СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

РАБОТА С **РУТОКЕН ЭЦП 2.0 FLASH** В РАМКАХ СКН

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

компания АКТИВ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

DALLAS LOCK 8.0

ОГЛАВЛЕНИЕ

1. Преобразование сменных накопителей 1
2. Создание ключей преобразования 2
3. Процесс преобразования накопителя 3
4. Доступ к преобразованным накопителям 4
5. Преимущество использования 6
6. Централизованное управление СКН уровня отчуждения 7

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ

Размещаемая в данном документе информация предназначена для свободного ознакомления. Центр защиты информации ООО «Конфидент» оставляет за собой право вносить без уведомления любые изменения в данный документ, а также в ПО, которое описано в документе.

Используя информацию, изложенную в данном документе, вы выражаете своё согласие с «Отказом от ответственности».

В СЗИ Dallas Lock 8.0 в формате двух отдельных модулей реализована система контроля съемных машинных накопителей (СКН). Данные сертифицированные модули предназначены для контроля подключения съемных машинных носителей информации и контроля отчуждения (переноса) информации на такие носители. В данном документе описывается функциональность переноса информации на сменные накопители.Основные сценарии применения модуля СКН уровня отчуждения (переноса) информации:
1. Исключение утечек конфиденциальной информации через различные сменные накопители, подключаемые через USB-порт. Достигается за счёт запрета подключения на АРМ пользователей всех USB-накопителей за исключением специальным образом преобразованных накопителей Рутокен ЭЦП 2.0 Flash.
2. Безопасный перенос конфиденциальной информации между АРМ пользователей. Достигается за счёт отчуждения информации на преобразованные накопители Рутокен ЭЦП 2.0 Flash.

1. ПРЕОБРАЗОВАНИЕ СМЕННЫХ НАКОПИТЕЛЕЙ

1.1 В системе защиты Dallas Lock 8.0 реализована возможность преобразования сменных накопителей. Преобразование сменных накопителей используется, например, при передаче документов ограниченного доступа или конфиденциальной информации между автономными рабочими станциями. Данная функциональная возможность 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. При подключении к ПК такой накопитель отмечается в СЗИ таким образом, что вся информация на нем при ее обработке будет автоматически преобразована.

1.2 Преобразование сменных накопителей доступно для устройств, которые распознаются ОС как сменный/съемный (removable) (USB-Flash накопители, карты памяти, Floppy-диски и прочие).

1.3 Для функционирования модуля СКН с изделием поставляется специализированный съемный машинный носитель информации — Рутокен ЭЦП 2.0 Flash. Указанный носитель может иметь следующие объемы памяти: 4Гб, 8Гб, 32Гб, 64Гб. Для разных объемов памяти предустановленное на носителе ПО не отличается.

1.4 Указанный накопитель сертифицирован ФСТЭК в рамках сертификата СКН и рекомендуется к использованию в СЗИ для выполнения требований Методических документов «Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации четвертого класса защиты ИТ.СКН.Н4.ПЗ» (ФСТЭК России, 2014).

1.5 СЗИ не предоставляет возможность выбора областей и размера преобразовываемой области диска — производится полное преобразование накопителей.

1.6 Преобразование сменных накопителей осуществляется через оболочку администратора (рис. 1).

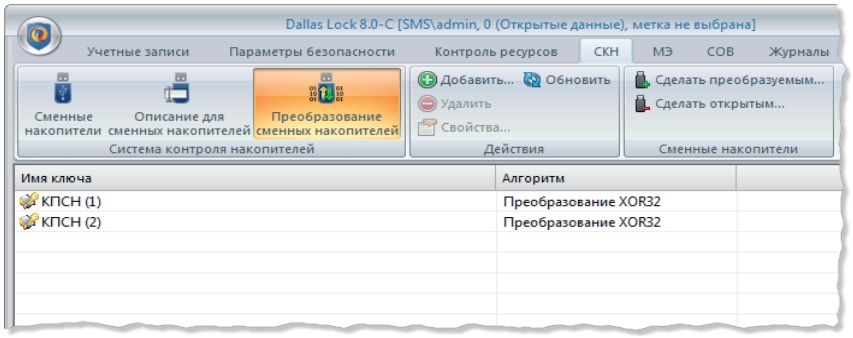

Рисунок 1 — Преобразование сменных накопителей

2. СОЗДАНИЕ КЛЮЧЕЙ ПРЕОБРАЗОВАНИЯ

2.1 Для создания преобразованных сменных накопителей необходимо наличие ключа преобразования. Окно ввода параметров ключа преобразования представлено на рис. 2.

