Создание отчета по назначенным правам и конфигурации

В появившемся окне необходимо ввести следующие данные:

- ввести информацию о реквизитах, которые должны содержаться в документе;

- выбрать настройки отчета: по назначенным правам, список пользователей, политики безопасности;
- если в настройках указан отчет по правам на ресурсы, то необходимо выбрать их параметры: все права, общие папки или конкретный ресурс, указав его размещение (путь) и способ сортировки;
- указать имя отчета и путь для его сохранения.

При нажатии кнопки **ОК** будет создан отчет и открыт в текстовом редакторе. В отчете будет представлена матрица доступа для выбранных ресурсов со следующими значениями:

!R/R — Чтение (запретить/разрешить);
!W/W — Изменение/Запись (запретить/разрешить);
!E/E — Выполнение (запретить/разрешить);
!RA/RA — Чтение разрешений (запретить/разрешить);
!WA/WA — Запись разрешений (запретить/разрешить).

Данная функция может быть удобна для фиксирования настроек матрицы доступа на ФС и для возможности дальнейшей проверки соответствия этих настроек, сравнив с эталонным отчетом.

Событие формирования отчета фиксируется в журнале управления политиками.

18.1.2 Создание отчета об уязвимостях ПО в соответствии с БДУ ФСТЭК России

В системе защиты **Dallas Lock 8.0** реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет со списком уязвимостей ПО в соответствии с БДУ ФСТЭК России.

Для создания отчета об уязвимостях ПО в соответствии с БДУ ФСТЭК России необходимо в оболочке администратора нажать кнопку основного меню и в появившемся меню выбрать *Отчеты → Уязвимость ПО в соответствии с БДУ ФСТЭК России…* (Рис. 376).

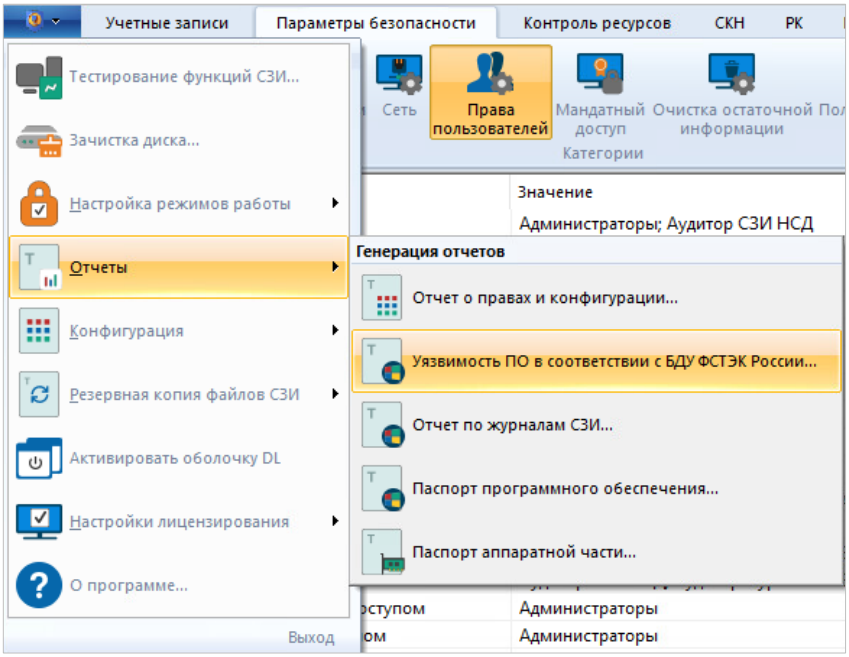


Рис. 376. Меню выбора дополнительных функций системы защиты

Появится окно ввода данных для формирования отчета «Уязвимость ПО в соответствии с БДУ», в котором необходимо ввести реквизиты (Рис. 377).

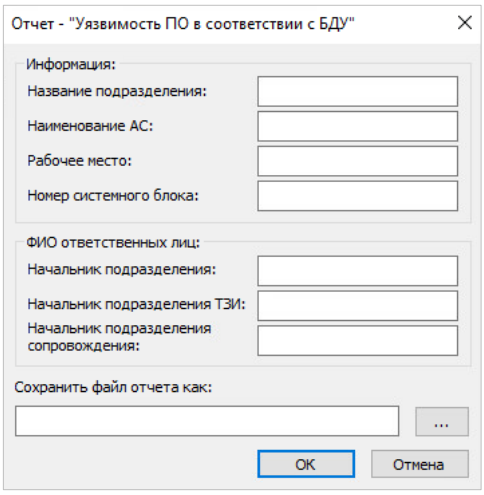


Рис. 377. Создание отчета по уязвимости ПО

Следует заполнить учетные данные и указать имя файла для сохранения отчета. После создания отчета будет предложено открыть его для просмотра (Рис. 378).

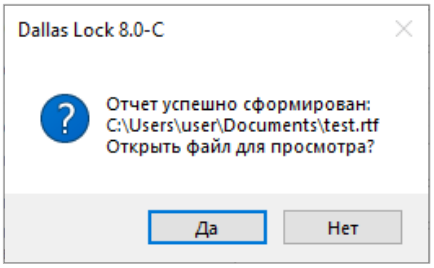


Рис. 378. Сохранение отчета по уязвимости ПО

Отчет об уязвимостях ПО будет сформирован в текстовом документе в указанном месте и содержать список найденных уязвимостей ПО в соответсвии с БДУ ФСТЭК России.

Событие формирования отчета об уязвимостях ПО фиксируется в журнале управления политиками.

18.1.3 Создание отчета по журналам СЗИ

В системе защиты **Dallas Lock 8.0** реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет по всем журналам СЗИ.

Для создания отчета по журналам СЗИ необходимо в оболочке администратора нажать кнопку основного меню и в появившемся меню выбрать *Отчеты → Отчет по журналам СЗИ* (Рис. 379).

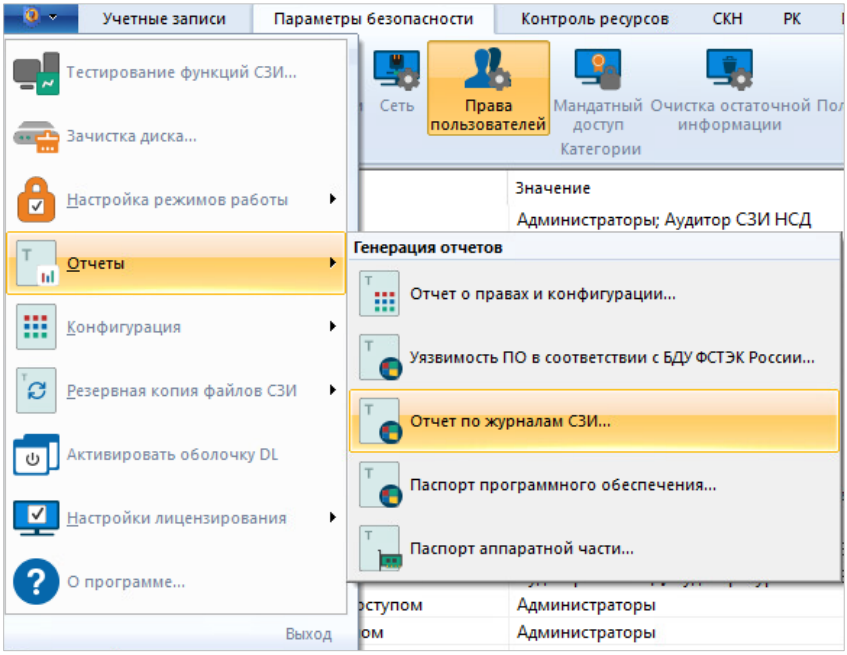


Рис. 379. Меню выбора дополнительных функций системы защиты

Появится окно ввода данных для формирования отчета по журналам СЗИ, в котором необходимо ввести реквизиты и указать путь для сохранения сформированного файла (Рис. 380).

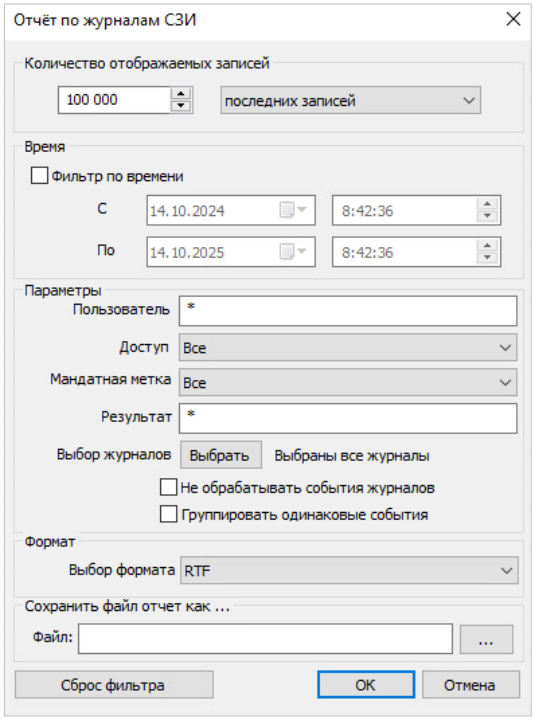


Рис. 380. Создание отчета по журналам СЗИ

Отчет по журналам СЗИ будет сформирован в текстовом документе в указанном месте и будет содержать данные по всем выбранным журналам.

Событие формирования отчета по журналам СЗИ фиксируется в журнале управления политиками.

18.1.4 Создание паспорта программного обеспечения

В системе защиты **Dallas Lock 8.0** реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет со списком программ, установленных на данном компьютере, размером их системных файлов и расчетом контрольных сумм — паспорт ПО автоматизированного рабочего места.

Для создания паспорта ПО необходимо в оболочке администратора нажать кнопку основного меню и в появившемся меню выбрать *Отчеты → Паспорт программного обеспечения* (рис. 381).

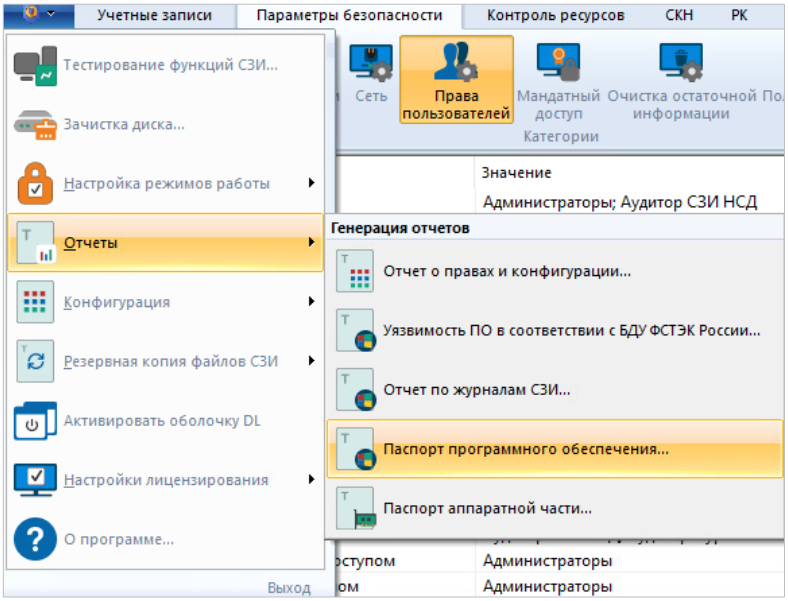


Рис. 381. Меню выбора дополнительных функций системы защиты

Появится окно ввода данных для формирования паспорта ПО, в котором необходимо ввести реквизиты (Рис. 382).

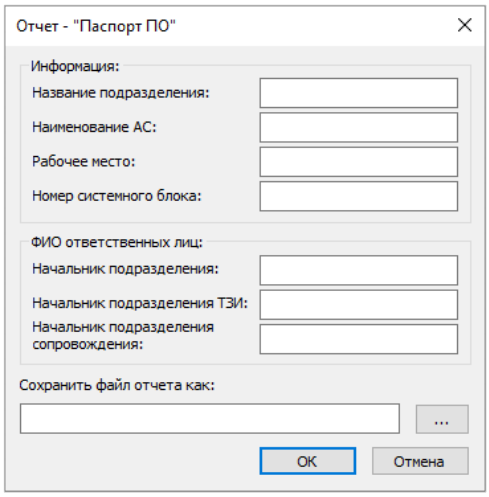


Рис. 382. Создание паспорта ПО

Следует заполнить учетные данные и указать имя файла для сохранения отчета. После создания отчета будет предложено открыть его для просмотра (Рис. 383).

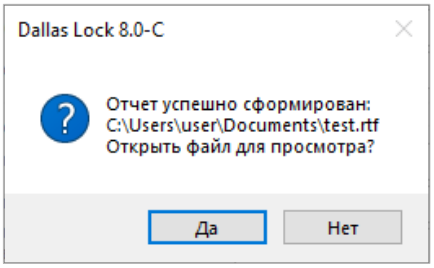


Рис. 383. Сохранение отчета паспорта ПО

Паспорт ПО будет сформирован в текстовом документе в указанном месте и содержать типовой[15] список параметров ПО, установленного на ПК.

Событие формирования паспорта ПО фиксируется в журнале управления политиками.

18.1.5 Создание паспорта аппаратной части ПК

В системе защиты **Dallas Lock 8.0** реализована функция, позволяющая пользователю, наделенному соответствующими полномочиями, сформировать отчет со списком и характеристиками установленных на данном компьютере устройств.

Для создания паспорта аппаратной части ПК необходимо в оболочке администратора нажать кнопку основного меню и в появившемся меню выбрать *Отчеты → Паспорт аппаратной части* (рис. 384).

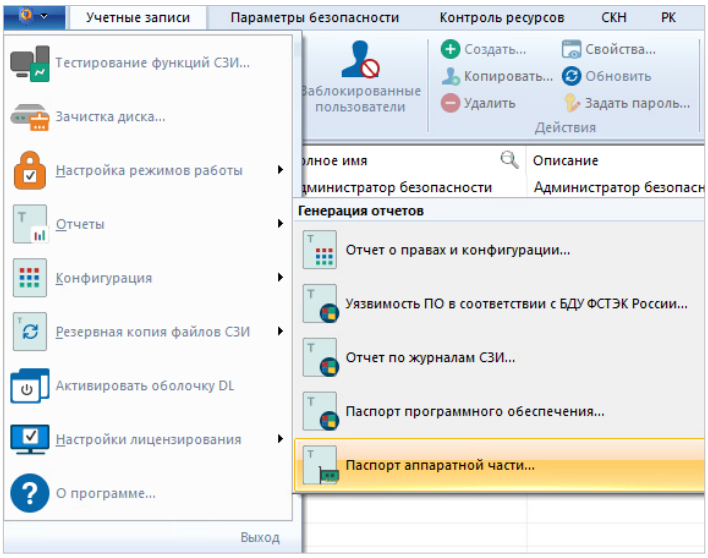


Рис. 384. Меню выбора дополнительных функций системы защиты

[15] В соответствии с Приложением 3 Приказа ЦБ РФ от 03.03.97 № 02-144.

Появится окно ввода данных для формирования документа, в котором необходимо ввести реквизиты и указать путь для сохранения сформированного файла (рис. 385).

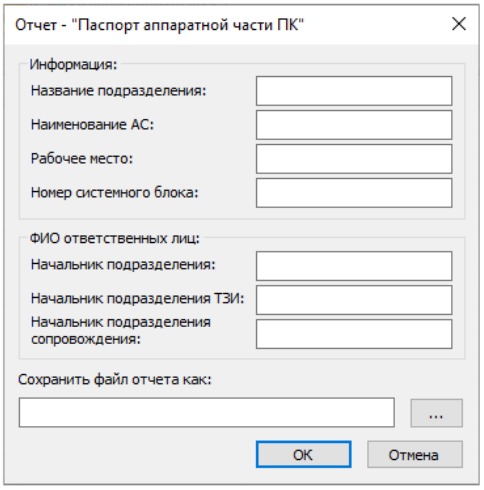


Рис. 385. Создание паспорта аппаратной части ПК

Паспорт аппаратной части будет сформирован в текстовом документе в указанном месте и будет содержать характеристики аппаратной конфигурации ПК.

Событие формирования паспорта аппаратной части ПК фиксируется в журнале управления политиками.

18.2 Автоматическое тестирование функций СЗИ

Данная функция позволяет выполнить автоматическое тестирование основных функциональных возможностей системы защиты (создание/удаление пользователя, назначение/снятие параметров доступа к ресурсам и пр.).

Для запуска автоматического тестирования функций **СЗИ** необходимо в оболочке администратора нажать кнопку основного меню и в списке функций выбрать пункт *Тестирование функций СЗИ* (рис. 386).

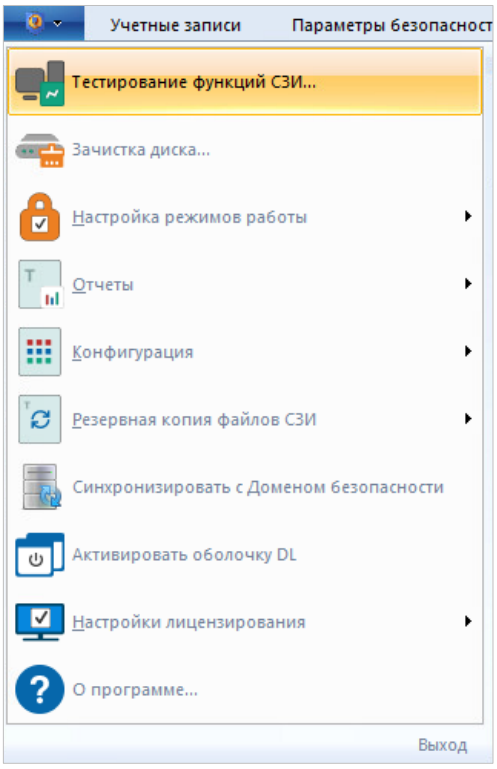


Рис. 386. Меню выбора дополнительных функций системы защиты

В появившемся окне нужно нажать кнопку **Запустить**.

По окончании тестирования, при необходимости, можно сохранить отчет, нажав кнопку **Сохранить** (рис. 387).