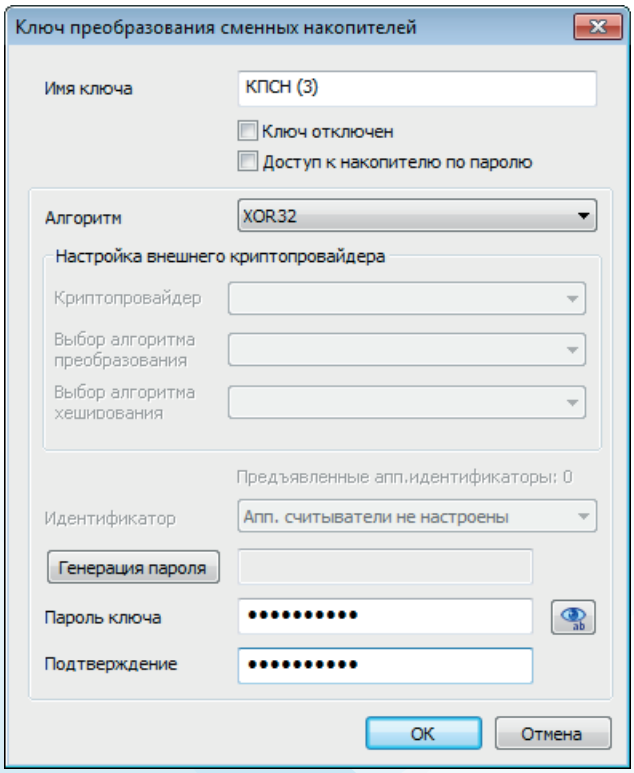

Рисунок 2 — Окно ввода параметров ключа преобразования

Параметры указаны в таблице 1.

Таблица 1

НАИМЕНОВАНИЕ ПОЛЯ	ОПИСАНИЕ
Имя ключа	Имя ключа предлагается по умолчанию «КПСН» — ключ преобразования сменных накопителей. Его можно изменить. Имя ключа должно быть уникальным, создание двух ключей с одинаковыми именами невозможно
Ключ отключен	Определяет активность ключа преобразования
Доступ к накопителю по паролю	Определяет необходимость предоставления пароля для доступа к накопителю. Функциональная возможность доступна в случае приобретения лицензии на модуль «Средство контроля съемных машинных носителей информации»
Алгоритм	Алгоритм преобразования
Идентификатор	Для назначения аппаратного идентификатора необходимо предварительно зарегистрировать идентификатор в СЗИ, предъявить и выбрать его из списка. При отсутствии аппаратного идентификатора преобразование происходит только по паролю
Пароль ключа и подтверждение	В качестве пароля может использоваться комбинация символов, удовлетворяющих установленным параметрам сложности паролей

Созданный ключ преобразования появится в списке. В отношении ключей преобразования доступны удаление, изменение параметров выбранного ключа, обновление всего списка ключей. Операции по преобразованию сменных накопителей и управлению списком ключей преобразования сменных накопителей фиксируются в журнале управления политиками.

3. ПРОЦЕСС ПРЕОБРАЗОВАНИЯ НАКОПИТЕЛЯ

Для преобразования[1] сменного накопителя необходимо:

1. Вставить накопитель в разъем.

2. Выбрать на панели действий со сменными накопителями «Сделать преобразуемым». Откроется окно параметров для преобразования (рис. 3).

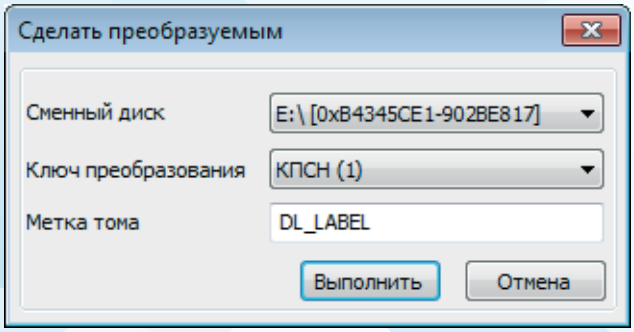

Рисунок 3 — Параметры для преобразования информации на выбранном диске

1- В процессе преобразования накопителя вся информация, расположенная на нем, будет утрачена, так как накопитель будет отформатирован.

3. В появившемся окне параметров преобразования:
- выбрать букву диска сменного накопителя, определенную ОС (если буква не определена, нужно перезапустить окно);
- выбрать ключ преобразования из списка созданных;
- ввести метку тома — произвольное имя будущего преобразованного накопителя.

4. Нажать «Выполнить» — запускается процесс форматирования диска, по окончании которого появится сообщение об успешности включения режима преобразования для диска E (рис. 4).

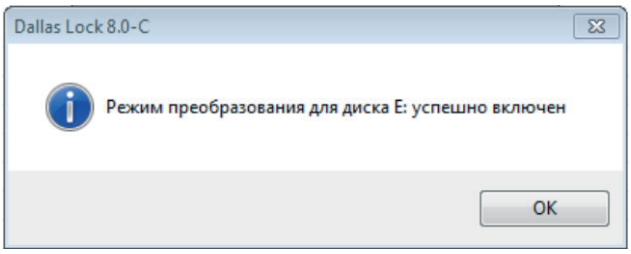

Рисунок 4 — Сообщение об успешном преобразовании накопителя

4. ДОСТУП К ПРЕОБРАЗОВАННЫМ НАКОПИТЕЛЯМ

4.1 После преобразования сменного накопителя работа с ним возможна только на компьютерах, которые защищены с помощью СЗИ 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.

4.2 В СЗИ есть возможность настройки доступа к съемному накопителю по паролю. Чтобы получить доступ к преобразованному сменному накопителю с установленным паролем, необходимо подключить данный накопитель к компьютеру. После подключения на экране появляется всплывающее уведомление (рис. 5) и окно для ввода пароля ключа преобразования (рис. 6).

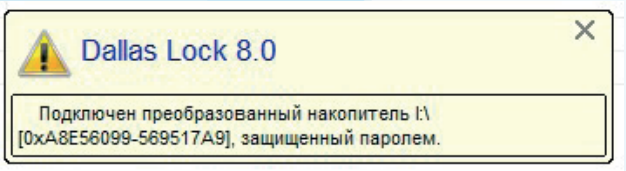

Рисунок 5 — Получение доступа к преобразованным съемным накопителям

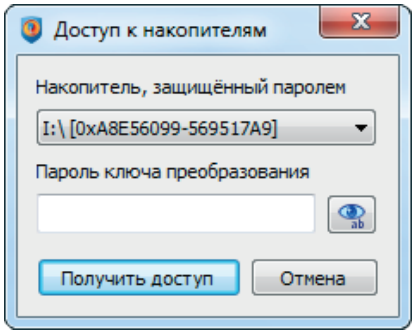

Рисунок 6 — Пароль ключа преобразования для доступа к преобразованным съемным накопителям

4.3 Также получение доступа к преобразованным накопителям возможно через панель задач. После выбора соответствующего пункта появится окно, в котором можно выбрать накопитель, к которому необходимо получить доступ, и ввести пароль ключа преобразования для него.

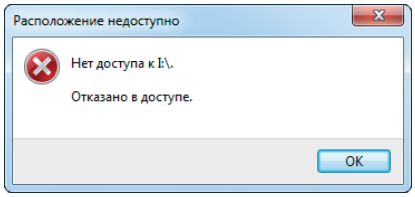

Рисунок 7 — Отказ доступа

4.4 При попытке открытия преобразованного съемного накопителя из проводника, возникает сообщение об отказе доступа (рис. 7).