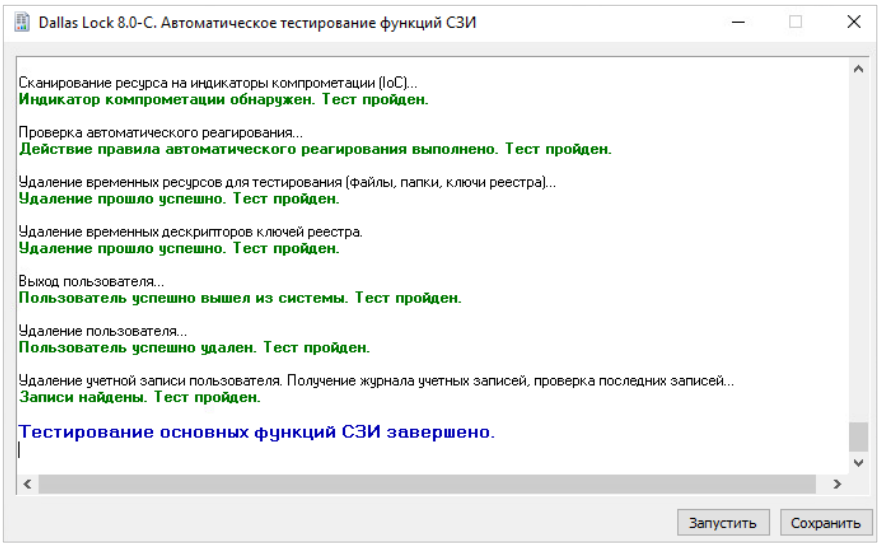


Рис. 387. Автоматическое тестирование функций СЗИ

Для сохранения отчета системой будет предложено выбрать папку для текстового файла. По умолчанию отчет сохранится в формате *.rtf.

В **Dallas Lock 8.0** редакции «С» функцию *Автоматическое тестирование функций СЗИ* можно запускать, только в случае авторизации под мандатным уровнем 0: «Открытые данные».

18.3 Сохранение резервной копии файлов СЗИ

В **СЗИ** реализован механизм создания и сохранения резервной копии файлов локально установленной **СЗИ**. Данная функция предназначена для ведения нескольких копий программных компонентов **СЗИ**, с возможностью последующей сверки с текущими файлами, используемыми в **СЗИ**, обнаружения несоответствий (проверяется не только совпадение размера, но и содержимое файлов) и возможностью восстановления.

Чтобы сохранить резервную копию файлов **СЗИ**, необходимо в оболочке администратора нажать кнопку основного меню и в появившемся списке дополнительных функций выбрать *Резервная копия файлов СЗИ → Сохранить резервную копию файлов СЗИ* (рис. 388).

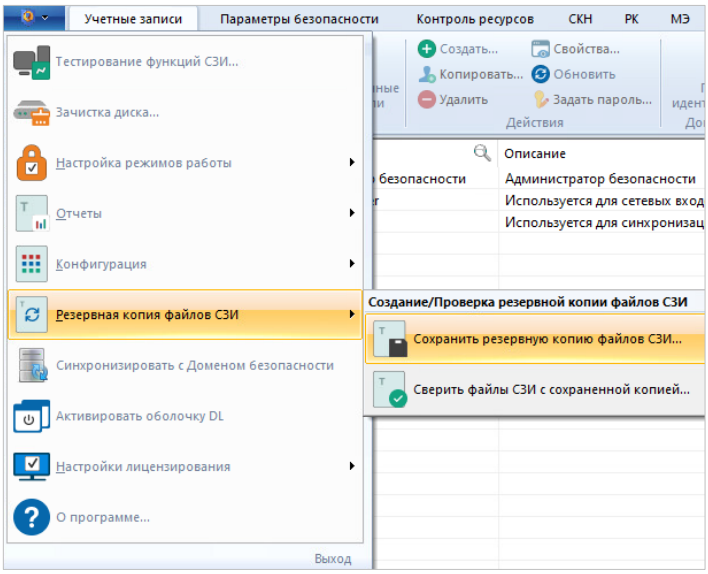


Рис. 388. Меню выбора дополнительных функций системы защиты

После этого выведутся окно проводника, в котором необходимо указать путь и название папки, в которой создастся новая папка, содержащая копии файлов системы защиты. Далее — нажать **Сохранить**. В указной папке будет сохранена резервная копия файлов **СЗИ**, и выведено соответствующее сообщение системы (рис. 389).

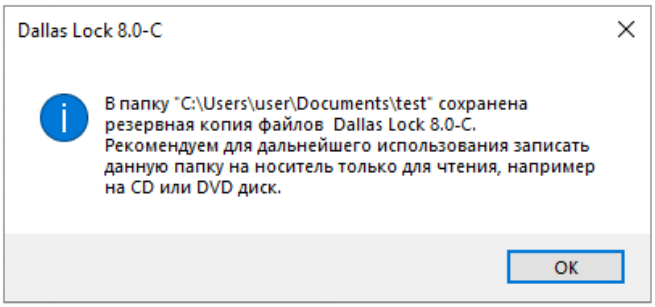


Рис. 389. Сообщение системы о сохранении резервной копии файлов

Для того, чтобы сверить резервную копию файлов **СЗИ** с файлами, используемыми в системе, необходимо в оболочке администратора выбрать соответствующий пункт (рис. 388).

После этого появится окно, в котором необходимо указать расположение сохраненной копии файлов **СЗИ** и выбрать файл конфигурации (*.ini). После нажатия кнопки **Открыть** система выполнит проверку и выведет сообщение о результатах сравнения.

Если копии файлов **СЗИ** и файлов, используемых в системе, совпадают, будет выведено соответствующее сообщение (рис. 390).

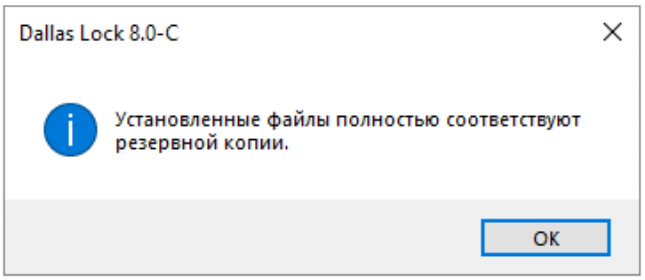


Рис. 390. Сообщение об успешной сверке файлов СЗИ

При обнаружении несоответствий (проверяется не только совпадение размера, но и содержимое файлов) будет выведено предупреждающее сообщение (рис. 391).

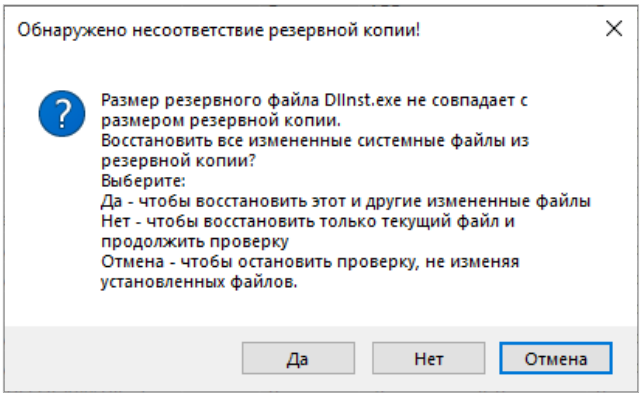


Рис. 391. Несоответствие файлов при сверке

Если выбрать **Да** или **Нет**, система восстановит Измененные файлы на основании сохраненной копии файлов и выведет сообщение о том, что файлы полностью соответствуют резервной копии. При нажатии кнопки **Отмена** система продолжит работу с измененными системными файлами, но выведет предупреждение (рис. 392).

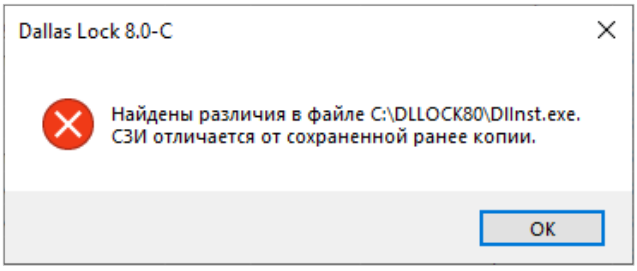


Рис. 392. Сообщение системы о несоответствии файлов при сверке

18.4 Возврат к настройкам по умолчанию

В некоторых случаях бывает необходимо полностью или в большой степени изменить параметры безопасности, установленные в системе защиты. С этой задачей можно справиться, не прибегая к переустановке системы, а вернув системе защиты **Dallas Lock 8.0** настройки по умолчанию.

Следует учесть, что помимо возврата всех настроек, в том числе настроек доступа и аудита к изначальным настройкам, учетных записей пользователей, созданных прежде в системе защиты, не окажется. Но так как при создании новых пользователей в **СЗИ**, их учетная запись создается и в ОС, то при возврате к настройкам по умолчанию, необходимые учетные записи можно снова зарегистрировать, выбрав их из списка локальных.

Для того, чтобы вернуть системе защиты ее исходное состояние, необходимо в списке функций кнопки основного меню выбрать *Конфигурация → Установить настройки по умолчанию* (рис. 393).

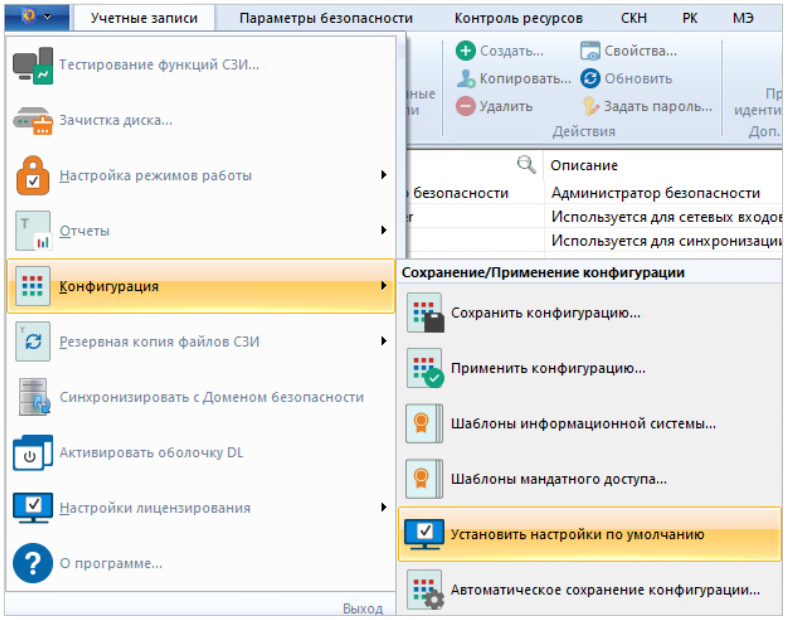


Рис. 393. Выбор установки настроек системы по умолчанию

Появится окно подтверждения установки настроек по умолчанию (рис. 394).

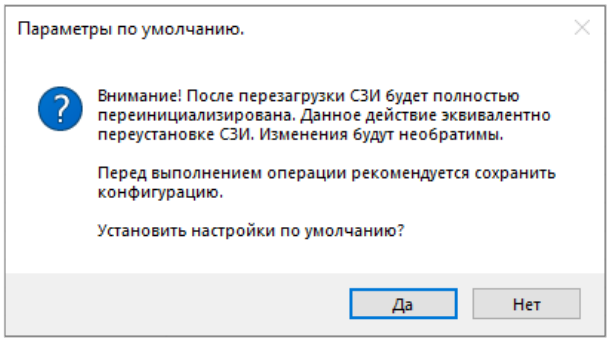


Рис. 394. Подтверждение установки настроек по умолчанию

После подтверждения установки появится сообщение об успешном завершении операции.

Для завершения установки первоначальных настроек системы защиты **Dallas Lock 8.0** необходимо самостоятельно перезагрузить компьютер.

> **!** После применения параметров по умолчанию и до перезагрузки ПК производить преобразование жесткого диска нельзя! Это приведет к невозможности загрузки ОС.
>
> Также следует учесть, что в процессе установок параметров по умолчанию будут удалены ключи преобразования съемных накопителей. Если в **СЗИ** были преобразованы съемные накопители, то параметры ключей необходимо заранее сохранить.

18.5 Шаблоны информационных систем

В СЗИ предусмотрены предустановленные шаблоны безопасности, соответствующие стандартам защиты автоматизированных систем, информационных систем персональных данных и государственных информационных систем.

Для применения предустановленного шаблона необходимо в главном меню выбрать функцию *Конфигурация → Шаблоны информационной системы*. Появится окно, в котором следует указать тип информационной системы и класс (уровень) защищенности, согласно следующим нормативным документам (рис. 395):

– Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) (АС).

– Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей. государственную тайну, содержащейся в государственных информационных системах» (ГИС).

– Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ИСПДн).

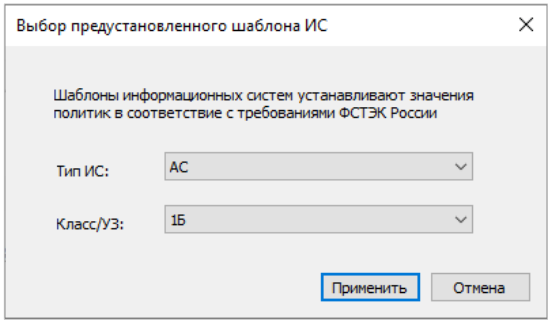


Рис. 395. Выбор предустановленного шаблона информационной системы

Изменение настроек применяется через диалоговое окно (рис. 396) с кнопками:

- **Да** — применяются только те настройки, которые в шаблоне более строгие, чем текущие; остальные остаются неизменными;
- **Нет** — применяются все настройки в соответствии с шаблонами, ПРИЛОЖЕНИЕ А;
- **Отмена** — окно закрывается без применения изменений.

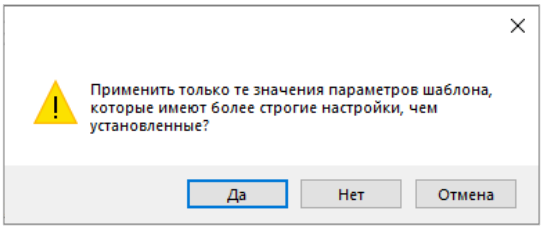


Рис. 396. Выбор параметров применения шаблона информационной системы

Если АИБ установил свои значения политик, то при применении шаблона, в котором эта политика не имеет конкретного значения (необязательная), данные политики не перезаписываются, а остаются теми, что установил АИБ.

19 СОХРАНЕНИЕ КОНФИГУРАЦИИ

19.1 Сохранение файла конфигурации Dallas Lock

После того, как была произведена настройка системы защиты **Dallas Lock 8.0** согласно требованиям, были зарегистрированы пользователи, и им были предоставлены необходимые права и полномочия, администратор безопасности может сохранить все или определенные настройки системы защиты в специальном файле конфигурации.
Для сохранения настроек системы защиты необходимо в списке функций кнопки основного меню выбрать *Конфигурация → Сохранить конфигурацию* (рис. 397).

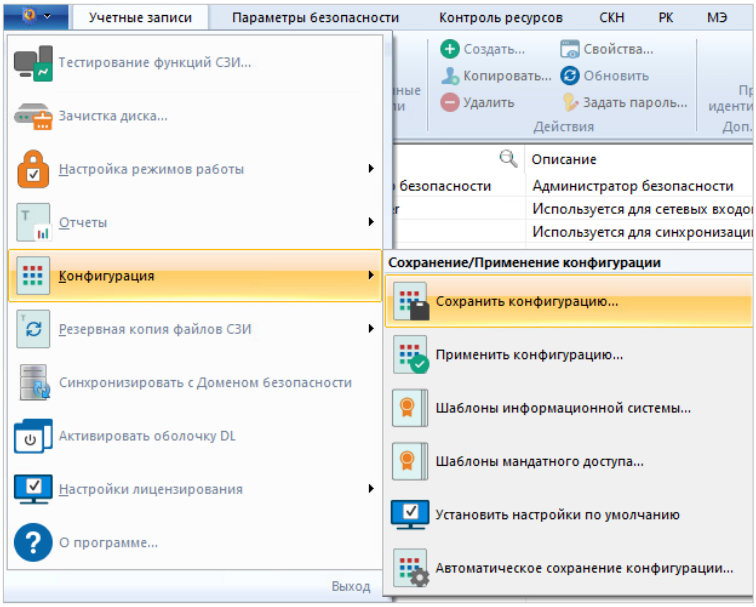


Рис. 397. Выбор сохранения конфигурации

Появится окно с выбором параметров системы защиты для их сохранения (рис. 398).

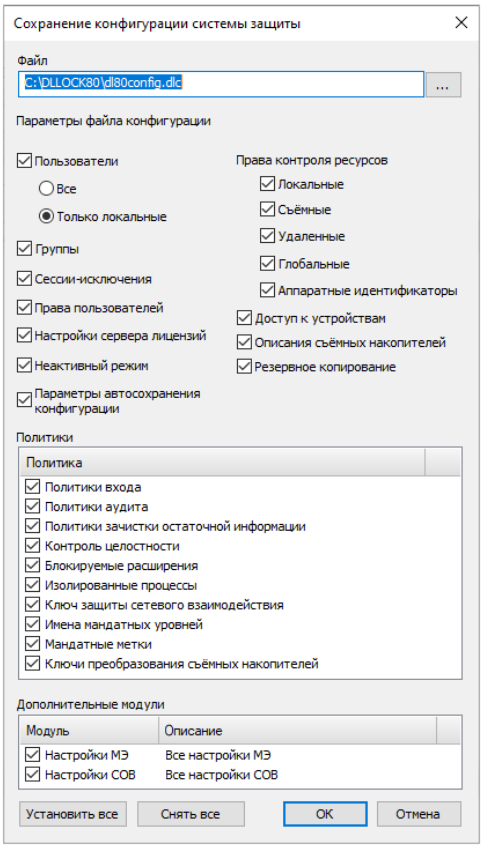


Рис. 398. Окно для выбора параметров при сохранении их в файле конфигурации

В данном окне необходимо отметить названия параметров, выбрать расположение и имя файла, в котором будет сохранена конфигурация (по умолчанию это системная папка DLLOCK80). После нажатия кнопки **ОК** файл конфигурации будет сформирован и сохранен. Появится подтверждение операции. Сохраненный файл конфигурации будет иметь расширение *.dlc.