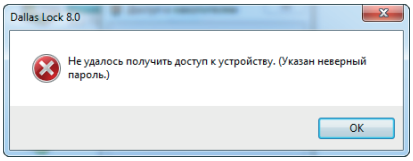

Рисунок 8 — Попытка доступа к устройству с неверным паролем

4.5 При вводе неверного пароля на экране появляется сообщение об ошибке (рис. 8).

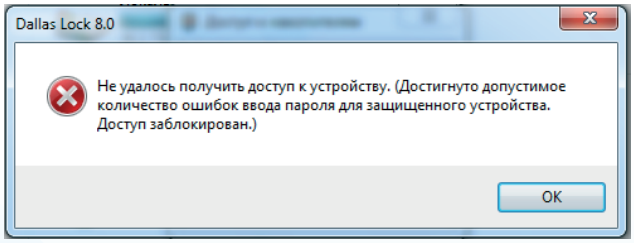

Рисунок 9 — Блокировка доступа к устройству

4.6 При превышении установленного допустимого количества неуспешных попыток аутентификации доступ к защищаемому устройству для данного пользователя блокируется. На экране появляется соответствующее сообщение (рис. 9), в «Журнале входов» регистрируются соответствующие события.

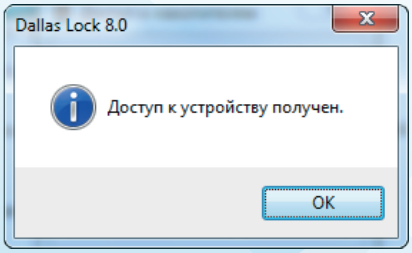

Рисунок 10 — Доступ к устройству

4.7 Блокировку доступа пользователя к защищенным накопителям снимает администратор.

4.8 При указании верного пароля для устройства пользователю предоставляется доступ. На экране появляется соответствующее сообщение (рис. 10).

4.9 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.

4.10 СЗИ предоставляет возможность настройки параметров доступа и аудита для преобразованных накопителей, а также возможность назначения теневого копирования информации с преобразованных накопителей.

5. ПРЕИМУЩЕСТВО ИСПОЛЬЗОВАНИЯ

5.1 При наличии соответствующей лицензии Dallas Lock 8.0 реализует функциональную возможность резервного копирования произвольных объектов. Модуль резервного копирования позволяет восстанавливать безвозвратно модифицированные или удаленные файлы, или каталоги (с поддержкой вложенных файлов). Управление резервным копированием может осуществляться как централизованно, с помощью Консоли Сервера безопасности Dallas Lock, так и локально с помощью оболочки администратора Dallas Lock 8.0.

5.2 В ходе настройки механизмов резервного копирования создаются задания на резервное копирование, определяющие периодичность создания резервных копий объектов ФС, их количество, длительность и место хранения. Задания на резервное копирование выполняются в фоновом режиме.

При этом возможность назначения прав доступа и контроля целостности на объекты, на которые установлено резервное копирование, отсутствует.

5.3 Сочетание механизмов преобразования сменных накопителей и резервного копирования обеспечивает возможность выполнения следующего сценария.

1. На сменном накопителе Рутокен ЭЦП 2.0 Flash размещена папка, в которой содержится объект файловой системы <объект1>, содержащий информацию, предназначенную для ограниченного круга лиц.

2. На <объект1> установлено резервное копирование.

3. На папку с указанным объектом файловой системы установлены права доступа.

4. Сменный накопитель преобразован в соответствии с разделом 3, установлен ключ преобразования.

При выполнении этого сценария работа с накопителем возможна только на компьютерах, которые защищены с помощью СЗИ Dallas Lock 8.0, и на которых установлен ключ преобразования, аналогичный тому, которым преобразование было выполнено.

Кроме того, доступ к папке, размещенной на сменном накопителе, будет строго ограничен в соответствии с установленными правами доступа.

Также стоит отметить, что установка резервного копирования на <объект1> позволяет восстановить его в случае безвозвратного удаления или модификации.

6. ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СКН УРОВНЯ ОТЧУЖДЕНИЯ

6.1 Управление ключами преобразования и работа с преобразованными сменными накопителями может осуществляться не только локально в оболочке администрирования СЗИ Dallas Lock 8.0, но и централизованно с помощью Консоли Сервера безопасности Dallas Lock (далее — КСБ) для всего домена безопасности, групп или отдельных клиентских АРМ.

6.2 Реализовано управление списком ключей преобразования для клиентских АРМ с помощью КСБ (Рис. 11), в рамках которого возможно:

1. создание ключей преобразования (имеет тот же механизм, что и в оболочке администратора СЗИ Dallas Lock 8.0);
2. индивидуальная настройка списка ключей преобразования для каждой группы и подгруппы клиентов, а также самих клиентов;
3. задание режима управления ключами преобразования: централизованного или локального:
   - централизованный режим управления (отмечено поле «Включить централизованный режим») — в процессе синхронизации клиентов, у которых также выбран режим централизованного управления, будут созданы отмеченные ключи (станут активны, если ранее были созданы), а не отмеченные будут заблокированы. Если на клиенте имелись локально созданные ключи преобразования, которые не совпадали с ключами, созданными в ДБ для данного клиента, то в процессе синхронизации с СБ, эти ключи будут отключены;
   - локальный режим управления (поле «Включить централизованный режим» не отмечено) — синхронизация ключей преобразования производиться не будет. При этом останется возможность редактирования списка ключей преобразования.
4. задание удаления неопределенных ключей клиента. Если на клиенте имелись локально созданные ключи преобразования, которые не совпадали с ключами, созданными в ДБ для данного клиента, то в процессе синхронизации они будут удалены.

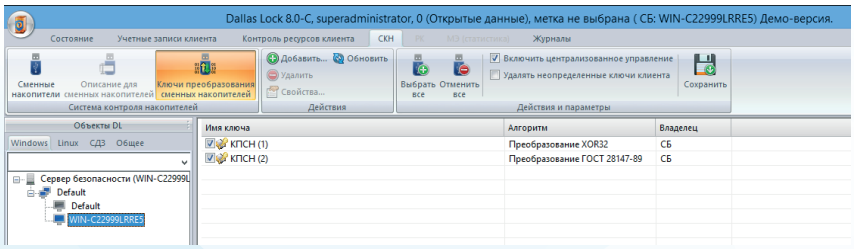

Рисунок 10 — Категория «Ключи преобразования сменных накопителей» вкладки СКН

6.3 С помощью глобальных параметров можно задать для пользователя права, запрещающие работу со всеми непреобразованными накопителями. Для исключения доступа к открытым накопителям необходимо:

1. перейти на вкладку «Контроль ресурсов домена» Консоли Сервера безопасности;
2. выбрать категорию «Глобальные»;
3. выбрать пункт «Параметры открытых сменных накопителей по умолчанию» (Рис. 12);