Если на клиенте системы защиты **Dallas Lock 8.0**, находящемся в одном домене AD, зарегистрированы учетные записи из другого домена AD, и эти домены не связаны, то сохранение конфигурации с параметром **Пользователи** → **Все** приведет к ошибке.

19.2 Автоматическое сохранение конфигурации

В **Dallas Lock 8.0** реализовано автоматическое сохранение конфигурации, которое позволяет настроить регулярное и автоматизированное сохранение конфигурации системы защиты **Dallas Lock 8.0**.

Для настройки автоматического сохранения конфигурации необходимо в списке функций кнопки основного меню выбрать *Конфигурация* → *Автоматическое сохранение конфигурации* (рис. 397). После будет открыто окно (Рис. 400), где необходимо указать следующие параметры автоматического сохранения:

- *Полный путь к файлу конфигурации* — путь, по которому будет осуществляться сохранение конфигураций;
- *Частота сохранения конфигурации* — позволяет указать периодичность сохранения конфигурации. Возможные значения от 5 минут до ежемесячно или «Не используется».
- *Расписание сохранения конфигурации* — позволяет задать расписание, по которому будет осуществляться сохранение конфигурации. При нажатии на кнопку открывается окно *Настройка расписания* (Рис. 399), где необходимо активировать чекбокс *Использовать расписание* и далее в поле *Время:* выбрать время сохранения конфигурации, в поле *Дни недели:* указать дни, в которые будет осуществляться сохранение. Нажать кнопку **Добавить** для добавления записи в список. Для удаления записи из списка необходимо выбрать запись и нажать кнопку **Удалить**. После настройки для сохранения расписания необходимо нажать кнопку **ОК**.

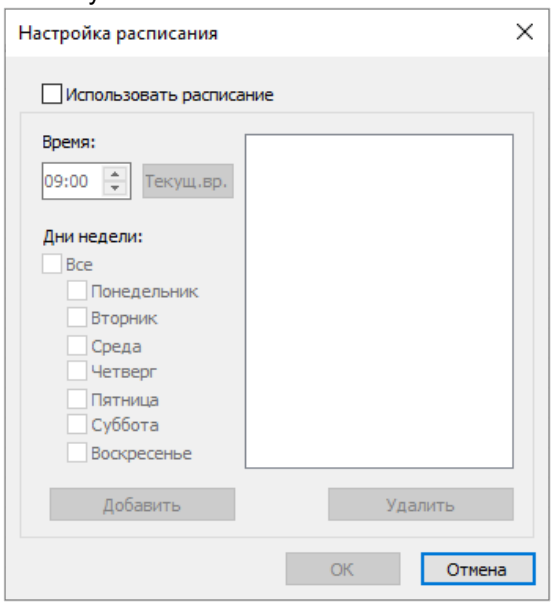


Рис. 399. Окно для настройки расписания для автоматического сохранения конфигурации

- *Максимальное количество* — позволяет указать максимальное количество сохраненных конфигураций. Возможные значения от 1 до 100, значение по умолчанию — 10.
- Чекбокс *При сохранении конфигурации использовать следующую учетную запись* позволяет указать логин и пароль учетной записи пользователя, от имени которого будет осуществляться сохранение конфигурации.

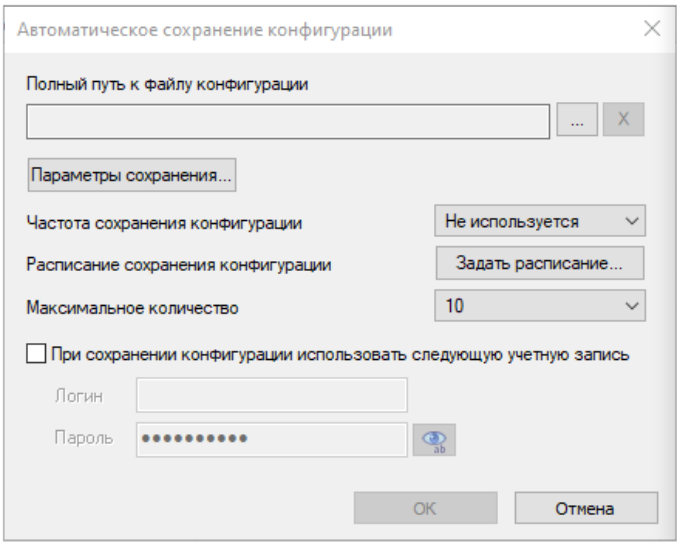


Рис. 400. Окно автоматического сохранения конфигурации

Для сохранения настроек необходимо нажать кнопку **ОК**.

Сохраненный файл конфигурации имеет следующее имя: ServerConfiguration YYYY-MM-DD hh-mm-ss.dlsc2, где YYYY-MM-DD — дата сохранения конфигурации, hh-mm-ss — время сохранения конфигурации.

Если количество файлов конфигурации в каталоге, указанном в поле *Полный путь к файлу конфигурации*, превышает максимальное количество — их количество приводится в соответствие параметру **Максимальное количество** путем удаления наиболее старых файлов. Наиболее старый файл конфигурации из оставшихся перезаписывается. Учитываются только файлы, имеющие формат имени YYYY-MM-DD hh-mm-ss.dlsc2.

19.3 Применение файла конфигурации Dallas Lock

Файл конфигурации может быть использован в следующих случаях:

1. При установке системы защиты. В этом случае рекомендуется сохранять файл конфигурации со всеми параметрами.

   Применение файлов конфигурации в процессе установки может быть полезно, если, например, необходимо защитить с помощью **Dallas Lock** несколько автономных компьютеров, но на настройку политик безопасности на каждом компьютере по отдельности тратить время нет возможности или желания. В этом случае можно настроить **СЗИ** на одном компьютере, сохранить его полную конфигурацию и при установке на остальные компьютеры, использовать полученный файл конфигурации.

2. В произвольный момент времени на локально установленной **СЗИ**.

   Для этого в списке функций кнопки основного меню оболочки администратора необходимо кликнуть пункт **Применить конфигурацию** (рис. 397).
   Откроется окно проводника для поиска файла конфигурации. Требуется выбрать данный файл и нажать кнопку **Открыть**. После этого система защиты применит данный файл, изменив свои параметры безопасности. На экране появится окно-отчет с информацией об операции.

20 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Для реализации централизованного управления различными модулями на клиентах необходимо использовать **Единый центр управления Dallas Lock** (**ЕЦУ Dallas Lock**), управление которым осуществляется отдельным приложением **Консоль ЕЦУ**.

ЕЦУ Dallas Lock позволяет осуществлять централизованное управление такими модулями клиентов, как **СЗИ Dallas Lock 8.0** редакций «К» и «С» (включая компоненты **МЭ**, **СОВ, СОР** и **СКН**), **СЗИ Dallas Lock Linux**, **СЗИ ВИ Dallas Lock**, **СДЗ Dallas Lock**, **СДЗ УБ Dallas Lock** и шлюз безопасности **WAF Dallas Lock**.

При работе с модулями **Dallas Lock 8.0** редакций «К» и «С» доступны следующие возможности:

- завершение работы и перезагрузка модуля;
- отображение информации о состоянии модуля;
- синхронизация политик/пользователей;
- удаленное развертывание модуля на АРМ;
- удаленное обновление модуля на АРМ;
- удаленная разблокировка АРМ;
- управление пользователями, в том числе заблокированными и группами пользователей на модуле;
- управление политиками безопасности;
- управление заданиями на:
  - получение отчета о локальных группах и входящих в них пользователях;
  - получение конфигурации;
  - применение конфигурации;
  - проверку целостности контролируемых объектов;
  - архивацию локальных журналов модуля;
  - сканирование системы на наличие индикаторов компрометации (IoC);
  - проверку установленного ПО на уязвимости;
  - удаление модуля;
  - изменение параметров лицензии;
  - формирование отчета по журналам;
  - самотестирование функций СЗИ;
  - сбор данных об АРМ;
- сбор журналов модуля;
- отправка сигнализации об инцидентах безопасности;
- настройка неактивного режима работы модуля или компонентов;
- управление мандатными метками (только для Dallas Lock 8.0 редакции «С»);
- настройка аппаратных идентификаторов;
- перераспределение терминальных сессий;
- управление профилем МЭ «Изоляция узла», позволяющим изолировать АРМ от сети передачи данных с возможностью управления со стороны ЕЦУ;
- централизованное управление межсетевым экраном;
- централизованное управление компонентом СОВ, включая управление индикаторами компрометации (IoC) и правилами автоматического реагирования в рамках СОР;
- централизованное управление компонентом СКН, включая управление ключами преобразованных съемных накопителей;
- централизованное управление контролем устройств, включая контроль отдельных принтеров;
- управление разблокировкой компьютера с установленным модулем.

Некоторые параметры безопасности могут быть настроены сразу для всего **ДБ**, некоторые — для отдельных клиентов.

ЕЦУ предназначен для использования на ТС, таких как: персональные компьютеры, портативные компьютеры (ноутбуки, планшеты), серверы и ТС с поддержкой виртуальных сред (по технологии VMware и пр.) и технологии Windows To Go[16], работающих на 64-битной архитектуре процессоров под управлением операционных систем семейства Windows (x64):

- Windows 8.1 (Core, Pro, Enterprise);
- Windows 10 (Enterprise, Education, Pro, Home);
- Windows 11 (Enterprise, Education, Pro, Home);

[16] Поддержка технологии Windows To Go осуществляется только для Консоли ЕЦУ Dallas Lock.

- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- Windows Server 2019 (Essentials, Standard, Datacenter);
- Windows Server 2022 (Standard, Datacenter);
- Windows Server 2025 (Standard, Datacenter);

и семейства GNU Linux[17] (x64):

- Debian 10.x;
- Debian 11.x;
- Debian 12.x;
- Ubuntu 18.04 LTS;
- Ubuntu 20.04 LTS;
- Ubuntu 22.04 LTS;
- Ubuntu 24.04 LTS;
- Astra Linux Common Edition (Орел) 2.12;
- Astra Linux Special Edition (Смоленск) 1.6, 1.7, 1.8;
- Альт Рабочая Станция 9.x;
- Альт Рабочая Станция 10.0, 10.1, 10.2, 10.4, 11.1;
- Альт Рабочая Станция К 10.0, 10.1, 10.3, 10.4;
- Альт Сервер 9;
- Альт Сервер 10.0, 10.1, 10.2, 10.4;
- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- РЕД ОС 7.3 Муром;
- РЕД ОС 8;
- МСВСфера АРМ 9;
- ROSA FRESH DESKTOP 12.



Для обработки обращений от **ЕЦУ** должны быть открыты TCP/IP порты 17901 и 17903.

С подробным описанием **ЕЦУ Dallas Lock** можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock (RU.48957919.26.20.40.142.001 И6).

[17] Для инсталляции и работы с консолью **ЕЦУ** под ОС семейства Linux требуется графическая оболочка.

21 ВОССТАНОВЛЕНИЕ КОМПЬЮТЕРА ПРИ СБОЕ СИСТЕМЫ ЗАЩИТЫ

В некоторых случаях возможны ситуации, когда по каким-либо причинам доступ на ЗАРМ осуществить невозможно. Невозможно загрузить ОС предположительно из-за сбоя работы системы защиты **Dallas Lock 8.0**.

В этом случае можно воспользоваться аварийным отключением системы защиты. Аварийное отключение может производиться в ручном режиме или в автоматическом с помощью диска восстановления.

В ситуациях, когда вход в ОС осуществляется, необходимо воспользоваться штатной функцией удаления, раздел 2.3 Удаление системы защиты.

Если Windows не загружается, однако модуль загрузчика DL работает корректно, значит, нет поврежденных зон преобразования, и дальнейшее аварийное восстановление имеет смысл.

Общий порядок аварийного отключения, следующий:

1. Восстановление преобразованных областей жесткого диска (данный этап не выполняется, если диски не были преобразованы) (для Dallas Lock 8.0-C) и отключение **модуля загрузчика DL**.
2. Отключение модуля интерактивного входа и подмена системных файлов **Dallas Lock 8.0** (подмена библиотек **Dallas Lock 8.0** на библиотеки Windows) вручную или с помощью загрузочного диска восстановления.
3. Редактирование реестра вручную или с помощью специальной утилиты.

21.1 Обратное преобразование жесткого диска в аварийном режиме

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

Обратное преобразование областей жесткого диска в аварийном режиме выполняется, если диски были преобразованы. Обратное преобразование следует произвести с помощью **модуля загрузчика DL**. Если модуль загрузчика DL работает корректно, то есть возможность вызвать аварийное обратное преобразование дисков прямо из загрузчика.

Для этого необходимо ввести в поле авторизации загрузчика PIN-код администратора и выбрать действие **Аварийное восстановление** (рис. 401), нажав **F2**.

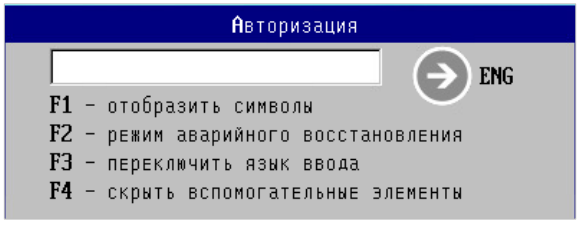


Рис. 401. Аварийное восстановление диска через загрузчик

Запустится процесс обратного преобразования, по завершении которого появится соответствующее сообщение.

Процесс аварийного восстановления жесткого диска используется в экстренных случаях и по времени является довольно длительным. Например, на физическом ПК под управлением ОС Windows 7 системный диск объемом 40 Гб аварийно восстанавливается 1 час 25 минут.

После завершения обратного преобразования областей дисков будет произведена попытка загрузки ОС. При сбое системы защиты **Dallas Lock 8.0** загрузка ОС станет невозможной, в этом случае необходимо произвести аварийное отключение системы защиты в ручном режиме или с помощью загрузочного диска, раздел 21.3 Аварийное отключение Dallas Lock 8.0 с помощью загрузочного диска.

21.2 Аварийное отключение загрузчика для ПК с UEFI-интерфейсом BIOS

Помимо стандартного BIOS модуль **загрузчика DL** поддерживается на ПК с материнскими платами, имеющими UEFI–интерфейс и GPT–разметку жесткого диска. Для данных ПК аварийное отключение загрузчика **Dallas Lock 8.0-C** имеет свои особенности.

Если включен **модуль загрузчика DL**, но нет возможности осуществить вход в загрузчике, то его можно отключить. Для этого необходимо выполнить следующие шаги:

1. Необходимо загрузиться с установочного диска Windows (или любого другого с доступом к командной строке и ФС) и получить доступ к командной строке, например, с помощью нажатия Shift+F10.
2. В командной строке необходимо ввести команду **«Diskpart»**. Откроется утилита (командный интерпретатор), позволяющая управлять объектами (дисками, разделами или томами).
3. Далее необходимо ввести команду **«List volume»**. Данная команда позволит отобразить список всех доступных объектов (разделов), определить их номер и букву. В списке нужно определить системный раздел, в котором хранится загрузчик. Это будет скрытый неименованный раздел размером ≈100 Мбайт. Необходимо определить, какой порядковый номер имеет данный раздел.
4. Далее необходимо ввести команду **«Select volume номер_раздела»**. На раздел с загрузчиком будет перемещен фокус.
5. Далее необходимо ввести команду **«Assign letter F»**. Для раздела с загрузчиком будет назначена буква диска (в данном примере — F).
6. Далее с помощью команды **«Exit»** необходимо выйти из утилиты. Командная строка вернется автоматически.
7. В командной строке необходимо перейти на раздел с загрузчиком с помощью команды **«Cd /d F:** (на раздел F в данном примере) или просто **«F: »**.
8. В выбранном разделе необходимо перейти в папку с загрузчиком с помощью команды **«Cd efi\microsoft\boot».**
9. Далее необходимо ввести следующие команды:
   - **«Rename bootmgfw.efi bootmgfw_dl.efi»**;
   - **«Rename bootmgfw_old.efi bootmgfw.efi»**.

   Данными командами файлы установленного загрузчика **Dallas Lock 8.0** («bootmgfw.efi») и стандартного загрузчика Windows («bootmgfw_dl.efi») переименовываются и меняются местами. Просмотреть содержимое папки, чтобы убедиться в наличии файлов загрузчика, можно с помощь команды **«dir: »**.
10. После этого необходимо перезагрузить компьютер и осуществить аварийное отключение системы защиты **Dallas Lock 8.0**. Если Загрузка ОС на защищенном ПК происходит корректно, то удаление **Dallas Lock 8.0** производится штатным образом с помощью Мастера установок Windows, раздел 2.3 Удаление системы защиты.



Следует иметь в виду, что если было произведено аварийное отключение загрузчика на ПК с UEFI-интерфейсом BIOS, то далее через оболочку администратора **Dallas Lock 8.0** производить отключение **модуля загрузчика DL** не нужно, так как один раз он был уже отключен вручную. Если же отключение загрузчика через оболочку администратора было выполнено, то необходимо повторно выполнить команду переименования файлов **«Rename bootmgfw_old.efi bootmgfw.efi»**.

11. После удаления **Dallas Lock 8.0** с помощью Мастера установок перед загрузкой ОС необходимо опять получить доступ к командной строке и переименовать файл загрузчика Windows, который был автоматически переименован уже в процессе удаления **Dallas Lock 8.0**:
    - **«Rename bootmgfw_old.efi bootmgfw.efi»**.
12. Если по каким-то причинам возможности загрузить ОС нет, то следует воспользоваться аварийным отключением системы защиты в ручном режиме или с помощью загрузочного диска (см. ниже).



Приоритет загрузки в UEFI–интерфейсе должен быть установлен у параметра **Загрузка Windows Boot Manager**.

21.3 Аварийное отключение Dallas Lock 8.0 с помощью загрузочного диска

После завершения восстановления преобразованных областей дисков (если такие были) необходимо загрузиться со специального диска восстановления **Dallas Lock 8.0**. Для получения данного диска необходимо обратиться к разработчику.

21.3.1 Отключение загрузчика и подмена системных файлов

Необходимо вставить компакт-диск для аварийного восстановления **Dallas Lock 8.0** в привод

и произвести загрузку с него (предварительно установив в BIOS загрузку с компакт-диска).

Если на диске есть преобразованные области, то при попытке загрузки диска восстановления появится сообщение о необходимости произвести предварительное восстановление зон преобразования. После вывода такого сообщения, нужно отправить компьютер в загрузку с жесткого диска (HDD) и руководствоваться предыдущим пунктом инструкции.

В появившемся меню загрузочного диска необходимо выбрать пункт **Аварийное отключение DL 8.0** (рис. 402).

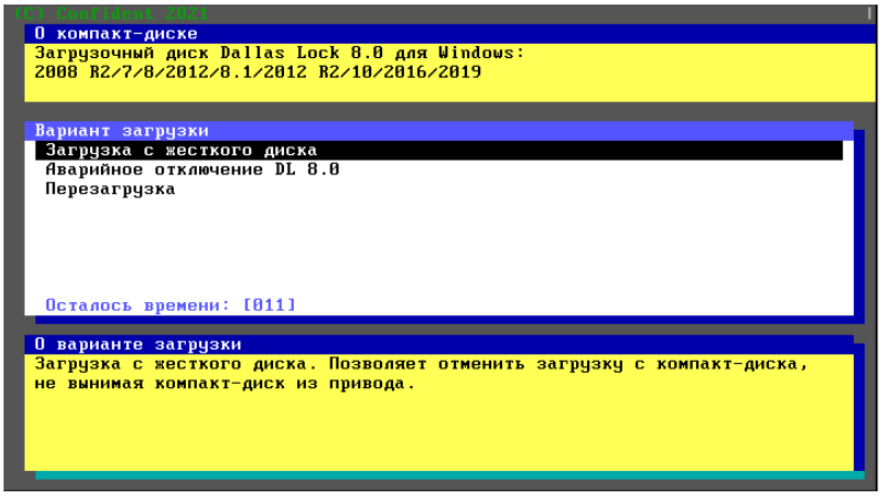


Рис. 402. Меню консоли диска восстановления

После загрузки в консоли аварийного восстановления будут предложены команды:

- **«DLOFF» —** аварийное отключение **Dallas Lock** в Windows;
- **«DLMBROFF» —** отключение загрузчика **Dallas Lock**;
- **«RESTART» —** перезагрузка;
- **«HELP» —** справка.

Если был активирован модуль загрузчика DL, то его необходимо отключить командой **«DLMBROFF»**. После этого система выведет сообщение о том, что в MBR установлен оригинальный загрузчик.

Далее необходимо отключить саму систему защиты **Dallas Lock 8.0** командой «**DLOFF»**. После этого система выведет сообщение о том, что система защиты аварийно отключена.

Затем необходимо ввести команду **«RESTART»** для перезагрузки компьютера. После перезагрузки система защиты **Dallas Lock 8.0** будет отключена.

21.3.2 Очистка реестра

Далее для корректного отключения системы защиты необходимо внести изменения в реестр. Сделать это вручную можно способом, описанным в предыдущем разделе, или с помощью специальной утилиты по очистке реестра **«DlRestoreSystem»**, которая находится на диске аварийного восстановления в директории **«util».**

Необходимо войти в ОС под учетной записью администратора Windows и запустить файл «DlRestoreSystem.exe» с диска (рис. 403).

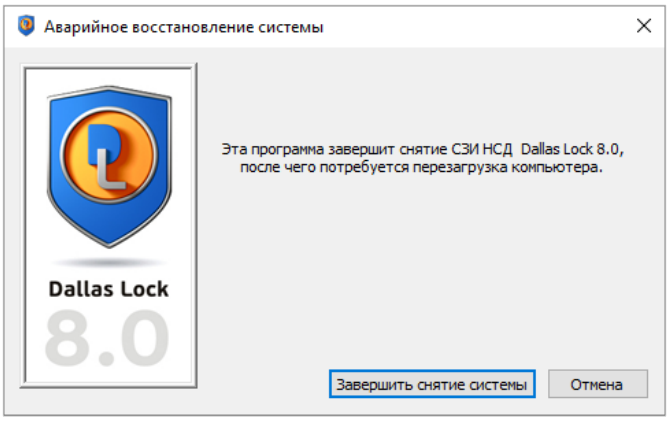


Рис. 403. Запуск утилиты по очистке реестра

После запуска данной утилиты с правами администратора и команды завершения снятия **СЗИ** будет предложено перезагрузиться. Также в процессе снятия системы защиты будет предложено оставить или удалить системную папку «DLLOCK80» с хранящимися в ней журналами и другими конфигурационными файлами.

После перезагрузки система защиты **Dallas Lock 8.0** будет удалена с компьютера, и можно будет снова запустить ее установку.

Если по каким-либо причинам данный способ аварийного восстановления не сработал, то необходимо воспользоваться аварийным восстановлением в ручном режиме, описанном в следующем разделе.

Перед выполнением очистки реестра необходимо отключить антивирус. В противном случае работа утилиты может быть заблокирована.

21.4 Аварийное отключение Dallas Lock 8.0 в ручном режиме

21.4.1 Порядок аварийного отключения для Windows

1. **Для аварийного отключения системы защиты Dallas Lock 8.0 в ОС Windows необходимо получить доступ к ФС.**

   Для этого можно воспользоваться, в том числе, платформой восстановления Windows Recovery Environment (WinRE), которая является «преемником» консоли восстановления для предыдущих версий ОС.

   WinRE может быть загружена с установочного диска ОС. Но можно воспользоваться встроенным инструментом восстановления, не требующим загрузки с компакт-диска. Для этого необходимо запустить меню дополнительных вариантов загрузки (перед началом загрузки ОС нажать **F8** на клавиатуре) (рис. 404).

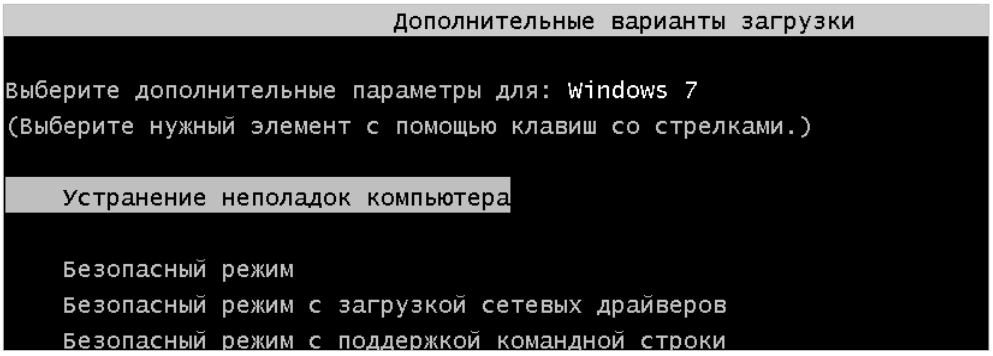


Рис. 404. Меню дополнительных вариантов загрузки ОС Windows 7

   Необходимо выбрать пункт *Устранение неполадок компьютера* (Repair Your Computer). Windows загрузит необходимые файлы и запустит процесс восстановления. Система попросит выбрать язык и ввести авторизационные данные. Появится необходимое окно параметров восстановления системы. В нем следует выбрать открытие окна командной строки.

   С помощью командной строки необходимо переключиться на диск (раздел жесткого диска), где установлена система защиты **Dallas Lock 8.0**. Следует учесть, что буква того диска, который

определен консолью восстановления как диск с установленной системой защиты, может не совпадать с буквой диска назначенного ОС, на который система защиты была установлена (диск C) (рис. 405).

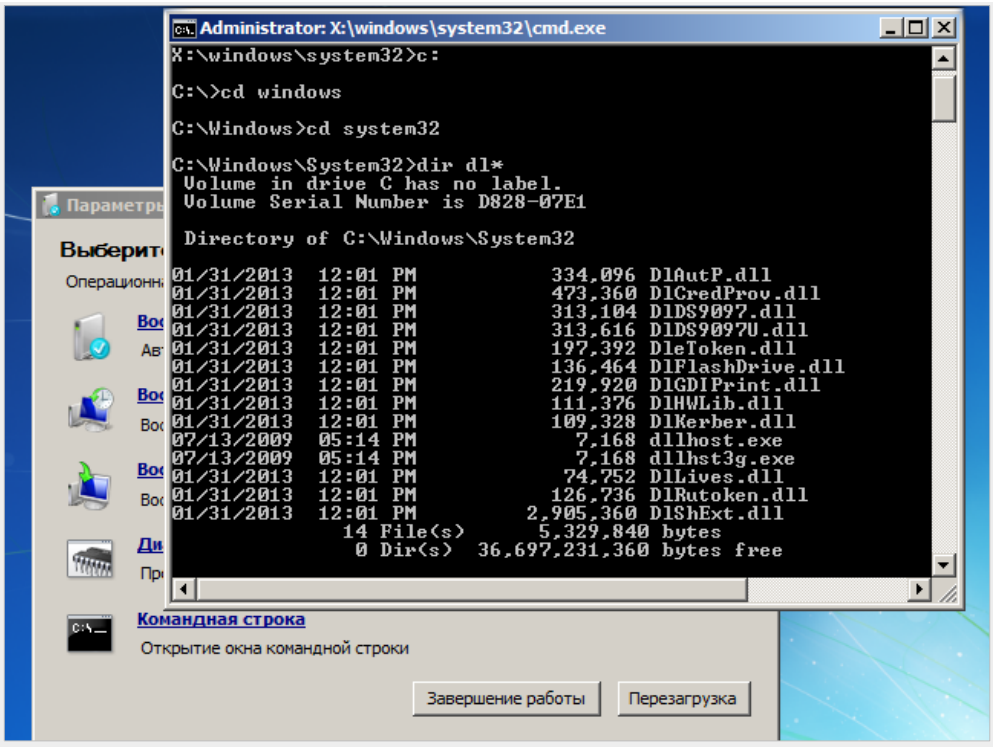


Рис. 405. Консоль восстановления системы в Windows 7 и список системных файлов

Следует учесть, что платформа восстановления WinRE имеется не на всех загрузочных дисках. Можно воспользоваться другими аварийно-восстановительными средствами получения прямого доступа к ФС в обход установленной ОС, например, Live CD Windows.

2. **После получения доступа к ФС необходимо подменить системные файлы.**

   После получения доступа к ФС необходимо зайти в папку System32 с помощью команды «cd %windir%\system32» и ввести следующие команды:

   - **«ren dlautp.dll dlautp_.dll»**;
   - **«copy msv1_0.dll dlautp.dll»**;
   - **«ren dlkerber.dll dlkerber_.dll»**;
   - **«copy kerberos.dll dlkerber.dll»**;
   - **«ren dllives.dll dllives_.dll»**;
   - **«copy livessp.dll dllives.dll»**[18];
   - **«ren dlcloud.dll dlcloud_.dll** (только для Windows 10)**»**;
   - **«copy cloudAP.dll dlcloud.dll** (только для Windows 10)**»**.

   Для отключения драйвера **МЭ** (при установленной версии с **МЭ** или **МЭ** и **СОВ**) необходимо выполнить команды **«cd %windir%\system32\drivers»**, **«ren dlfirewall.sys»** и **«dlfirewall_.sys»**.

3. **После подмены системных файлов необходимо очистить реестр.**

   После отключения модуля интерактивного входа для корректного отключения системы защиты необходимо внести изменения в реестр. Открыть редактор реестра можно с помощью командной строки командой **«regedit»** после ввода предыдущих команд. Можно открыть реестр из ОС, так как после подмены системных файлов компьютер должен успешно загрузиться (в поле ввода меню **Пуск** ввести команду **«regedit»**). В редакторе реестра следует проделать следующие операции:

4. Изменить значение на «*0*» параметра **Disabled** по пути:
   - для Windows 7/2008R2 «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}»;

[18] Отсутствие файлов «dllives.dll» и «livessp.dll» не является критичным.

5. Удалить ветки реестра «{9123E0C2-FF5E-4b38-BAB9-E2FA800D2548}» и «{9123E0C2-FF5E-4b38-BAB9-E2FA810E2649}» по пути
   «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers».
6. Полностью удалить из реестра следующие разделы:
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlDisk»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlFlt»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlHwCtrl»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dlfirewall»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlLwf»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlIPSService»;
   - «HKEY_CLASSES_ROOT\DaLoDisk»;
   - «HKEY_LOCAL_MACHINE\SOFTWARE\Classes\DaLoDisk».

   Актуально только для 32-х битных ОС Windows 7 и Windows Server 2008 R2:
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLCRYPT»;
   - «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DLFlt».

   Для удаления разделов из ветки «*Root*» необходимо изменить права доступа для текущего пользователя (это удобнее сделать не для каждого ключа, а для ветки «*Root*»).
7. Изменить значение ключа «*UpperFilters*» в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}» вместо «DlDisk PartMgr» следует оставить «PartMgr».
8. Необходимо удалить значение «*dlhwctrl*» для ключей в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\...» в тех разделах, в которых он имеется. Для этого можно воспользоваться автопоиском по ветке реестра (функция «Найти…» в контекстном меню и кнопка F3 для перехода к следующей записи).
9. Необходимо удалить значение «*DlDisk*» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E965-E325-11CE-BFC1-08002BE10318}».
10. Необходимо удалить значение «*DlDisk*» для ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E980-E325-11CE-BFC1-08002BE10318}».
11. Необходимо изменить значение ключа UpperFilters в ветке «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4D36E96B-E325-11CE-BFC1-08002BE10318}» вместо «*kbdclass DlFlt*» следует оставить «*kbdclass*».



При корректной загрузке ОС данные операции возможны и в режиме **Безопасный режим с поддержкой командной строки**. В этом случае потребуется дополнительная авторизация в ОС Windows с правами администратора.

После выполнения описанных операций необходимо перезагрузить компьютер. После перезагрузки система защиты будет отключена, теперь можно снова запустить ее установку либо воспользоваться функцией «Восстановить» в окне установки и удаления программ.



Для корректной установки **Dallas Lock 8.0** после ее аварийного отключения необходимо удостовериться в отсутствии приложения **BlockIcon**. Для этого нужно получить доступ в папку по пути «C:\Users\All users\Start Menu\Programs\Start Up» («C:\Documents snd Settings\All users\Start Menu\Programs\Start Up» или «C:\Documents and Settings\All Users\Главное меню\Программы\Автозагрузка»). Сделать это можно, например, с помощью командной строки. В случае наличия **BlockIcon** его необходимо удалить.

22 РЕЗЕРВНОЕ ВОССТАНОВЛЕНИЕ ДИСКА

НСД может привести не только к потере ценных данных, но и к выводу из строя ОС в процессе доступа к данным в обход **СЗИ**. Данный вид потери данных относится к человеческому фактору, но ОС может выйти из строя в результате воздействия вредоносных программ, стихийных или техногенных бедствий, или производственного брака. Чтобы иметь возможность быстро восстановить ОС можно создать образа диска.

Создание образа диска (image) — это процесс создания резервной копии раздела или всего жесткого диска, то есть резервное копирование Windows, настроек, драйверов, программ, данных пользователя.

Простой рабочей станции компании даже в течение часа может привести к крупным финансовым потерям. Восстановление системы из сохраненного образа диска занимает значительно меньше времени, чем установка заново ОС, программ, создание пользователей и выполнение настроек.

На сегодняшний день существует множество программ, позволяющих создавать образы дисков. В данном разделе будет рассмотрено восстановление с помощью программы **Acronis**. **Acronis** — это современная линейка сертифицированных корпоративных средств резервного копирования и восстановления.

Большинство программ по работе с жестким диском являются корпоративными, поэтому компания должна самостоятельно и своевременно их приобрести.

Рекомендуется сохранять образ диска до установки **Dallas Lock 8.0**. Не обязательно делать образ всего жесткого диска, достаточно сделать образ только системного диска с установленной ОС.

Если же необходимо сделать образ диска с установленной **Dallas Lock 8.0**, то необходимо сохранять образ всего жесткого диска, так как при установке **Dallas Lock 8.0** прописывается информация о **Dallas Lock** в загрузочную область жесткого диска (master boot record — MBR).

22.1 Создание загрузочного диска Acronis

Существует несколько версий **Acronis** для резервного копирования и аварийного восстановления рабочих станций, физических серверов, виртуальных машин, баз данных и т. д. Во всех версиях алгоритм создания образа примерно одинаковый.

Существуют автономные версии программы и расширенные версии с централизованным управлением. Версии с централизованным управлением предназначены для создания резервных копий для нескольких машин. Они включают в себя сервер управления, обеспечивающий централизованное управление, и узлы хранения резервных копий данных. В отличие от автономных версий расширенные версии обеспечивают удаленное подключение к ПК. В обоих случаях для каждой машины, для которой должна создаваться резервная копия, требуется отдельная лицензия.

Далее будет рассмотрено создание образа диска защищенной **Dallas Lock 8.0** автономной рабочей станции при помощи **Acronis Backup** & **Recovery 11 Workstation**. В разных версиях **Acronis** последовательность действий сохранения и восстановления образа диска может несколько отличаться.



Для корректного сохранения и восстановления образа диска с помощью программы Acronis необходимо выполнение следующих условий:

1. На диске не должно быть преобразованных областей жесткого диска 12.1 Прозрачное преобразование дисков.
2. Если включен модуль загрузчика DL, то в процессе резервного восстановления диска дополнительно необходимо отметить сохранение и восстановление MBR (или раздела с загрузчиком для материнских плат с интерфейсом UEFI).
3. Если восстановление образа диска происходит не на том ПК, с которого был снят образ, необходимо учесть, что разметка разделов диска должна быть одинаковой с тем ПК, с которого был снят образ.

Установка программы **Acronis** подробно описана в соответствующей документации, с которой можно ознакомиться на официальном сайте продукта[19]. После установки на локальный компьютер программа полностью готова к работе и не требует дополнительных настроек.

[19] https://www.acronis.ru/support/documentation/

В меню **Пуск** появляется пункт меню **Acronis**, который содержит значки компонентов **Acronis Backup & Recovery 11** (рис. 406):

- Консоль управления — инструмент для локальной работы с программой восстановления.
- Мастер создания загрузочного носителя для аварийного восстановления.

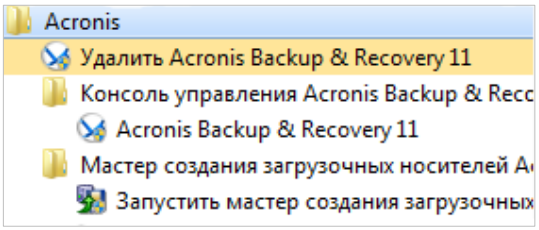


Рис. 406. Меню компонентов программы Acronis

Чтобы запустить программу, необходимо выбрать **Acronis Backup & Recovery 11**.

При первом запуске программа известит о необходимости создания загрузочного диска. Это действие можно отложить и запустить мастер создания загрузочных носителей позже. Созданный этой программой загрузочный носитель позволит в дальнейшем восстановить ОС компьютера, которую не удастся запустить, или работать с сохранением и восстановлением файлов на компьютере без установленной программы **Acronis** (рис. 407).

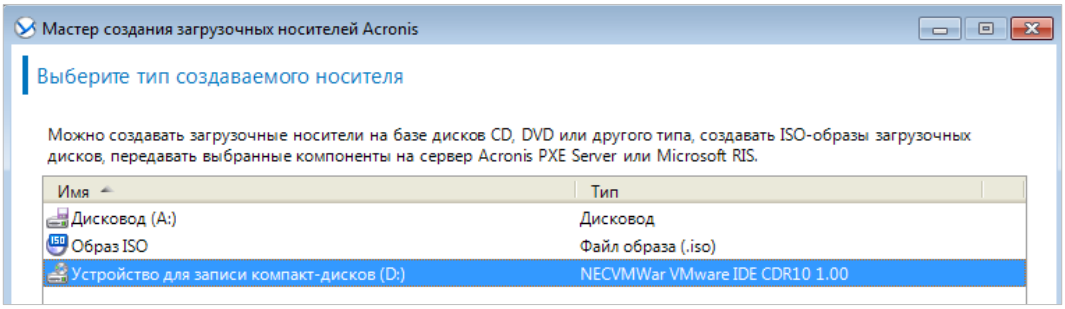


Рис. 407. Создание загрузочного носителя для восстановления

После выбора необходимых параметров и нажатия кнопки **Продолжить** загрузочный диск для восстановления будет записан (рис. 408).

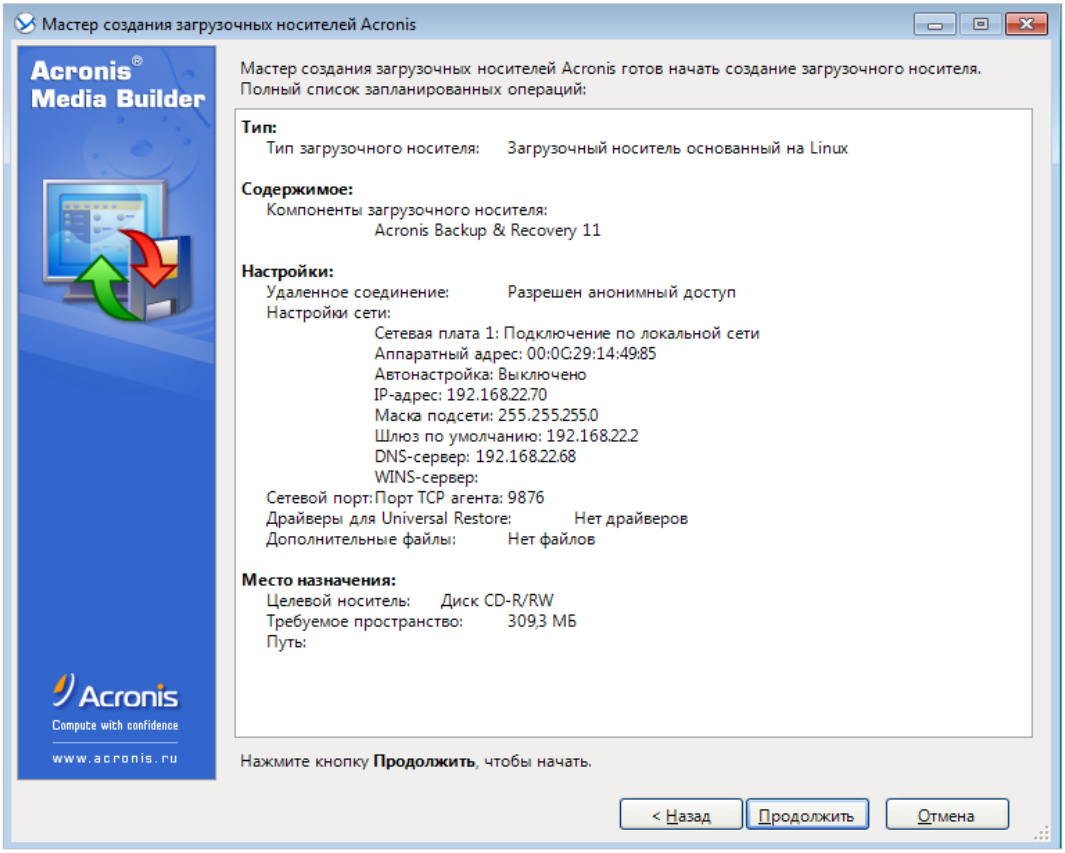


Рис. 408. Настройки мастера создания загрузочного носителя

При запуске **Acronis Backup & Recovery 11/11.5** на Windows 8/8.1 может возникать ошибка «*Error 1075 The dependency service does not exist or has be marked for deletion*». Для корректного продолжения работы программы необходимо удалить запись «*protected storage*» из ключа реестра Windows HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MMS\DependOnService и перезагрузить компьютер.

22.2 Сохранение образа диска с помощью Acronis

Чтобы сохранить сам образ диска, необходимо воспользоваться Консолью управления.

Данную консоль можно запустить, воспользовавшись пунктом меню, а можно — запустив компьютер с предварительно записанного загрузочного компакт-диска, настроив BIOS компьютера на загрузку с диска (рис. 409).

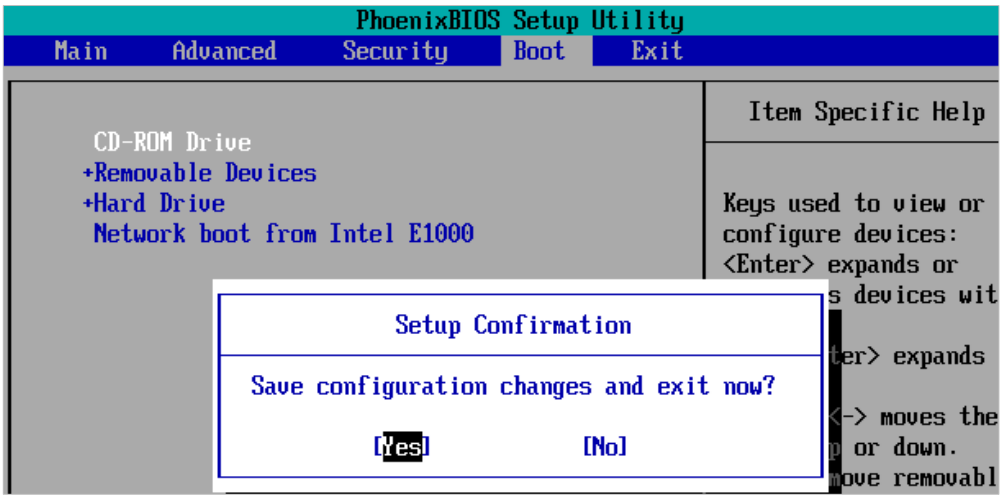


Рис. 409. Настройка BIOS компьютера для загрузки с диска

Следует учесть следующее. При запуске Консоли управления с защищенного **Dallas Lock 8.0** компьютера не с загрузочного диска, а через меню программ, необходимо зарегистрировать в системе защиты учетную запись для запуска служб **Acronis**.

После установки программы в ОС автоматически создаются учетные записи данных для служб **Acronis**. Для корректной работы программы учетную запись **Acronis** необходимо зарегистрировать еще и в **СЗИ** обычным созданием учетной записи и включить для нее свойство *Служебный пользователь*. В противном случае ОС выдаст сообщение: «*Служба Managed Machine Service Acronis недоступна*», и программа не сможет работать.

Зарегистрировать службу **Acronis** можно, выбрав ее из списка локальных учетных записей, воспользовавшись кнопкой поиска (рис. 410).

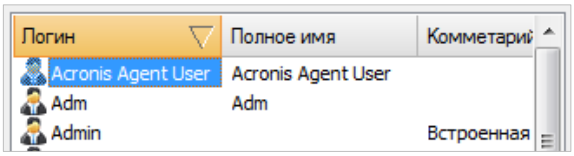


Рис. 410. Регистрация учетной записи службы Acronis в СЗИ

После регистрации учетной записи для службы необходимо перезагрузить компьютер. После этого на вкладке *Сессии* в списке появится сессия службы **Acronis** (рис. 411).

Пользователь запись	Источник	Тип входа	Время входа	Идентификатор сессии
Acronis Agent User		Служба	10.10.2012 16:07:52	0 116271
superadm		Локальный	10.10.2012 16:10:27	0 417921; 0 417994

Рис. 411. Сессия учетной записи службы Acronis

После этого консоль управления **Acronis** запустится корректно (рис. 412).

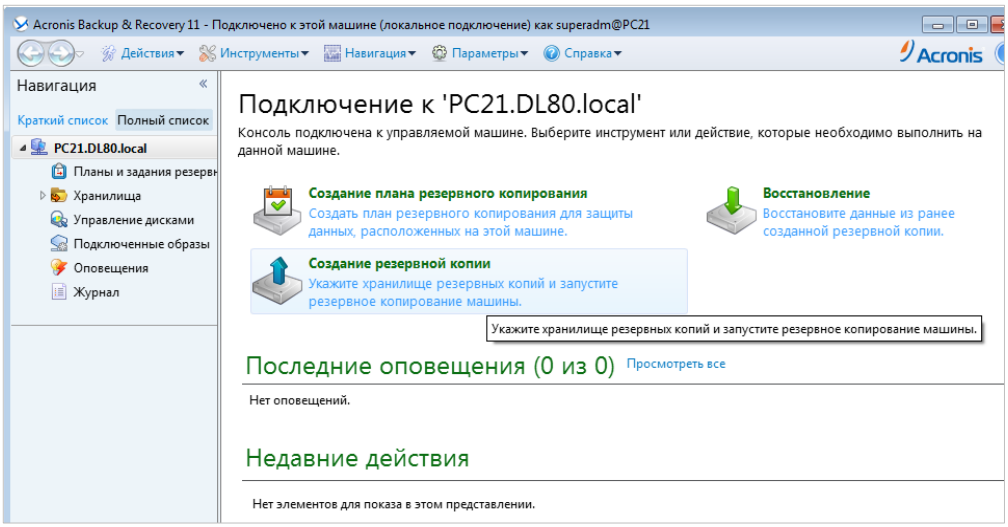


Рис. 412. Окно консоли управления Acronis

Окно программы состоит из дерева пунктов меню, основной области и верней строки меню. Дерево меню содержит следующие основные элементы:

- **Имя машины**, к которой в настоящий момент подключена консоль.
- Элемент для управления **планами и заданиями резервного копирования** на ПК: запуск, изменение, остановку и удаление планов и заданий резервного копирования, просмотра хода их выполнения.
- **Хранилища** — для управления индивидуальными хранилищами и архивами для создаваемых резервных копий и выполнения операций с ними.
- **Оповещения** — для просмотра предупреждающих сообщений.
- **Управление дисками** — для выполнения операций на жестких дисках машины.
- **Журнал** — для просмотра сведений об операциях, выполненных программой на управляемой машине.
- **Подключенные образы** — для управления подключенными образами.

Для того, чтобы создать и сохранить резервную копию диска, необходимо выбрать в основном окне программы соответствующий пункт **Создание резервной копии**. Появится окно выбора параметров для создания резервной копии (рис. 413).

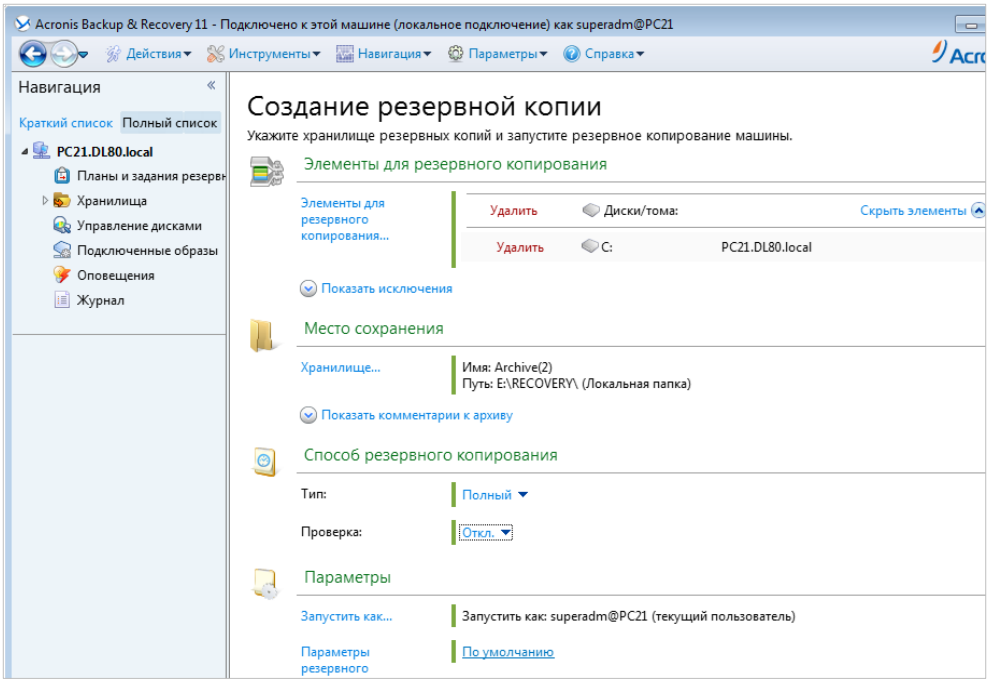


Рис. 413. Настройки создания резервной копии образа диска

В этом окне необходимо обязательно выбрать элемент для резервного копирования: весь жесткий диск или раздел, и место для сохранения резервной копии (рис. 414, рис. 415).

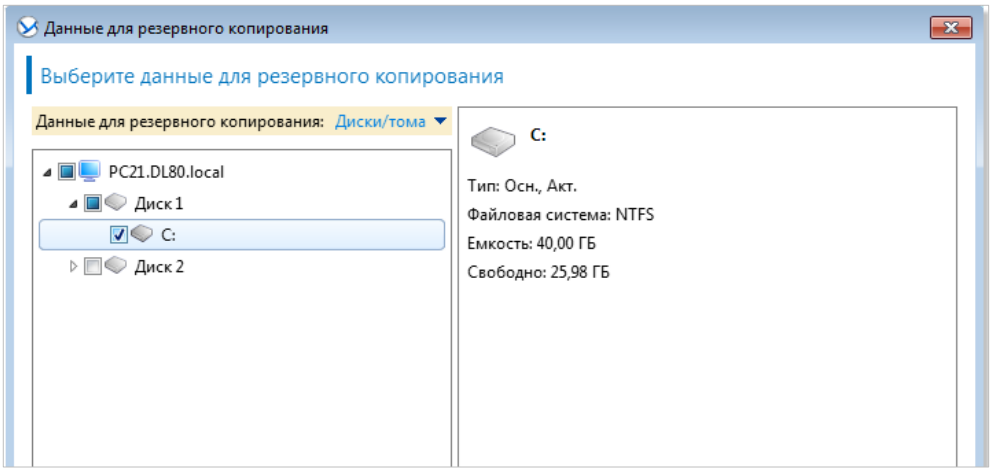


Рис. 414. Выбор диска для создания его образа

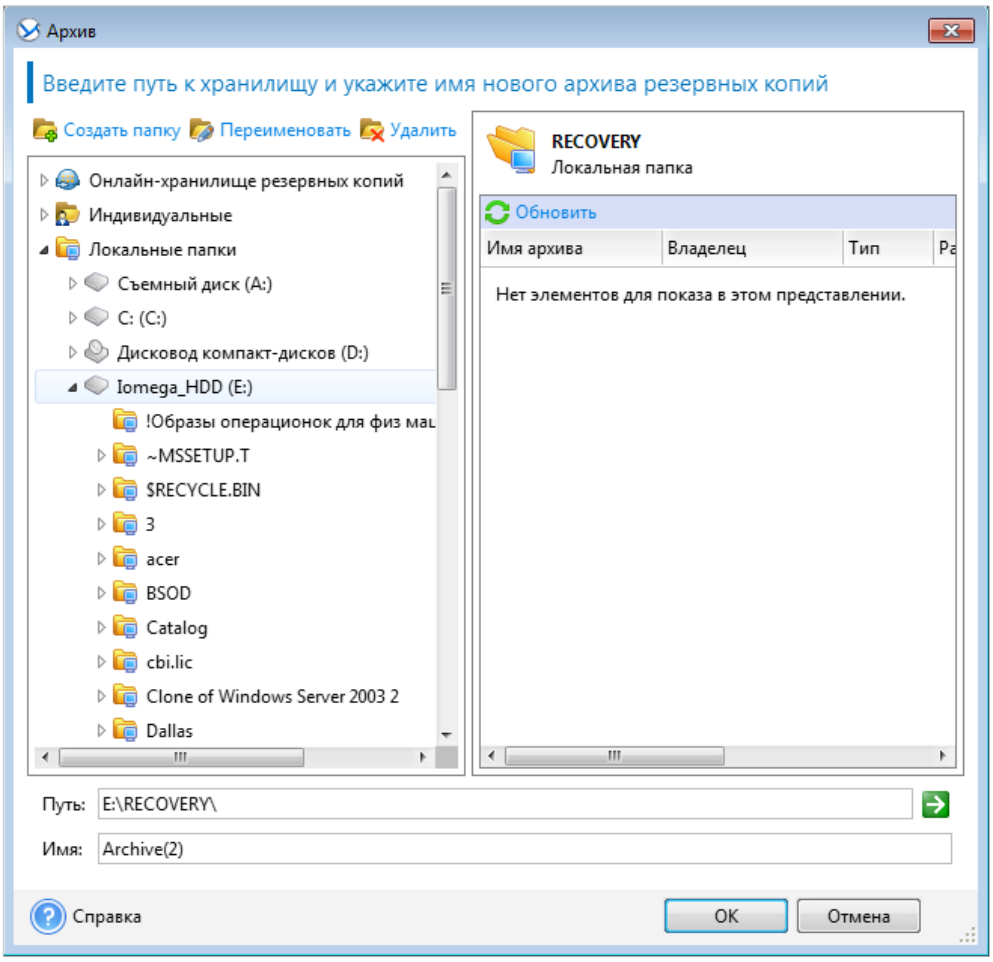


Рис. 415. Выбор хранилища для резервной копии образа диска

Параметры способов резервного копирования стоит оставить без изменения. После нажатия кнопки **OK** запустится процесс резервного копирования образа диска в выбранное хранилище (рис. 416).

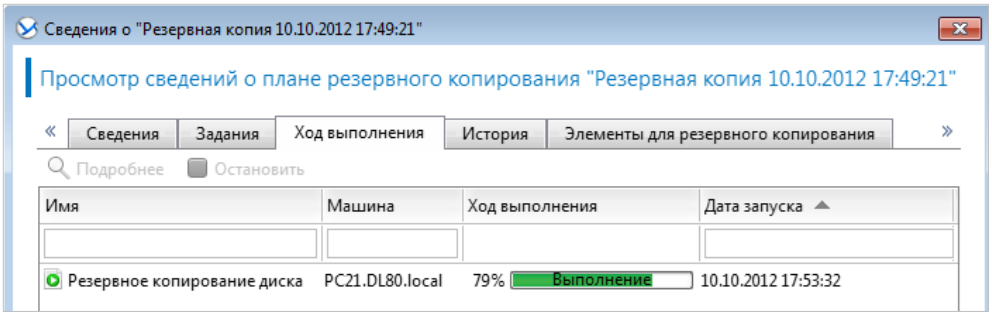


Рис. 416. Процесс создания резервной копии

После завершения создания образа появится соответствующее сообщение об успешном окончании операции.

22.3 Восстановление образа диска с помощью Acronis

При выходе из строя ОС компьютера, когда отсутствуют возможность ее загрузки, можно воспользоваться восстановлением образа диска с данными с помощью его сохраненной копии программой **Acronis**. Для этого необходим загрузочный диск с консолью управления программы **Acronis Backup & Recovery 11**, с которого нужно запустить ПК, предварительно настроив для этого BIOS (рис. 417).

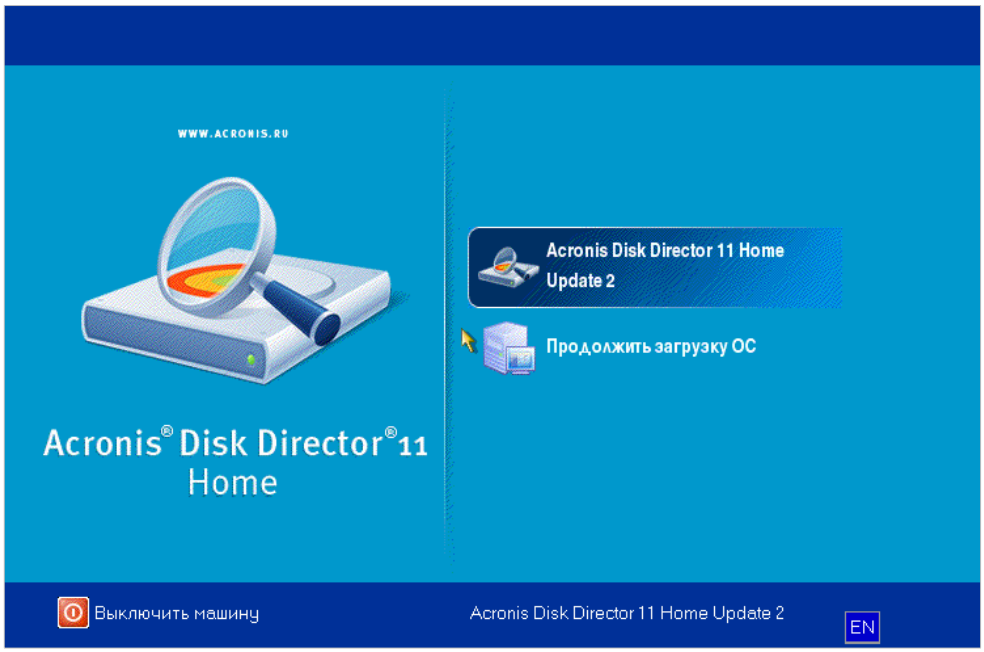


Рис. 417. Окно приветствия при загрузке с диска Acronis

После выбора в окне приветствия загрузку программы **Acronis** появится окно описанной выше Консоли управления **Acronis**, в которой необходимо выбрать пункт **Восстановление** (рис. 418).

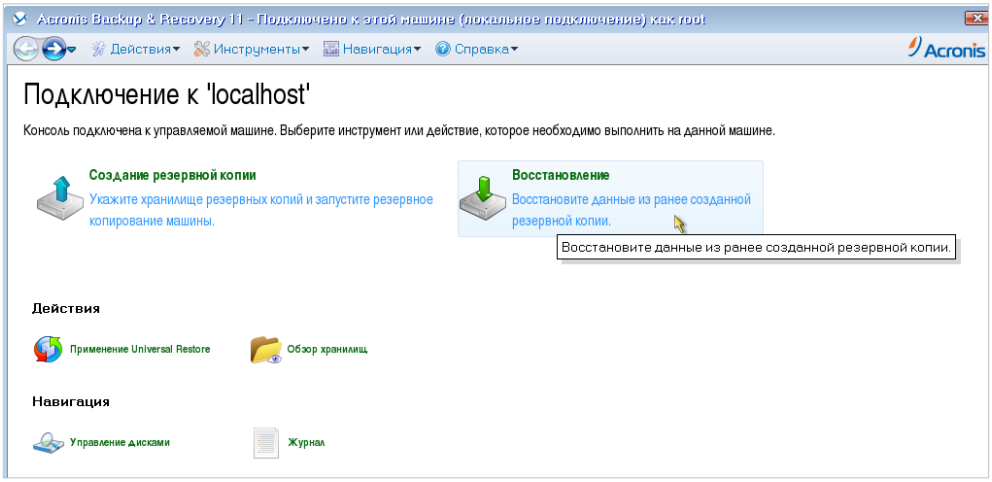


Рис. 418. Выбор пункта восстановления в консоли управления Acronis

В параметрах восстановления необходимо указать хранилище сохраненного образа, предварительно подключив его, если это съемный носитель (рис. 419, рис. 420).

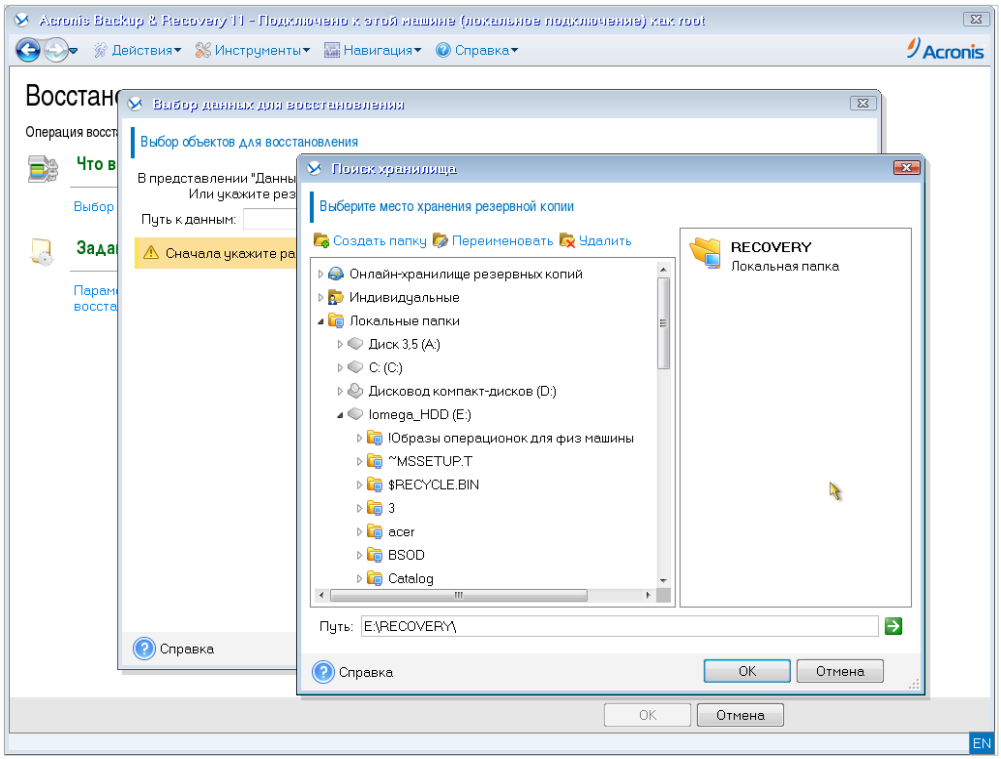


Рис. 419. Выбор хранилища созданной резервной копии для восстановления

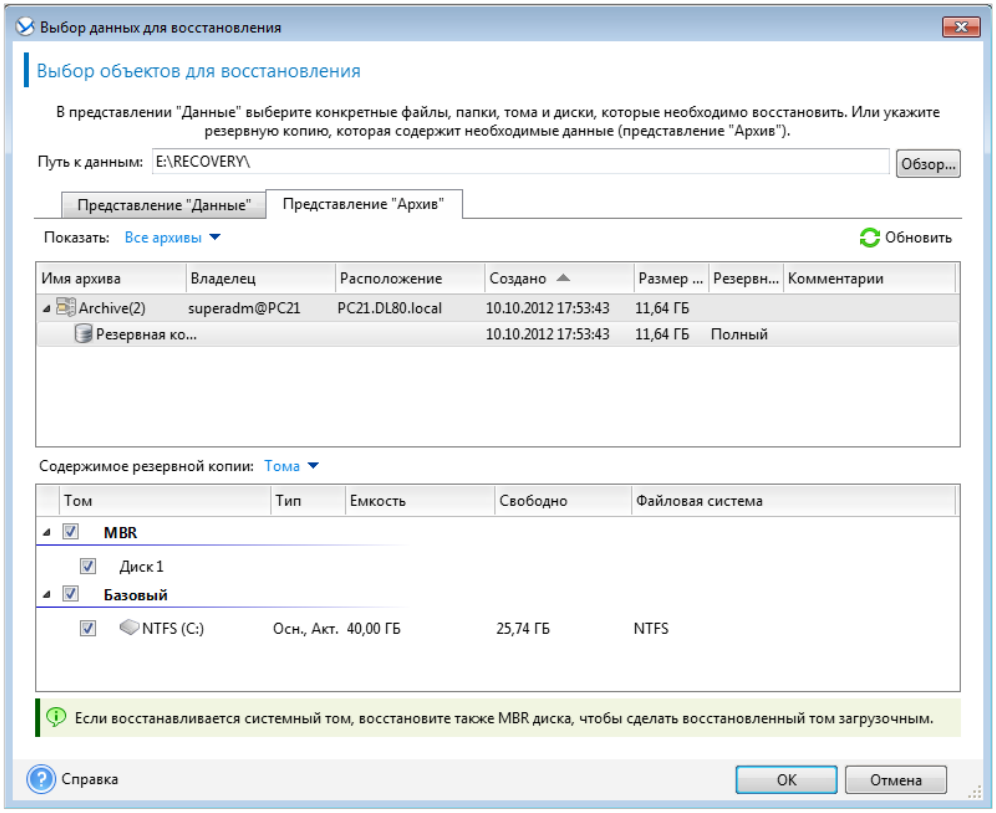


Рис. 420. Параметры восстановления резервной копии

Также необходимо указать место назначения, в которое будут восстановлены выбранные данные. Автоматически выбранные объекты восстановления будут восстановлены на физические диски ПК, так как **Acronis Backup & Recovery 11** автоматически сопоставляет образы дисков или томов с целевыми дисками, но при определенных настройках программы это можно сделать вручную.

После установки параметров и нажатия **OK** начнется процесс восстановления. По завершении которого потребуется перезагрузка компьютера и вход в восстановленную ОС (рис. 421).

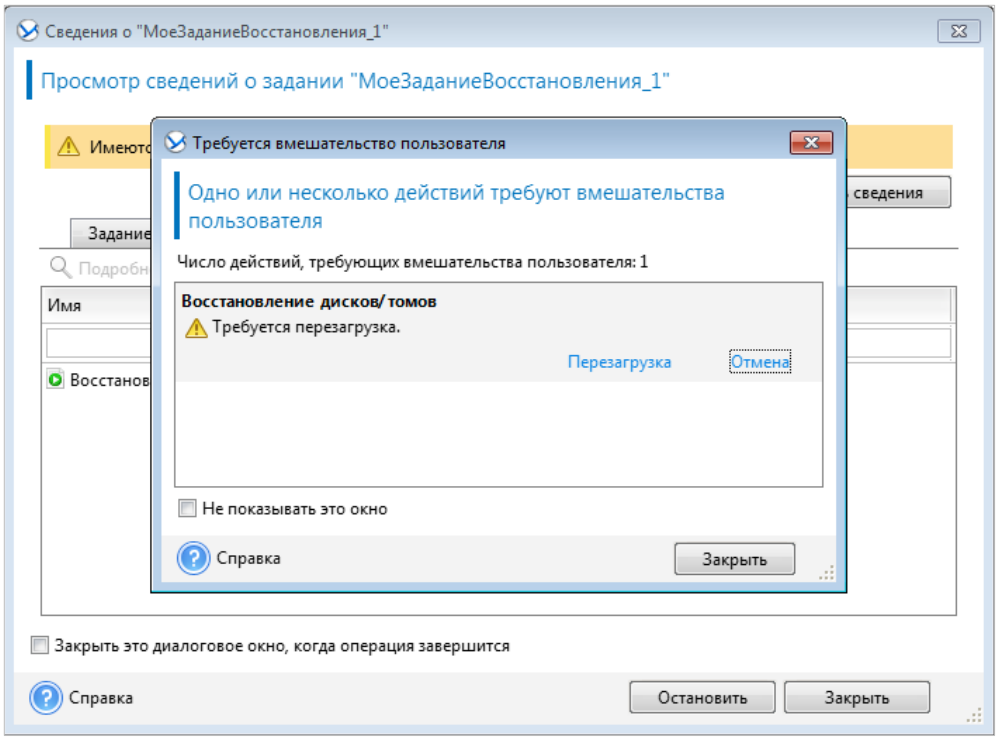


Рис. 421. Завершение процесса восстановления

Таким образом, данные жесткого диска ПК будут восстановлены. Следует учесть, что восстановление данных будет произведено с той версией системы **Dallas Lock 8.0** и теми настройками, которые были установлены при создании образа.

ПРИЛОЖЕНИЕ А
Предустановленные значения политик безопасности

А.1 Шаблоны автоматизированных систем

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Вкладка «Параметры безопасности» категория «Политики авторизации»			
Запретить смену пользователя без перезагрузки	1Б: Вкл. 1В, 1Г, 1Д: Выкл.	2А: Вкл. 2Б: Выкл.	АИБ
Отображать имя последнего вошедшего пользователя	Да	Да	Да
Максимальное количество ошибок ввода пароля	3	3	3
Время блокировки учетной записи в случае ввода неправильных паролей	15 мин.	15 мин.	15 мин.
Отображать информацию о последнем успешном входе	Нет	Нет	Нет
Разрешить использование смарт-карт	Нет	Нет	Нет
Запретить использование парольного интерфейса входа	Нет	Нет	Нет
Автоматический выбор аппаратного идентификатора при авторизации	Нет	Нет	Нет
Использовать авторизационной информацию с СДЗ Dallas Lock	Нет	Нет	Нет
Аппаратная идентификация	Выкл.	Выкл.	Выкл.
Текст сообщения при входе	Выкл.	Выкл.	Выкл.
Автоматическая загрузка ШОС	АИБ	АИБ	АИБ
Вкладка «Параметры безопасности» категория «Политики аудита»			
Журнал входов/выходов	Вкл.	Вкл.	Вкл.
Журнал ресурсов	Вкл.	Вкл.	Вкл.
Журнал управления политиками безопасности	Вкл.	Вкл.	Вкл.
Журнал управления пользователями и группами	Вкл.	Вкл.	Вкл.
Журнал печати	1Б, 1В, 1Г: Вкл. 1Д: Выкл.	2А: Вкл. 2Б: Выкл.	3А: Вкл. 3Б: Выкл.
Журнал запуска/завершения процессов	Вкл.	Вкл.	Вкл.
Служебный журнал МЭ (пакеты в формате Pcap)	Выкл.	Выкл.	Выкл.
Журнал пакетов МЭ	Выкл.	Выкл.	Выкл.
Журнал соединений МЭ	Выкл.	Выкл.	Выкл.
Журнал трафика фильтрации МЭ	Вкл.	Вкл.	Вкл.
Системный журнал	Вкл.	Вкл.	Вкл.
Журнал трафика	Вкл.	Вкл.	Вкл.
Журнал контроля приложений СОВ	Вкл.	Вкл.	Вкл.
Фиксировать в журнале неправильные пароли	1Б, 1В, 1Г: Да 1Д: Нет	Нет	Нет
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Нет	Нет	Нет
Заносить в журнал события	Да	Да	Да

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
запуска и остановки ОС			
Заносить в журнал события запуска и остановки модулей администрирования DL	Да	Да	Да
Аудит устройств	Вкл.	Вкл.	Вкл.
Аудит событий зачистки	Вкл.	Вкл.	Вкл.
Заносить в журналы ошибки ОС	Выкл.	Выкл.	Выкл.
Аудит системных пользователей	Выкл.	Выкл.	Выкл.
Печать/редактировать штамп	1Б, 1В: Да 1Г, 1Д: Нет	2А: Да 2Б: Нет	3А: Да 3Б: Нет
Создавать теневые копии распечатываемых документов	Нет	Нет	Нет
Выгрузка журналов	АИБ	Выкл	Выкл
Максимальное количество записей в журналах	10000	10000	10000
Периодическая архивация журналов	Выкл.	Выкл.	Выкл.
Вкладка «Параметры безопасности» категория «Политики паролей»			
Максимальный срок действия пароля	6 нед.	6 нед.	6 нед.
Минимальный срок действия пароля	Выкл.	Выкл.	Выкл.
Напоминать о смене пароля за	2 нед.	2 нед.	2 нед.
Минимальная длина пароля	1Б: 8 симв. 1В, 1Г, 1Д: 6 симв.	6 симв.	6 симв.
Необходимо наличие цифр	Да	Да	Да
Необходимо наличие спецсимволов	1Б: Да 1В, 1Г, 1Д: Нет	Нет	Нет
Необходимо наличие строчных и прописных букв	1Б: Да 1В, 1Г, 1Д: Нет	Нет	Нет
Необходимо отсутствие цифры в первом и последнем символах	Нет	Нет	Нет
Необходимо изменение пароля не меньше, чем в	Выкл.	Выкл.	Выкл.
Вкладка «Параметры безопасности» категория «Политики доступа»			
Блокировать компьютер при отключении аппаратного идентификатора	Нет	Нет	Нет
Блокировать файл-диски при отключении аппаратного идентификатора	Да	Да	Да
Вкладка «Параметры безопасности» категория «Сеть»			
Домен безопасности	Выкл.	Выкл.	Выкл.
Ключ защиты сетевого взаимодействия	Выкл.	Выкл.	Выкл.
Время хранения сетевого кэша	30 мин.	30 мин.	30 мин.
Список незащищенных серверов	Выкл.	Выкл.	Выкл.
Вкладка «Параметры безопасности» категория «Права пользователей»			
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации.			

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Вкладка «Параметры безопасности» категория «Мандатный доступ»			
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками.			
Вкладка «Параметры безопасности» категория «Очистка остаточной информации»			
Очищать освобождаемое дисковое пространство	1Б, 1В, 1Г: Да 1Д: Нет	2А: Да 2Б: Нет	3А: Да 3Б: Нет
Очищать файл подкачки виртуальной памяти	1Б, 1В, 1Г: Да 1Д: Нет	2А: Да 2Б: Нет	3А: Да 3Б: Нет
Очищать данные в конфиденциальных сеансах доступа	Да	Да	Да
Проверять очистку информации	Нет	Нет	Нет
Количество циклов затирания	1Б, 1В, 1Д: 2 1Г: 1	2	3А: 2 3Б: 1
Затирающая последовательность	00 00 00 00	00 00 00 00	00 00 00 00
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Политики»)			
Проверять целостность ФС при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль ФС	Не используется	Не используется	Не используется
Контроль ФС по расписанию	Выкл.	Выкл.	Выкл.
Проверять целостность прогр.апп.среды при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль прогр.апп.среды	3 ч.	3 ч.	3 ч.
Контроль прогр.апп.среды по расписанию	Выкл.	Выкл.	Выкл.
Проверять целостность реестра при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль реестра	Не используется	Не используется	Не используется
Контроль реестра по расписанию	Выкл.	Выкл.	Выкл.
Изменение файлов с назначенным контролем целостности	Разрешить	Разрешить	Разрешить
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Прогр.апп. среда»)			
Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно.			
Вкладка «Параметры безопасности» категория «Изолированные процессы»			
В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать / не изолировать. По умолчанию все процессы не изолированы.			
Вкладка «Параметры безопасности» категория «Загрузчик DL»			
Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютеру.			
Вкладка «Контроль ресурсов» категория «Дискреционный доступ»			
По умолчанию заданы следующие параметры: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports - C:\DLLOCK80\def_settings.reg - C:\DLLOCK80\zpsshell.ini			

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Параметры, заданные по умолчанию, рекомендуется оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Мандатный доступ»			
Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Аудит»			
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Контроль целостности»			
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Глобальные»			
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.			
Вкладка «Контроль ресурсов» категория «Устройства»			
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.			
Вкладка «МЭ» категория «Параметры»			
Доверенные правила МЭ	Вкл.	Вкл.	Вкл.
Отключать GZIP для анализа HTTP трафика	Вкл.	Вкл.	Вкл.
Сохранять локальные правила МЭ при синхронизации с Доменом безопасности	Да	Да	Да
Режим обучения МЭ	Выкл.	Выкл.	Выкл.
Протоколирование событий МЭ	Все события	Все события	Все события
Периодичность проверки защищенности системы	10 минут	10 минут	10 минут
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	Вкл.	Вкл.	Вкл.
Отключать локальные правила МЭ при автовыборе профиля МЭ	Да	Да	Да
Отображать сообщения о заблокированном соединении (сайте)	Нет	Нет	Нет
Межсетевой экран	Вкл.	Вкл.	Вкл.
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно.		
Вкладка «МЭ» категория «Правила МЭ»			
По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуется оставить в состоянии «Активировано».			
Вкладка «МЭ» категория «Профили МЭ»			
По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили.			
Вкладка «МЭ» категория «Фильтрация»			
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуется их оставить. Администратор информационной безопасности может самостоятельно дополнять список.		
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроме исключений».		
Включить фильтрацию	(АИБ)	(АИБ)	(АИБ)
Фильтрация SSL	(АИБ)	(АИБ)	(АИБ)
Максимальный размер http-заголовка	2048	2048	2048
Включить уведомление в	Вкл.	Вкл.	Вкл.

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
трей при блокировке соединения			
Использовать безопасный веб-серфинг	Нет	Нет	Нет
Блокировать протокол QUIC	Да	Да	Да
Вкладка «СОВ» категория «Сигнатуры»			
По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуется их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры журналов.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль приложений»)			
По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль реестра»)			
Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Настройки эвристики»)			
Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуется оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Глобальные параметры»)			
Анализ журналов ОС	Вкл.	Вкл.	Вкл.
Анализ сигнатур атак в сетевом трафике	Вкл.	Вкл.	Вкл.
Контроль приложений	Вкл.	Вкл.	Вкл.
Включить систему обнаружения вторжений	(АИБ)	(АИБ)	(АИБ)
Эвристика СОВ	Вкл.	Вкл.	Вкл.
Не заносить повторы в журнал контроля приложений	Вкл.	Вкл.	Вкл.
Блокировать снятие скриншотов по клавише PrintScreen	Выкл.	Выкл.	Выкл.
Расширенное определение атак подмены адресов	Выкл.	Выкл.	Выкл.
Маскирование датчика СОВ	Выкл.	Выкл.	Выкл.
Источник обновлений	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update
Регулярность обновлений	Раз в сутки	Раз в сутки	Раз в сутки
Заносить в журнал политик проверки наличия обновлений	Выкл.	Выкл.	Выкл.
Обновление сигнатур журналов	(АИБ)	(АИБ)	(АИБ)
Обновление детектора атак	(АИБ)	(АИБ)	(АИБ)
Обновление настроек эвристики	(АИБ)	(АИБ)	(АИБ)
Обновление сигнатур трафика	(АИБ)	(АИБ)	(АИБ)
Обновление переменных трафика	(АИБ)	(АИБ)	(АИБ)
Настройки оповещения контроля приложений	Выкл.	Выкл.	Выкл.
Настройки списков блокировок	Выкл.	Выкл.	Выкл.

Параметры	Классы защищенности АС / Значения параметров		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Защита от вирусов шифровальщиков	(АИБ)	(АИБ)	(АИБ)
Протоколирование событий СОВ	Все события	Все события	Все события
Блокировка отправки телеметрии Windows	Выкл.	Выкл.	Выкл.
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Настройки»)			
Безопасная среда	Вкл.	Вкл.	Вкл.
Возможность перенести изменения из БС в систему	Вкл.	Вкл.	Вкл.
Автоматическая очистка по завершении всех процессов	Вкл.	Вкл.	Вкл.
Эвристический анализ для блокировки опасных процессов	Выкл.	Выкл.	Выкл.
Порог срабатывания эвристики	100	100	100
Отчет по завершении работы процесса в БС	Выкл.	Выкл.	Выкл.
Автоматический запуск приложений в БС	Выкл.	Выкл.	Выкл.
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Контроль приложений»)			
Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила.			
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Файловая система и реестр»)			
Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать.			
Вкладка «СОР» категория «Параметры СОР»			
Источник обновлений	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update
Регулярность обновлений	(АИБ)	(АИБ)	(АИБ)
Заносить в журнал политик проверки наличия обновлений	Выкл.	Выкл.	Выкл.
Обновление базы индикаторов компрометации (IoC)	Вкл.	Вкл.	Вкл.
Расписание сканирования системы на индикаторы компрометации	(АИБ)	(АИБ)	(АИБ)
Область сканирования	(АИБ)	(АИБ)	(АИБ)
Сканирование новых файлов на индикаторы компрометации	(АИБ)	(АИБ)	(АИБ)
Правила автоматического реагирования	Вкл.	Вкл.	Вкл.

А.2 Шаблоны государственных информационных систем

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
Вкладка «Параметры безопасности» категория «Политики авторизации»			
Запретить смену пользователя без перезагрузки	Вкл.	Вкл.	Вкл.
Отображать имя последнего вошедшего пользователя	Да	Да	Да
Максимальное количество	3	3	3

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
ошибок ввода пароля			
Время блокировки учетной записи в случае ввода неправильных паролей	60 мин.	30 мин.	30 мин.
Отображать информацию о последнем успешном входе	Да	Да	Да
Разрешить использование смарт-карт	Нет	Нет	Нет
Запретить использование парольного интерфейса входа	Нет	Нет	Нет
Автоматический выбор аппаратного идентификатора при авторизации	Нет	Нет	Нет
Использовать авторизационной информацию с СДЗ Dallas Lock	Нет	Нет	Нет
Аппаратная идентификация	Выкл.	Выкл.	Выкл.
Текст сообщения при входе	Выкл.	Выкл.	Выкл.
Автоматическая загрузка ШОС	(АИБ)	(АИБ)	(АИБ)
Вкладка «Параметры безопасности» категория «Политики аудита»			
Журнал входов/выходов	Вкл.	Вкл.	Вкл.
Журнал ресурсов	Вкл.	Вкл.	Вкл.
Журнал управления политиками безопасности	Вкл.	Вкл.	Вкл.
Журнал управления пользователями и группами	Вкл.	Вкл.	Вкл.
Журнал печати	Выкл.	Выкл.	Выкл.
Журнал запуска/завершения процессов	Вкл.	Вкл.	Вкл.
Служебный журнал МЭ (пакеты в формате Pcap)	Выкл.	Выкл.	Выкл.
Журнал пакетов МЭ	Выкл.	Выкл.	Выкл.
Журнал соединений МЭ	Выкл.	Выкл.	Выкл.
Журнал трафика фильтрации МЭ	Вкл.	Вкл.	Вкл.
Системный журнал	Вкл.	Вкл.	Вкл.
Журнал трафика	Вкл.	Вкл.	Вкл.
Журнал контроля приложений СОВ	Вкл.	Вкл.	Вкл.
Фиксировать в журнале неправильные пароли	Выкл.	Выкл.	Выкл.
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Да	Да	Да
Заносить в журнал события запуска и остановки ОС	Да	Да	Да
Заносить в журнал события запуска и остановки модулей администрирования DL	Да	Да	Да
Аудит устройств	Вкл.	Вкл.	Вкл.
Аудит событий зачистки	Вкл.	Вкл.	Вкл.
Заносить в журналы ошибки ОС	Вкл.	Выкл.	Выкл.
Аудит системных пользователей	Вкл.	Вкл.	Вкл.
Печать/редактировать штамп	Нет	Нет	Нет
Создавать теневые копии распечатываемых	Нет	Нет	Нет

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
документов			
Выгрузка журналов	Выкл.	Выкл	Выкл
Максимальное количество записей в журналах	100000	100000	100000
Периодическая архивация журналов	Не используется	Не используется	Не используется
Вкладка «Параметры безопасности» категория «Политики паролей»			
Максимальный срок действия пароля	Не более 60 дн.	Не более 90 дн.	Не более 120 дн.
Минимальный срок действия пароля	От 1 до 30 дней	От 1 до 30 дней	От 1 до 30 дней
Напоминать о смене пароля за	14 дн.	14 дн.	14 дн.
Минимальная длина пароля	Не менее 8 симв.	Не менее 6 симв.	Не менее 6 симв.
Необходимо наличие цифр	Да	Да	Да
Необходимо наличие спецсимволов	Да	Да	Да
Необходимо наличие строчных и прописных букв	Да	Да	Да
Необходимо отсутствие цифры в первом и последнем символах	Нет	Нет	Нет
Необходимо изменение пароля не меньше, чем в	От 1 до 10 симв.	От 1 до 10 симв.	От 1 до 10 симв.
Вкладка «Параметры безопасности» категория «Политики доступа»			
Блокировать компьютер при отключении аппаратного идентификатора	Нет	Нет	Нет
Блокировать файл-диски при отключении аппаратного идентификатора	Да	Да	Да
Вкладка «Параметры безопасности» категория «Сеть»			
Домен безопасности	Выкл.	Выкл.	Выкл.
Ключ защиты сетевого взаимодействия	Выкл.	Выкл.	Выкл.
Время хранения сетевого кэша	30 мин.	30 мин.	30 мин.
Список незащищенных серверов	Выкл.	Выкл.	Выкл.
Вкладка «Параметры безопасности» категория «Права пользователей»			
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации.			
Вкладка «Параметры безопасности» категория «Мандатный доступ»			
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками.			
Вкладка «Параметры безопасности» категория «Очистка остаточной информации»			
Очищать освобождаемое дисковое пространство	Да	Да	Да
Очищать файл подкачки виртуальной памяти	Да	Да	Да
Очищать данные в конфиденциальных сеансах доступа	Да	Да	Да
Проверять очистку информации	Нет	Нет	Нет
Количество циклов затирания	От 1	От 1	От 1
Затирающая	00 00 00 00	00 00 00 00	00 00 00 00

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
последовательность			
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Политики»)			
Проверять целостность ФС при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль ФС	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Контроль ФС по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность прогр.апп.среды при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль прогр.апп.среды	3 ч.	3 ч.	3 ч.
Контроль прогр.апп.среды по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность реестра при загрузке ОС	Вкл.	Вкл.	Вкл.
Периодический контроль реестра	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Контроль реестра по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Изменение файлов с назначенным контролем целостности	Разрешить	Разрешить	Разрешить
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Прогр.апп. среда»)			
Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно.			
Вкладка «Параметры безопасности» категория «Изолированные процессы»			
В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать / не изолировать. По умолчанию все процессы не изолированы.			
Вкладка «Параметры безопасности» категория «Загрузчик DL»			
Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютеру.			
Вкладка «Контроль ресурсов» категория «Дискреционный доступ»			
По умолчанию заданы следующие параметры: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports - C:\DLLOCK80\def_settings.reg - C:\DLLOCK80\zpsshell.ini Параметры, заданные по умолчанию, рекомендуется оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Мандатный доступ»			
Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Аудит»			
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
Вкладка «Контроль ресурсов» категория «Контроль целостности»			
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.			
Вкладка «Контроль ресурсов» категория «Глобальные»			
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.			
Вкладка «Контроль ресурсов» категория «Устройства»			
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.			
Вкладка «МЭ» категория «Параметры»			
Доверенные правила МЭ	Вкл.	Вкл.	Вкл.
Отключать GZIP для анализа HTTP трафика	Вкл.	Вкл.	Вкл.
Сохранять локальные правила МЭ при синхронизации с Доменом безопасности	Да	Да	Да
Режим обучения МЭ	Выкл.	Выкл.	Выкл.
Протоколирование событий МЭ	Все события	Все события	Все события
Периодичность проверки защищенности системы	10 минут	10 минут	10 минут
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	Вкл.	Вкл.	Вкл.
Отключать локальные правила МЭ при автовыборе профиля МЭ	Да	Да	Да
Отображать сообщения о заблокированном соединении (сайте)	Нет	Нет	Нет
Межсетевой экран	Вкл.	Вкл.	Вкл.
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно.		
Вкладка «МЭ» категория «Правила МЭ»			
По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуется оставить в состоянии «Активировано».			
Вкладка «МЭ» категория «Профили МЭ»			
По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили.			
Вкладка «МЭ» категория «Фильтрация»			
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуется их оставить. Администратор информационной безопасности может самостоятельно дополнять список.		
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроме исключений».		
Включить фильтрацию	Вкл.	Вкл.	(АИБ)
Фильтрация SSL	Вкл.	Вкл.	(АИБ)
Максимальный размер http-заголовка	2048	2048	2048
Включить уведомление в трей при блокировке соединения	Вкл.	Вкл.	Вкл.
Использовать безопасный веб-серфинг	Нет	Нет	Нет
Блокировать протокол QUIC	Да	Да	Да
Вкладка «СОВ» категория «Сигнатуры»			
По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуется их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры			

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
журналов.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль приложений»)			
По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль реестра»)			
Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Настройки эвристики»)			
Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуется оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки.			
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Глобальные параметры»)			
Анализ журналов ОС	Вкл.	Вкл.	Вкл.
Анализ сигнатур атак в сетевом трафике	Вкл.	Вкл.	Вкл.
Включить систему обнаружения вторжений	Вкл.	Вкл.	(АИБ)
Контроль приложений	Вкл.	Вкл.	Вкл.
Эвристика СОВ	Вкл.	Вкл.	Вкл.
Не заносить повторы в журнал контроля приложений	Вкл.	Вкл.	Вкл.
Блокировать снятие скриншотов по клавише PrintScreen	Выкл.	Выкл.	Выкл.
Расширенное определение атак подмены адресов	Выкл.	Выкл.	Выкл.
Маскирование датчика СОВ	Выкл.	Выкл.	Выкл.
Источник обновлений	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update
Регулярность обновлений	Раз в сутки	Раз в сутки	Раз в сутки
Заносить в журнал политик проверки наличия обновлений	Выкл.	Выкл.	Выкл.
Обновление сигнатур журналов	Вкл.	Вкл.	(АИБ)
Обновление детектора атак	Вкл.	Вкл.	(АИБ)
Обновление настроек эвристики	Вкл.	Вкл.	(АИБ)
Обновление сигнатур трафика	Вкл.	Вкл.	(АИБ)
Обновление переменных трафика	Вкл.	Вкл.	(АИБ)
Настройки оповещения контроля приложений	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Настройки списков блокировок	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Защита от вирусов шифровальщиков	Вкл.	Вкл.	(АИБ)
Протоколирование событий СОВ	Все события	Все события	Все события
Блокировка отправки телеметрии Windows	Выкл.	Выкл.	Выкл.
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Настройки»)			

Параметры	Классы защищенности ГИС / Значения параметров		
	К1	К2	К3
Безопасная среда	Вкл.	Вкл.	Вкл.
Возможность перенести изменения из БС в систему	Вкл.	Вкл.	Вкл.
Автоматическая очистка по завершении всех процессов	Вкл.	Вкл.	Вкл.
Эвристический анализ для блокировки опасных процессов	Выкл.	Выкл.	Выкл.
Порог срабатывания эвристики	100	100	100
Отчет по завершении работы процесса в БС	Выкл.	Выкл.	Выкл.
Автоматический запуск приложений в БС	Выкл.	Выкл.	Выкл.
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Контроль приложений»)			
Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила.			
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Файловая система и реестр»)			
Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать.			
Вкладка «СОР» категория «Параметры СОР»			
Источник обновлений	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update
Регулярность обновлений	(АИБ)	(АИБ)	(АИБ)
Заносить в журнал политик проверки наличия обновлений	(АИБ)	(АИБ)	(АИБ)
Обновление базы индикаторов компрометации (IoC)	Вкл.	Вкл.	Вкл.
Расписание сканирования системы на индикаторы компрометации	(АИБ)	(АИБ)	(АИБ)
Область сканирования	(АИБ)	(АИБ)	(АИБ)
Сканирование новых файлов на индикаторы компрометации	(АИБ)	(АИБ)	(АИБ)
Правила автоматического реагирования	Вкл.	Вкл.	Вкл.

А.3 Шаблоны информационных систем персональных данных

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
Вкладка «Параметры безопасности» категория «Политики авторизации»				
Запретить смену пользователя без перезагрузки	Вкл.	Вкл.	Вкл.	Вкл.
Отображать имя последнего вошедшего пользователя	Да	Да	Да	Да
Максимальное количество ошибок ввода пароля	От 3 до 4	От 3 до 8	От 3 до 10	От 3 до 10
Время блокировки учетной записи в случае ввода неправильных паролей	От 15 до 60 мин.	ОТ 10 до 30 мин.	От 5 до 30 мин.	От 3 до 15 мин
Отображать	Да	Да	Да	Да

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
информацию о последнем успешном входе				
Разрешить использование смарт-карт	Нет	Нет	Нет	Нет
Запретить использование парольного интерфейса входа	Нет	Нет	Нет	Нет
Автоматический выбор аппаратного идентификатора при авторизации	Нет	Нет	Нет	Нет
Использовать авторизационной информацию с СДЗ Dallas Lock	Нет	Нет	Нет	Нет
Аппаратная идентификация	Нет	Нет	Нет	Нет
Текст сообщения при входе	Выкл.	Выкл.	Выкл.	Выкл.
Автоматическая загрузка ШОС	АИБ	АИБ	АИБ	АИБ
Вкладка «Параметры безопасности» категория «Политики аудита»				
Журнал входов/выходов	Вкл.	Вкл.	Вкл.	Вкл.
Журнал ресурсов	Вкл.	Вкл.	Вкл.	Вкл.
Журнал управления политиками безопасности	Вкл.	Вкл.	Вкл.	Вкл.
Журнал управления пользователями и группами	Вкл.	Вкл.	Вкл.	Вкл.
Журнал печати	Выкл.	Выкл.	Выкл.	Выкл.
Журнал запуска/завершения процессов	Вкл.	Вкл.	Вкл.	Вкл.
Служебный журнал МЭ (пакеты в формате Pcap)	Выкл.	Выкл.	Выкл.	Выкл.
Журнал пакетов МЭ	Выкл.	Выкл.	Выкл.	Выкл.
Журнал соединений МЭ	Выкл.	Выкл.	Выкл.	Выкл.
Журнал трафика фильтрации МЭ	Вкл.	Вкл.	Вкл.	Вкл.
Системный журнал	Вкл.	Вкл.	Вкл.	Вкл.
Журнал трафика	Вкл.	Вкл.	Вкл.	Вкл.
Журнал контроля приложений СОВ	Вкл.	Вкл.	Вкл.	Вкл.
Фиксировать в журнале неправильные пароли	Выкл.	Выкл.	Выкл.	Выкл.
Заносить в журнал исходящие попытки входа на удаленные компьютеры	Да	Да	Да	Да
Заносить в журнал события запуска и остановки ОС	Да	Да	Да	Да
Заносить в журнал события запуска и остановки модулей администрирования DL	Да	Да	Да	Да

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
Аудит устройств	Вкл.	Вкл.	Вкл.	Вкл.
Аудит событий зачистки	Вкл.	Вкл.	Вкл.	Вкл.
Заносить в журналы ошибки ОС	Вкл.	Выкл.	Выкл.	Выкл.
Аудит системных пользователей	Вкл.	Вкл.	Вкл.	Вкл.
Печать/редактировать штамп	Нет	Нет	Нет	Нет
Создавать теневые копии распечатываемых документов	Нет	Нет	Нет	Нет
Выгрузка журналов	Выкл.	Выкл.	Выкл.	Выкл.
Максимальное количество записей в журналах	10000	10000	10000	10000
Периодическая архивация журналов	Не менее 3 мес.	Не менее 3 мес.	Не менее 3 мес.	Не менее 3 мес.
Вкладка «Параметры безопасности» категория «Политики паролей»				
Максимальный срок действия пароля	Не более 60 дн.	Не более 90 дн.	Не более 120 дн.	Не более 180 дней
Минимальный срок действия пароля	От 1 до 30 дней	От 1 до 30 дней	От 1 до 30 дней	От 1 до 30 дней
Напоминать о смене пароля за	14 дн.	14 дн.	14 дн.	14 дн.
Минимальная длина пароля	Не менее 8 симв.	Не менее 6 симв.	Не менее 6 симв.	Не менее 6 симв.
Необходимо наличие цифр	Да	Да	Да	Да
Необходимо наличие спецсимволов	Да	Да	Да	Да
Необходимо наличие строчных и прописных букв	Да	Да	Да	Да
Необходимо отсутствие цифры в первом и последнем символах	Нет	Нет	Нет	Нет
Необходимо изменение пароля не меньше, чем в	От 1 до 10 симв.	От 1 до 10 симв.	От 1 до 10 симв.	От 1 до 10 симв.
Вкладка «Параметры безопасности» категория «Политики доступа»				
Блокировать компьютер при отключении аппаратного идентификатора	Нет	Нет	Нет	Нет
Блокировать файл-диски при отключении аппаратного идентификатора	Да	Да	Да	Да
Вкладка «Параметры безопасности» категория «Сеть»				
Домен безопасности	Выкл.	Выкл.	Выкл.	Выкл.
Ключ защиты сетевого взаимодействия	Выкл.	Выкл.	Выкл.	Выкл.
Время хранения сетевого кэша	30 мин.	30 мин.	30 мин.	30 мин.
Список незащищенных серверов	Выкл.	Выкл.	Выкл.	Выкл.
Вкладка «Параметры безопасности» категория «Права пользователей»				

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
Все значения параметров данной категории выставлены по умолчанию как рекомендуемые для выполнения, но могут быть настроены на усмотрение администратора безопасности, в соответствии с требованиями безопасности организации.				
Вкладка «Параметры безопасности» категория «Мандатный доступ»				
Категория «Мандатный доступ» доступна только для редакции «С», включает в состав подкатегорию «Уровни доступа» и «Мандатные метки». Предоставлено 7 уровней мандатного доступа (начиная с 0), АИБ может переименовывать название уровней и выполнять действия по управлению мандатными метками.				
Вкладка «Параметры безопасности» категория «Очистка остаточной информации»				
Очищать освобождаемое дисковое пространство	Да	Да	Да	Да
Очищать файл подкачки виртуальной памяти	Да	Да	Да	Да
Очищать данные в конфиденциальных сеансах доступа	Да	Да	Да	Да
Проверять очистку информации	Нет	Нет	Нет	Нет
Количество циклов затирания	От 1	От 1	От 1	От 1
Затирающая последовательность	00 00 00 00	00 00 00 00	00 00 00 00	-
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Политики»)				
Проверять целостность ФС при загрузке ОС	Вкл.	Вкл.	Вкл.	Вкл.
Периодический контроль ФС	Вкл.	Вкл.	Вкл.	Вкл.
Контроль ФС по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность прогр.апп.среды при загрузке ОС	Вкл.	Вкл.	Вкл.	Вкл.
Периодический контроль прогр.апп.среды	3 ч.	3 ч.	3 ч.	3 ч.
Контроль прогр.апп.среды по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Проверять целостность реестра при загрузке ОС	Вкл.	Вкл.	Вкл.	Вкл.
Периодический контроль реестра	Вкл.	Вкл.	Вкл.	Вкл.
Контроль реестра по расписанию	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ	Данный параметр можно включить или не использовать, определяется АИБ
Изменение файлов с назначенным контролем целостности	Разрешить	Разрешить	Разрешить	Разрешить
Вкладка «Параметры безопасности» категория «Политики контроля целостности» (Подкатегория «Прогр.апп. среда»)				
Для параметров данной категории выставлено значение «Выключено», необходимые значения выставляет администратор информационной безопасности самостоятельно.				
Вкладка «Параметры безопасности» категория «Изолированные процессы»				
В данной категории администратор информационной безопасности самостоятельно настраивает список процессов, которые необходимо изолировать / не изолировать. По умолчанию все процессы не изолированы.				

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
Вкладка «Параметры безопасности» категория «Загрузчик DL»				
Категория доступна только для редакции «С» и предназначена для включения и настройки режима загрузчика DL. Модуль загрузчика отрабатывает до загрузки ОС и выполняет роль дополнительного уровня защиты при попытке доступа к компьютеру.				
Вкладка «Контроль ресурсов» категория «Дискреционный доступ»				
По умолчанию заданы следующие параметры: - Параметры фиксированных дисков по умолчанию - C:\DLLOCK80\Logs - C:\DLLOCK80\Passports - C:\DLLOCK80\def_settings.reg - C:\DLLOCK80\zpsshell.ini Параметры, заданные по умолчанию, рекомендуется оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.				
Вкладка «Контроль ресурсов» категория «Мандатный доступ»				
Данная категория доступна только для редакции «С». Параметры данной категории настраиваются самостоятельно администратором информационной безопасности.				
Вкладка «Контроль ресурсов» категория «Аудит»				
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.				
Вкладка «Контроль ресурсов» категория «Контроль целостности»				
В данной категории по умолчанию уже добавлены имена и параметры файлов, рекомендуется их оставить. Остальные параметры данной категории настраиваются самостоятельно администратором информационной безопасности.				
Вкладка «Контроль ресурсов» категория «Глобальные»				
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.				
Вкладка «Контроль ресурсов» категория «Устройства»				
Параметры данной категории администратор информационной безопасности настраивает самостоятельно.				
Вкладка «МЭ» категория «Параметры»				
Доверенные правила МЭ	Вкл.	Вкл.	Вкл.	Вкл.
Отключать GZIP для анализа HTTP трафика	Вкл.	Вкл.	Вкл.	Вкл.
Сохранять локальные правила МЭ при синхронизации с Доменом безопасности	Да	Да	Да	Да
Режим обучения МЭ	Выкл.	Выкл.	Выкл.	Выкл.
Протоколирование событий МЭ	Все события	Все события	Все события	Все события
Периодичность проверки защищенности системы	10 минут	10 минут	10 минут	10 минут
Уведомления по событиям отсутствия антивируса и обновлений ОС и DL	Вкл.	Вкл.	Вкл.	Вкл.
Отключать локальные правила МЭ при автовыборе профиля МЭ	Да	Да	Да	Да
Отображать сообщения о заблокированном соединении (сайте)	Нет	Нет	Нет	Нет
Межсетевой экран	Вкл.	Вкл.	Вкл.	Вкл.
Порты сторонних программ	Необходимые значения администратор информационной безопасности устанавливает самостоятельно.			
Вкладка «МЭ» категория «Правила МЭ»				
По умолчанию в данную категорию уже добавлен набор правил. Все правила, кроме «Действия с пакетами, не попавшими ни под одно правило», деактивированы. Администратор информационной безопасности может				

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
самостоятельно добавить новое правило и активировать его, либо активировать правило по умолчанию. Правило «Действия с пакетами, не попавшими ни под одно правило» рекомендуется оставить в состоянии «Активировано».				
Вкладка «МЭ» категория «Профили МЭ»				
По умолчанию уже добавлен один профиль. Администратор информационной безопасности может самостоятельно настроить профиль по умолчанию или добавить собственные профили.				
Вкладка «МЭ» категория «Фильтрация»				
Список перехватываемых исходящих портов	По умолчанию добавлены порты: 80, 443, 3128, 8080, рекомендуется их оставить. Администратор информационной безопасности может самостоятельно дополнять список.			
Режим работы	По умолчанию выставлено значение «Фильтровать все, кроме исключений».			
Включить фильтрацию	Вкл.	Вкл.	(АИБ)	(АИБ)
Фильтрация SSL	Вкл.	Вкл.	(АИБ)	(АИБ)
Максимальный размер http- заголовка	2048	2048	2048	2048
Включить уведомление в трей при блокировке соединения	Вкл.	Вкл.	Вкл.	Вкл.
Использовать безопасный веб-серфинг	Нет	Нет	Нет	Нет
Блокировать протокол QUIC	Да	Да	Да	Да
Вкладка «СОВ» категория «Сигнатуры»				
По умолчанию в категорию уже добавлен набор сигнатур, все они находятся в состоянии «Активировано», рекомендуется их оставить. Администратор информационной безопасности может самостоятельно добавлять сигнатуры журналов.				
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль приложений»)				
По умолчанию в категорию добавлено три правила журнала приложений СОВ. Администратор информационной безопасности может самостоятельно добавить новые правила или редактировать правила по умолчанию.				
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Контроль реестра»)				
Данная категория уже содержит список ключей, находящихся в состоянии «Деактивировано». Администратор информационной безопасности может самостоятельно добавлять новые ключи или активировать ключи по умолчанию.				
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Настройки эвристики»)				
Данная категория уже содержит список атак и настройки эвристики для каждой из них. Рекомендуется оставить все атаки в состоянии «Вкл.» (реагирование на атаки). Администратор информационной безопасности может самостоятельно редактировать настройки эвристики для каждой атаки.				
Вкладка «СОВ» категория «Параметры СОВ» (подкатегория «Глобальные параметры»)				
Анализ журналов ОС	Вкл.	Вкл.	Вкл.	Вкл.
Анализ сигнатур атак в сетевом трафике	Вкл.	Вкл.	Вкл.	Вкл.
Контроль приложений	Вкл.	Вкл.	Вкл.	Вкл.
Эвристика СОВ	Вкл.	Вкл.	Вкл.	Вкл.
Не заносить повторы в журнал контроля приложений	Вкл.	Вкл.	Вкл.	Вкл.
Блокировать снятие скриншотов по клавише PrintScreen	Выкл.	Выкл.	Выкл.	Выкл.
Расширенное определение атак подмены адресов	Выкл.	Выкл.	Выкл.	Выкл.
Маскирование датчика СОВ	Выкл.	Выкл.	Выкл.	Выкл.
Источник обновлений	updates.dallaslock.ru/ Update	updates.dallaslock.ru/ Update	updates.dallaslock.ru/ Update	updates.dallaslock. ru/Update

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
Регулярность обновлений	Раз в сутки	Раз в сутки	Раз в сутки	Раз в сутки
Заносить в журнал политик проверки наличия обновлений	Выкл.	Выкл.	Выкл.	Выкл.
Обновление сигнатур журналов	Вкл.	Вкл.	Вкл.	Вкл.
Обновление детектора атак	Вкл.	Вкл.	Вкл.	Вкл.
Обновление настроек эвристики	Вкл.	Вкл.	Вкл.	Вкл.
Обновление сигнатур трафика	Вкл.	Вкл.	Вкл.	Вкл.
Обновление переменных трафика	Вкл.	Вкл.	Вкл.	Вкл.
Настройки оповещения контроля приложений	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Настройки списков блокировок	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ	Список настраивается АИБ
Защита от вирусов шифровальщиков	Вкл.	АИБ	АИБ	
Протоколирование событий СОВ	Все события	Все события	Все события	
Блокировка отправки телеметрии Windows	Выкл.	Выкл.	Выкл.	
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Настройки»)				
Безопасная среда	Вкл.	Вкл.	Вкл.	Вкл.
Возможность перенести изменения из БС в систему	Вкл.	Вкл.	Вкл.	Вкл.
Показывать диалог с сохранением изменений после завершения	Вкл.	Вкл.	Вкл.	Вкл.
Автоматическая очистка по завершении всех процессов	Вкл.	Вкл.	Вкл.	Вкл.
Эвристический анализ для блокировки опасных процессов	Выкл.	Выкл.	Выкл.	Выкл.
Порог срабатывания эвристики	100	100	100	100
Отчет по завершении работы процесса в БС	Выкл.	Выкл.	Выкл.	Выкл.
Автоматический запуск приложений в БС	Выкл.	Выкл.	Выкл.	Выкл.
Вкладка «СОВ» категория «Безопасная среда СОВ» (подкатегория «Контроль приложений»)				
Данная подкатегория уже содержит правило безопасной среды по умолчанию. Администратор информационной безопасности самостоятельно может настраивать дополнительные правила.				
Вкладка «СОВ» категория «Безопасная среда» (подкатегория «Файловая система и реестр»)				
Данная подкатегория уже содержит правило по умолчанию, администратор информационной безопасности может самостоятельно его редактировать.				
Вкладка «СОР» категория «Параметры СОР»				
Источник обновлений	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update	updates.dallaslock.ru/Update
Регулярность обновления	Вручную	Вручную	Вручную	Вручную
Заносить в журнал	(АИБ)	(АИБ)	(АИБ)	(АИБ)

Параметры	Уровни защищенности ИСПДн / Значения параметров			
	1	2	3	4
политик проверки наличия обновлений				
Обновление базы индикаторов компрометации (IoC)	Вкл.	Вкл.	Вкл.	Вкл.
Расписание сканирования системы на индикаторы компрометации	Вкл.	Вкл.	Вкл.	Вкл.
Область сканирования	(АИБ)	(АИБ)	(АИБ)	(АИБ)
Сканирование новых файлов на индикаторы компрометации	(АИБ)	(АИБ)	(АИБ)	(АИБ)
Правила автоматического реагирования	Вкл.	Вкл.	Вкл.	Вкл.