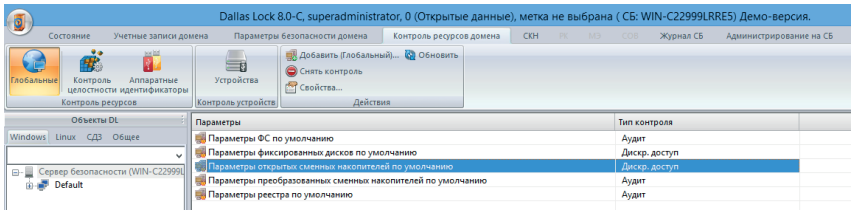

Рисунок 12 — Вкладка «Контроль ресурсов домена» КСБ

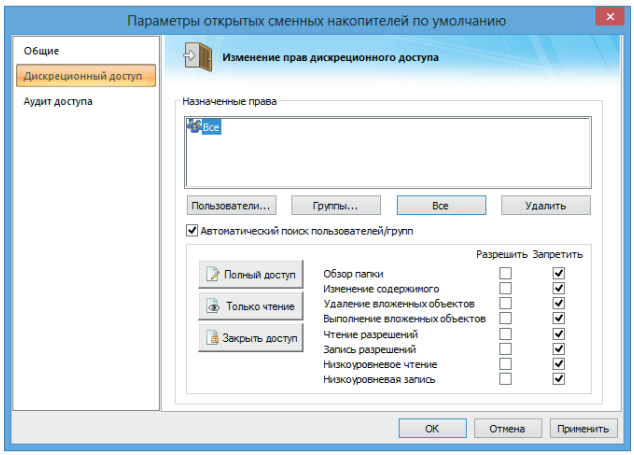

Рисунок 13 — Запрет работы со всеми непреобразованными накопителями

4. в открывшемся окне (Рис. 13) перейти на вкладку «Дискреционный доступ»;
5. выбрать категорию пользователей «Все» и нажать кнопку «Закрыть доступ»;
6. нажать «ОК».

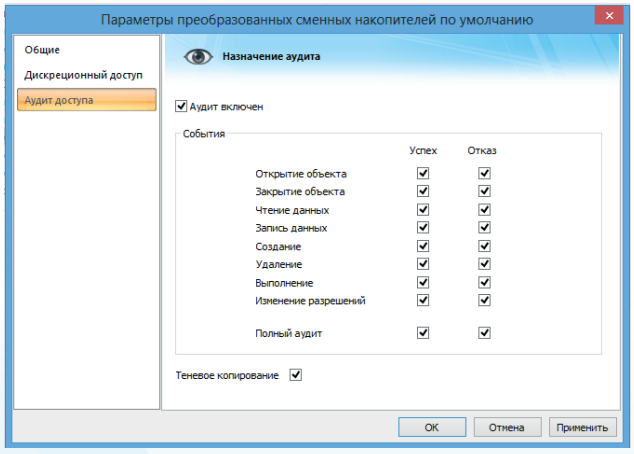

Рисунок 14 — Настройка аудита для преобразованных сменных накопителей

6.4 Также с помощью глобальных параметров можно настроить подробное журналирование действий по работе с преобразованными накопителями. Для этого необходимо:
1. перейти на вкладку «Контроль ресурсов домена» Консоли Сервера безопасности;
2. выбрать категорию «Глобальные»;
3. выбрать пункт «Параметры преобразованных сменных накопителей по умолчанию»;
4. в открывшемся окне (Рис. 14) перейти на вкладку «Аудит доступа»;
5. отметить флагом поле «Аудит включен»;
6. включить полный аудит успехов и отказов;
7. отметить флагом поле «Теневое копирование»;
8. нажать «ОК».

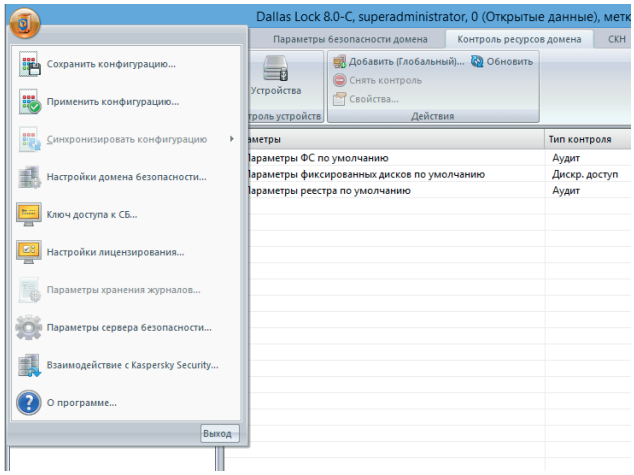

Рисунок 15 — Главное меню Консоли Сервера безопасности

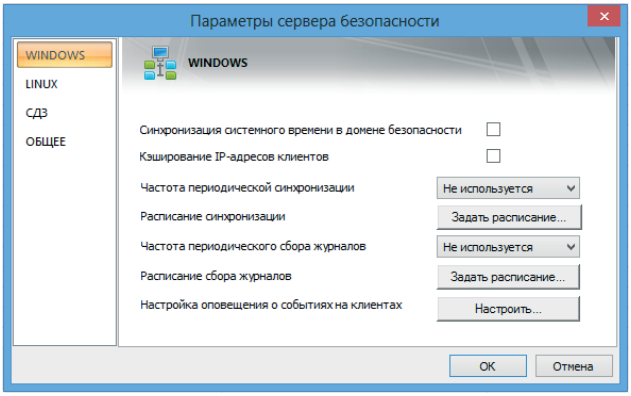

Рисунок 16 — Параметры сервера безопасности

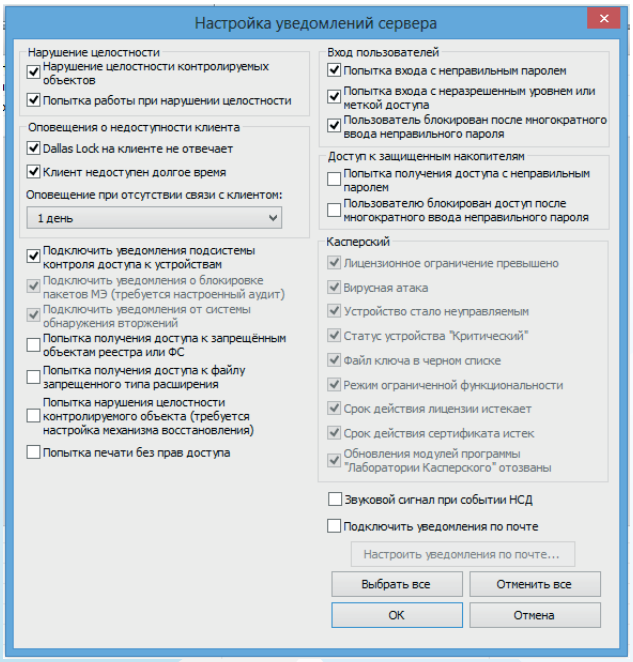

Рисунок 17 — Настройка уведомлений сервера безопасности

6.5 Таким образом, в рамках Домена безопасности пользователи смогут переносить данные только на преобразованные накопители, и эти данные будут храниться в преобразованном виде. Это обеспечивает возможность легитимно переносить информацию, предназначенную для ограниченного круга лиц, на съемных накопителях между защищенными рабочими станциями.

6.6 Кроме того, Сервер безопасности предоставляет возможность настройки сигнализации о попытках доступа к запрещенным накопителям. Для настройки сигнализации о подобных событиях необходимо:

1. в главном меню Консоли Сервера безопасности выбрать пункт «Параметры сервера безопасности» (Рис. 15);
2. в открывшемся окне на вкладке Windows выбрать пункт «Настройка оповещений о событиях на клиентах» (Рис. 16);
3. установить необходимые флаги в категории «Доступ к запрещенным накопителям» (Рис. 17).

6.7 Для организации доступа к преобразованным накопителям в пределах одного Домена безопасности необходимо:

1. создать ключ преобразования;
2. в контекстном меню Сервера безопасности выбрать пункт «Синхронизировать всех клиентов» (синхронизация также возможна на уровне группы клиентов и на уровне отдельного клиента);
3. создать один или несколько преобразованных накопителей с помощью ранее созданного ключа.

6.8 КСБ Dallas Lock предоставляет возможность организации переноса информации на съемных накопителях между разными Доменами безопасности. Для этого необходимо:

1. создать ключ преобразования в другом Домене безопасности таким образом, что параметры ключей преобразования из разных Доменов безопасности совпадали;
2. в контекстном меню Сервера безопасности выбрать пункт «Синхронизировать всех клиентов» (синхронизация также возможна на уровне группы клиентов и на уровне отдельного клиента).

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

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

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

Схема проезда: