Министерство образования и науки Российской Федерации

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

С.А. ТУМАНОВ, И.Л. РЕВА

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОСНОВЕ «DallasLock 8.0»

Учебно-методическое пособие

НОВОСИБИРСК
2016

УДК 004.056.53(075.8)
Т 83

Рецензент
Гужева В.А., начальник отдела специальных исследований
НвсФ ФГУП «НТЦ “Атлас”»

Туманов С.А.

Т 83 Система защиты информации от несанкционированного доступа на основе «DallasLock 8.0»: учеб.-метод. пособие / С.А. Туманов, И.Л. Рева. – Новосибирск: Изд-во НГТУ, 2016. – 56 с.

ISBN 978-5-7782-2826-9

Учебно-методическое пособие к лабораторному практикуму посвящено вопросам изучения и применения системы защиты DallasLock 8.0 и предназначено для студентов и специалистов, проходящих обучение по направлению «Информационная безопасность», а также желающих получить дополнительные сведения по применению и использованию DallasLock 8.0.

В учебно-методическом пособии приведены требования руководящих документов по защите информации от несанкционированного доступа (НСД), рассматриваются основные возможности и общие принципы работы, механизмы идентификации и аутентификации, управления доступом и защиты объектов.

В пособие включены две лабораторные работы, более 50 % учебного времени уделяется практическим работам по настройке программных компонентов в соответствии с типовыми задачами и регламентами. В процессе обучения применяются технологии виртуализации серверов и рабочих мест, что позволяет каждому слушателю индивидуально выполнять практические работы в собственной инфраструктуре.

Работа подготовлена на кафедре защиты информации
и утверждена Редакционно-издательским советом
в качестве учебно-методического пособия

УДК 004.056.53(075.8)

ISBN 978-5-7782-2826-9

ОГЛАВЛЕНИЕ

1. ТРЕБОВАНИЯ РУКОВОДЯЩИЙ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД

В соответствии с «РД Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 года, деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Устанавливается следующий порядок классификации АС в зависимости от вида сведений конфиденциального характера:

- АС, обрабатывающие информацию, составляющую служебную тайну, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Г;

- АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.

Рекомендуется относить АС, обрабатывающие информацию, составляющую коммерческую тайну, режим защиты которой определяет ее собственник, по уровню защищенности к классам 3Б, 2Б и не ниже 1Д (если по решению руководителя предприятия не предъявляются более высокие требования).

АС на базе автономных ПЭВМ должны быть классифицированы и отнесены:

- к третьей группе АС, если в ней работает только один пользователь, допущенный ко всей информации АС;
- ко второй и первой группе АС, если в ней последовательно работают несколько пользователей с равными или разными правами доступа (полномочиями), соответственно.

Для повышения уровня защищенности информации рекомендуется использовать сертифицированные по требованиям безопасности информации СВТ.

При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- не ниже четвертого класса – для класса защищенности АС 1В;
- не ниже третьего класса – для класса защищенности АС 1Б;
- не ниже второго класса – для класса защищенности АС 1А.

СЗИ НСД DallasLock 8.0-C может быть использована при создании защищенных автоматизированных систем до класса защищенности 1Б включительно, для обеспечения первого уровня защищенности персональных данных и в информационных системах первого класса защищенности при условии выполнения ограничений в соответствии с разделом 4 формуляра (RU.48957919.501410-02 30).

СЗИ НСД DallasLock 8.0-C служит для защиты от несанкционированного доступа и раскрытия информации ограниченного доступа до уровня «совершенно секретно».

В общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования, указанные в таблице.

Обозначения:

«–» – нет требований к данному классу;

«+» – есть требования к данному классу.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	–	–	–	+	–	+	+	+	+
к программам	–	–	–	+	–	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	–	–	–	+	–	+	+	+	+
1.2. Управление потоками информации	–	–	–	+	–	–	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа (выхода) субъектов доступа в (из) системы (узел сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов	–	+	–	+	–	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	–	–	–	+	–	+	+	+	+

Продолжение табл.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	–	–	–	+	–	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	–	–	–	+	–	+	+	+	+
изменения полномочий субъектов доступа	–	–	–	–	–	–	+	+	+
создаваемых защищаемых объектов доступа	–	–	–	+	–	–	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	–	+	–	+	–	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	–	–	–	–	–	–	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации	–	–	–	+	–	–	–	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–	–	–	–	–	–	–	–	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	–	–	–	+	–	–	–	+	+

Окончание табл.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	–	–	–	+	–	–	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	–	+	–	+	–	–	+	+	+

2. НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ

2.1. ОБЩИЕ СВЕДЕНИЯ

Система защиты информации от несанкционированного доступа DallasLock 8.0-C (далее по тексту – система защиты, СЗИ НСД или DallasLock 8.0-C) 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.

DallasLock 8.0-C представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

СЗИ НСД DallasLock 8.0-C обеспечивает защиту информации от несанкционированного доступа на ПК в ЛВС через локальный, сетевой и терминальный входы. Также обеспечивает разграничение полномо-

чий пользователей по доступу к файловой системе, устройствам и другим ресурсам компьютера. Разграничения касаются всех пользователей – локальных, сетевых, доменных, терминальных.

2.2. СОСТАВ СИСТЕМЫ ЗАЩИТЫ

Система защиты DallasLock 8.0-C состоит из следующих основных компонентов.

Драйвер защиты. Является ядром системы защиты и выполняет основные функции СЗИ НСД.

Драйвер защиты автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы. Драйвер осуществляет управление подсистемами и модулями системы защиты и обеспечивает их взаимодействие. Драйвер защиты выполняет следующие функции:

- обеспечивает мандатный и дискреционный режимы контроля доступа к объектам файловой системы, реестру и устройствам;
- обеспечивает доступ к журналам, параметрам пользователей и параметрам СЗИ НСД в соответствии с правами пользователей;
- обеспечивает работу механизма делегирования полномочий;
- обеспечивает проверку целостности СЗИ НСД, объектов ФС, программно-аппаратной среды и реестра;
- драйвер защиты осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД.

С драйвером защиты взаимодействуют следующие защитные подсистемы.

Подсистема локального администрирования. Обеспечивает все возможности по управлению СЗИ НСД, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Включает в себя подсистему внедрения в интерфейс windowsexplorer («проводник»). Обеспечивает отображение пунктов в контекстном меню объектов, необходимых для назначения прав доступа к объектам ФС, вызова функции принудительной зачистки объектов ФС, преобразования.

Подсистема удаленного администрирования. Позволяет выполнять настройку системы защиты с удаленного компьютера.

Подсистема централизованного управления. Включает в себя основные компоненты:

- модуль «Сервер безопасности», который позволяет объединять защищенные компьютеры в Домен безопасности для централизованного и оперативного управления клиентами;

- модуль «Менеджер серверов безопасности», который позволяет объединить несколько серверов безопасности в единую логическую единицу «Лес безопасности».

Подсистема управления доступом. Включает в себя:

- подсистему входов. Обеспечивает идентификацию и аутентификацию локальных, доменных, терминальных и удаленных пользователей на этапе входа в операционную систему;
- подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов;
- подсистему доступа к файловой системе, реестру и устройствам, в составе которой:
  - подсистема дискреционного доступа;
  - подсистема мандатного доступа;
- модуль доверенной загрузки уровня загрузочной записи. Является опционным модулем, включается по команде администратора и может быть неактивированным. Активный модуль отрабатывает до начала загрузки ОС;
- подсистему преобразования, которая включает в себя:
  - преобразование информации в файлах-контейнерах;
  - преобразование сменных накопителей для защиты от доступа в обход СЗИ НСД;
  - работа с данными при одновременном их преобразовании в файл-дисках;
  - прозрачное преобразование жестких дисков для предотвращения доступа к данным, расположенным на жестких дисках, в обход СЗИ НСД.

Подсистема регистрации и учета. Включает в себя:

- подсистему аудита. Обеспечивает ведение аудита и хранение информации шести категорий событий в журналах;
- подсистему очистки остаточной информации;
- подсистему печати. Обеспечивает разграничение доступа к печати, добавление штампа на документы, сохранение их теневых копий, регистрацию событий печати.

Подсистема контроля целостности. Обеспечивает контроль целостности файловой системы, программно-аппаратной среды и реестра, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД, восстановление файлов и веток реестра в случае нарушения их целостности.

2.3. ОСНОВНЫЕ ВОЗМОЖНОСТИ

В соответствии со своим назначением СЗИ НСД DallasLock 8.0-C запрещает посторонним лицам доступ к ресурсам ПК и позволяет разграничить права пользователей при работе на компьютере (постороннее лицо, в данном контексте – человек, не имеющий своей учетной записи на данном компьютере). Разграничения касаются прав доступа к сети, к объектам файловой системы, веткам реестра и к устройствам. Для облегчения администрирования возможно объединение пользователей в группы. Контролируются права доступа для локальных, доменных, сетевых и терминальных пользователей.

Для предотвращения утечки информации с использованием сменных накопителей (таких как CD-диск, USB-Flash-диск и пр.) СЗИ НСД обеспечивает следующие функции:

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

СЗИ НСД DallasLock 8.0-C позволяет в качестве средства опознавания пользователей использовать электронные идентификаторы:

- USB-Flash-накопители;
- электронные ключи TouchMemory (iButton);
- USB-ключи Aladdin eToken Pro/Java;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи Rutoken (Рутокен);
- USB-ключи JaCarta (JaCarta GOST и JaCarta PKI).

Дополнительно имеется возможность определения принадлежности аппаратного идентификатора.

В DallasLock 8.0-C реализовано хранение авторизационной информации в аппаратном идентификаторе. Определенные настройки при назначении идентификатора в профиле учетной записи делают возможным вход пользователя на защищенный компьютер только по одному предъявлению идентификатора. Сохранение информации возможно в защищенной памяти идентификатора или в открытой. В случае если информация сохранена в защищённой памяти, запрашивается PIN-код.

Возможно включение функции блокировки компьютера пользователя при отключении назначенного аппаратного идентификатора.

Для решения проблемы «простых» паролей СЗИ НСД 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.

Для создания пароля, соответствующего всем установленным настройкам, в СЗИ НСД реализована функция генерации пароля. Генератор пароля также присутствует при формировании других параметров, включающих аутентификацию: создание PIN-кодов, ключей преобразования, паролей учетных записей и преобразования.

Выбор значения «Число разрешенных сеансов» позволяет осуществлять проверку количества интерактивных сессий для данной учетной записи пользователя в настоящий момент в сети: если число больше разрешенного – вход пользователя на ПК запрещается.

Включение модуля доверенной загрузки уровня загрузочной записи позволяет авторизовать пользователя при входе на ПК до загрузки ОС. Загрузка операционной системы с жесткого диска осуществляется только после ввода особого PIN-кода и его проверки в СЗИ НСД.

Помимо стандартного BIOS модуль доверенной загрузки уровня загрузочной записи поддерживается ПК с материнскими платами, поддерживающими UEFI-интерфейс и GPT-разметку жесткого диска.

В DallasLock 8.0-C используется два принципа разграничения доступа (применяется полностью независимый от ОС механизм).

- Мандатный – каждому пользователю и каждому защищаемому объекту присваивается уровень доступа (по умолчанию, все объекты имеют уровень 0 «открытые данные», но он может быть поднят до любого из семи доступных). Пользователь будет иметь доступ к объектам, уровень доступа которых не превышает его собственный.
- 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).

DallasLock 8.0-C позволяет настраивать «Замкнутую программную среду» (ЗПС) – режим, в котором пользователь может запускать только программы, определенные администратором.

Для удобства и облегчения настройки ЗПС и мандатного доступа реализованы:

- «режим обучения» – в этом режиме при обращении к ресурсу, доступ к которому запрещен, на этот ресурс автоматически назначаются выбранные администратором права;
- «неактивный режим» – режим, в котором возможно полное или частичное отключение подсистем СЗИ НСД DallasLock 8.0-C.

Настройка мандатного доступа для корректной работы пользователей с установленным ПО упрощена автоматической настройкой. В автоматическом режиме данная настройка представляет собой применение определенного шаблона мандатного доступа с помощью специальной встроенной утилиты.

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

В DallasLock 8.0-C реализован контроль доступа к подключаемым (несистемным) 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.

В DallasLock 8.0-C реализована функция разграничения доступа к буферу обмена «Изолированные процессы», которая позволяет исключить возможность копирования информации через буфер обмена средствами терминального подключения к удаленному компьютеру.

В СЗИ НСД DallasLock 8.0-C 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.

СЗИ НСД DallasLock 8.0-C включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Параметрами определяется: количество циклов очистки (1, 2 или 3); производится ли очистка для всех или только конфиденциальных данных. 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 (windowsexplorer);
- осуществлять контроль процесса очистки;
- предотвращать смену пользователя без перезагрузки.

В СЗИ НСД DallasLock 8.0-C 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.

В СЗИ НСД DallasLock 8.0-C реализовано ведение шести 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 НСД. Также в этот журнал заносятся события запуска/завершения модулей администрирования DallasLock 8.0;
- журнал процессов. Заносятся события запуска и завершения процессов в ОС.

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

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.

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 DallasLock 8.0 («С» или «К» при отсутствии метки конфиденциальности) при условии ввода верного пароля и наличии аппаратного идентификатора, используемых при преобразовании.

Преобразование информации средствами СЗИ НСД осуществляется встроенными алгоритмами преобразования: ГОСТ 28147–89 и XOR32. Для функций: создание преобразованных файлов-контейнеров, создание преобразованных файл-дисков, создание преобразованных сменных накопителей доступно использование внешних криптопровайдеров.

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 выпол-

няется одновременно с преобразованием данных, алгоритм преобразования указывается при создании файл-диска.

При использовании нескольких защищенных СЗИ НСД Dallas Lock 8.0-C компьютеров в ЛВС возможно удаленное (сетевое) администрирование. Средствами удаленного администрирования осуществляются 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.

При использовании нескольких защищенных СЗИ НСД Dallas Lock 8.0-C компьютеров в ЛВС возможно централизованное управление ими. Это осуществляется с использованием специального модуля – «Сервер безопасности» (СБ). Этот модуль должен быть установлен на отдельный компьютер, защищенный СЗИ НСД DallasLock 8.0-C. Остальные компьютеры, введенные под контроль данного Сервера безопасности, становятся его клиентами и образуют домен безопасности (ДБ).

С сервера безопасности осуществляются централизованное управление политиками безопасности, просмотр состояния, сбор журналов, создание/удаление/редактирование параметров пользователей, просмотр событий сигнализации о несанкционированном доступе на клиентах, управление ключами преобразования и прочее. Кроме того, с помощью модуля «Менеджер серверов безопасности» (МСБ) имеется возможность объединения нескольких серверов безопасности в лес безопасности (ЛБ).

С помощью сервера безопасности возможны централизованная установка и удаление СЗИ НСД DallasLock 8.0 на компьютерах в сети, ввод в домен безопасности защищенных ПК и обновление версий DallasLock 8.0.

Для ускорения внедрения СЗИ НСД DallasLock 8.0-C в крупных сетях может использоваться механизм удаленной установки и удаленного обновления версий средствами групповых политик ActiveDirectory с использованием сформированного на СБ msi-файла.

В модули централизованного управления (СБ и МСБ) встроен механизм визуализации сети, защищаемой DallasLock 8.0-C. На отдельной вкладке есть возможность просмотреть и отредактировать блок-схему объектов ДБ, сохранить схему в файл.

СЗИ НСД DallasLock 8.0-C содержит подсистему самодиагностики основного функционала СЗИ НСД (тестирование).

Для удобства администрирования СЗИ НСД, 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.).

Для проверки соответствия настроек СЗИ НСД 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».

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

При необходимости переноса настроек DallasLock 8.0-C и сервера безопасности (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 НСД, обновления или на уже защищенный компьютер локально или средствами СБ.

3. ОБЩИЕ ПРИНЦИПЫ РАБОТЫ

Система защиты DallasLock 8.0-C обеспечивает многоуровневую защиту локальных и сетевых ресурсов компьютера как в виде автономной рабочей станции, так и в составе локальной вычислительной сети.

Основные принципы защиты безопасности информации связаны с недопустимостью риска потери или искажения информации несанкционированными и непреднамеренными воздействиями на ресурсы автоматизированной информационной системы предприятия. Они подразумевают:

- защиту от несанкционированного входа на компьютер (защиту по входу);

- разграничение доступа к ресурсам файловой системы и подключаемым устройствам.

Защита от несанкционированного входа предназначена для защиты компьютера от посторонних пользователей.

Действие защиты по входу сводится к проверке полномочий пользователя на вход при попытке загрузки операционной системы и попытке войти в операционную систему.

После включения ПК загрузка ОС осуществляется после верного ввода особого PIN-кода модуля доверенной загрузки. Данный модуль является опционным и может быть не активизирован администратором. После верной авторизации происходит загрузка операционной системы. После загрузки ОС происходит авторизация пользователя. При проверке авторизационных данных и наличия полномочий на загрузку ПК пользователь получает право на вход в систему и может работать с теми ресурсами компьютера или сети, доступ к которым для него разрешен. При отсутствии требуемых полномочий вход в систему пользователю запрещается.

Разграничение доступа к ресурсам предназначено для управления доступом к ресурсам файловой системы зарегистрированными пользователями. С помощью средств разграничения доступа для каждого пользователя устанавливаются определенные права доступа к определенным ресурсам. Пользователю разрешается использовать ресурсы файловой системы только в рамках установленных для него прав. При отсутствии таковых доступ к ресурсу запрещается.

При загрузке компьютера осуществляются идентификация и аутентификация пользователя. Также выполняется проверка целостности контролируемых объектов средствами механизма контроля целостности. В том случае, если имя пользователя и пароль указаны верно, предъявлен верный аппаратный идентификатор и целостность контролируемых объектов не нарушена, загрузка компьютера продолжается. Иначе загрузка компьютера прерывается.

В процессе работы текущего пользователя с ресурсами компьютера драйвер защиты контролирует доступ пользователя к ресурсам. Если пользователь превышает свои права доступа к ресурсу, его действия ограничиваются способом, заданным параметрами работы системы защиты. Также средствами механизма регистрации событий осуществляется регистрация в соответствующих журналах всех событий, связанных с безопасностью системы и работой пользователя на компьютере.

Подобным образом контролируется доступ к подключаемым устройствам (не системным) и ведется аудит монтирования/демонтирования устройств.

В системе DallasLock 8.0-C каждому зарегистрированному пользователю назначаются соответствующие права на доступ к ресурсам файловой системы, устройствам и полномочия на администрирование системы защиты.

3.1. МЕХАНИЗМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Защита от несанкционированного входа предназначена для защиты компьютера от посторонних пользователей.

Защита от несанкционированного входа реализуется механизмом идентификации и аутентификации пользователей, обеспечивающим (в том числе с помощью аппаратных средств) защиту от входа постороннего пользователя в систему при загрузке компьютера.

Идентификация (распознавание) и аутентификация (проверка подлинности) пользователей осуществляются при каждом входе пользователя на защищенный компьютер и при входе в ОС.

Последовательность входа на защищенный ПК следующая. Если включен режим доверенной загрузки, то в нем нужно ввести PIN-код. Далее, при загрузке ОС компьютера система DallasLock 8.0-C запрашивает у пользователя его имя и пароль (если пользователю присвоены аппаратные средства, то запрашивается идентификатор). Затем осуществляется проверка наличия в системе зарегистрированного пользователя с указанным именем. После этого проверяется правильность указанного пользователем пароля. Если сведения указаны верно, то пользователю разрешается вход в систему, иначе вход в систему пользователю запрещается.

Для идентификации пользователей в системе DallasLock 8.0-C могут использоваться следующие виды идентификаторов:

- уникальные имена длиной до 32 символов;
- уникальные номера персональных аппаратных идентификаторов.

Имя присваивается пользователю при его регистрации в системе DallasLock 8.0-C. Если компьютер оснащен устройством чтения персональных идентификаторов, пользователю может быть присвоен один персональный аппаратный идентификатор, серийный номер которого может использоваться для идентификации пользователя.

Аутентификация пользователя осуществляется после его идентификации для подтверждения того, что пользователь действительно является тем, кем представился.

При аутентификации пользователя осуществляется проверка правильности указанного им пароля.

В DallasLock 8.0-C поддерживается работа с паролями длиной до 32 символов. Дополнительно, соответствующей политикой безопасности системы защиты для пароля могут быть заданы следующие атрибуты:

- минимальная длина пароля;
- правила, обеспечивающие сложность пароля (необходимость наличия цифр, специальных символов, строчных и прописных букв и необходимость изменения пароля, в сравнении с предыдущим, на определенное количество символов, необходимое отсутствие цифры в первом и последнем символе);
- минимальный/максимальный срок действия пароля.

Чем больше длина пароля и чем он сложнее, тем надежнее защита. Для создания пароля, отвечающего всем установленным требованиям параметров безопасности, существует механизм генерации пароля системы защиты. Для этого необходимо нажать кнопку с надписью «Генерация пароля».

Вводимый пароль не отображается на экране компьютера. Если пароль при входе указан неверно, то система защиты сообщает об этом, и в системном журнале регистрируется попытка несанкционированного доступа к компьютеру. Если пользователь несколько раз подряд неверно указал пароль и превысил число попыток, отводящихся ему для правильного ввода пароля, то выдается сообщение о блокировании учетной записи этого пользователя. Теперь этот пользователь может осуществить новую попытку входа только после разблокирования учетной записи, которое производится администратором. Максимальное количество ошибок ввода пароля и время блокировки учетной записи в случае ввода неправильного пароля регулируются настройками системы защиты.

Пароль может быть изменен только самим пользователем или администратором безопасности (пользователем, имеющим соответствующие полномочия).

Администратор может назначать пользователям новые пароли, но не имеет возможности узнать значения старых паролей. Администратор также может потребовать смену пароля при следующем входе или запретить смену пароля пользователем.

3.2. МЕХАНИЗМЫ УПРАВЛЕНИЯ ДОСТУПОМ

Разграничение доступа к объектам

В системе защиты DallasLock 8.0-C имеется возможность ограничивать перечень доступных объектов: объектов ФС, веток реестра и подключаемых несистемных устройств, – для каждого пользователя в рамках его функциональных обязанностей. Возможны ограничения на чтение данных, запись данных, выполнение (запуск), создание файлов, создание папок, удаление файлов, удаление папок, обзор содержимого папки и пр.

При попытке пользователя запустить программу, запрещенную для доступа или выполнения, операционная система вместо загрузки программы будет выдавать сообщение об ошибке, например:

Доступ запрещен

или при попытке открыть запрещенный файл:

Не удается открыть файл

Предусмотрены два принципа ограничения доступа.

- Согласно индивидуальному списку доступа к объекту (дискреционный доступ).
- Согласно классификационной метке объекта (мандатный доступ).

Дискреционный доступ

В системе защиты DallasLock 8.0-C для ограничения доступа к объектам предусмотрен дискреционный принцип ограничения доступа к объектам, т. е. согласно индивидуальному списку.

Применительно к правам доступа всех пользователей, зарегистрированных в системе защиты, можно разделить на три разряда.

- 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.
- Группы пользователей. Всем пользователями, входящим в одну группу, автоматически назначаются права на доступ, установленные для группы.

• Все. К этому разряду относятся все пользователи, для которых не установлены индивидуальные права доступа и одновременно не входящие 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 файловой системы.

В системе защиты DallasLock 8.0-C каждому объекту может быть сопоставлен список, элементами которого могут являться индивидуальные пользователи, учетные записи по маске, группы пользователей и разряд «Все». Каждому элементу списка сопоставляется свой набор значений параметров безопасности.

Механизм определения права доступа пользователя к объекту

В системе защиты DallasLock 8.0-C права доступа пользователя к объекту определяются:

• параметрами безопасности объекта, установленными на сам ресурс;

• параметрами безопасности родительского объекта.

Набор параметров (локальных и глобальных) в системе защиты представлен в виде списка. Каждому параметру из списка можно явно указать значение: разрешить или запретить.

3.3. ПАРАМЕТРЫ БЕЗОПАСНОСТИ РЕСУРСОВ

В соответствии с этим принципом доступа каждый зарегистрированный пользователь/группа пользователей компьютера наделяется определенными правами доступа к объектам.

Каждый объект системы защиты характеризуется набором параметров безопасности. Каждый параметр безопасности контролирует определенную операцию (удаление, перемещение, выполнение, изменение и т. д.), которая может быть произведена с объектом. Любая операция с объектом может быть разрешена либо запрещена пользователю. Соответственно каждый параметр может иметь значение разрешить либо запретить.

В системе DallasLock 8.0-C действуют следующие общие правила управления доступом к объектам.

• Если права доступа пользователя к ресурсу не позволяют ему выполнить некоторую операцию с ресурсом, система DallasLock 8.0-C блокирует выполнение этой операции.

- Возможность изменения параметров доступа, присвоенных существующим объектам, ограничена и определяется полномочиями на администрирование системы защиты, предоставленными пользователю.
- Операции, которые можно производить с объектом в системе защиты, зависят от типа объекта.

Локальные, сменные и удаленные диски, каталоги и подкаталоги характеризуются следующими параметрами.

- Обзор папки. Чтение содержимого. Позволяет увидеть все вложенные в данную папку каталоги, подкаталоги, файлы, содержащиеся в корневом каталоге объекта.
- Выполнение вложенных объектов. Выполнение находящихся в папке файлов.
- Изменение содержимого. Изменение находящихся в папке вложенных папок и файлов (запись, удаление, создание).

Для файлов возможны следующие параметры (файлы могут находиться на локальных дисках, на сменных носителях, на сетевых ресурсах).

- Чтение. Позволяет прочитать содержимое файла любого типа.
- Запись. Удаление файла, а также запись на диск модифицированного (измененного) файла.
- Выполнение. Имеет смысл только для программ. Позволяет запускать программу на выполнение.

Ветки реестра характеризуются следующими параметрами.

- Чтение. Позволяет прочитать содержимое.
- Запись. Создание и удаление параметров в ветке реестра и ее самой.

Также имеются следующие дополнительные параметры объектов (ФС и реестра).

- Чтение разрешений. Позволяет просмотреть значения параметров, установленные для ресурса.
- Изменение разрешений. Позволяет не только читать разрешения, но и изменять их.

Устройства характеризуются параметрами доступа «*Разрешить*» *и* «*Запретить*».

«*Неактивный*» *режим контроля доступа к ресурсам*

В системе защиты DallasLock 8.0-C реализован особый механизм контроля доступа к ресурсам, который позволяет отключать подсистемы СЗИ НСД. Настройки позволяют определить такой режим работы, при котором:

- проверяются все права дискреционного доступа;

- сообщения о запрете при попытке пользователя произвести запрещенную политиками безопасности операцию заносятся в журнал доступа к ресурсам;
- доступ к запрещенным пользователю объектам дается, несмотря на запрет.

«Неактивный» режим полезен при настройке замкнутой программной среды (см. далее), а также для временного отключения контроля доступа системой защиты.

Механизм замкнутой программной среды

Для усиленных мер безопасности в системе DallasLock 8.0-C существует механизм «замкнутой программной среды» (ЗПС), который позволяет явно указать, с какими программами пользователь может работать (со всеми же остальными программами пользователь работать соответственно не сможет).

Для реализации механизма ЗПС 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 используется механизмы дискреционного контроля доступа. А конкретно – право «Выполнение».

Механизм замкнутой программной среды дополняет включение оболочки DallasLock вместо стандартной графической оболочки пользователя Windows. Защищенная оболочка DallasLock – это программа, которая отвечает за создание рабочего стола, наличие на нем ярлыков программ, панели задач и меню «Пуск».

Локальные и глобальные параметры безопасности ресурсов

Для любого пользователя можно установить набор значений параметров ресурсов, который будет действовать для всех ресурсов. Например, запретить удалять и создавать любые папки. Такая настройка параметров для данного пользователя в системе защиты имеет название глобальной настройки, а параметры, установленные при глобальной настройке, – глобальные параметры.

С другой стороны, для любого пользователя можно установить параметры конкретному ресурсу, например, запретить удалять только конкретную папку. Параметры безопасности конкретного ресурса,

установленные для данного пользователя, в системе условно называются локальными параметрами.

Совокупность значений параметров безопасности, установленных для данного пользователя по отношению к конкретному ресурсу, определяет права доступа пользователя к этому ресурсу.

Если пользователю разрешены все операции с объектом, то считается, что пользователь имеет полный доступ к данному объекту. Соответственно, если часть операций запрещена, то пользователь имеет частичный доступ. Запрет любых операций означает отсутствие доступа.

Любому пользователю (кроме суперадминистратора) можно полностью или частично ограничить доступ к любому объекту.

Мандатный доступ

Каждому объекту файловой системы и подключаемому несистемному устройству можно присвоить метку конфиденциальности. Метки конфиденциальности имеют номера от 0 до 7. Чем больше номер, тем выше уровень конфиденциальности. Если не указана никакая метка, то считается, что объект имеет метку 0 (ноль) – открытые данные. Если метку конфиденциальности присвоить папке (диску), то все объекты, находящиеся в данной папке (диске) будут иметь ту же метку, за исключением тех случаев, когда им явно присвоены другие метки конфиденциальности.

Для удобства работы меткам конфиденциальности можно присваивать имена. По умолчанию первым пяти уровням конфиденциальности (от 0 до 4) присвоены следующие наименования:

- 0 (открытые данные);
- 1 (конфиденциальные данные);
- 2 (персональные данные);
- 3 (секретные данные);
- 4 (совершенно секретно).

Эти имена можно сменить на любые другие, на работу системы защиты это никак не повлияет. Для системы защиты имеет значение только номер.

Присвоить метку конфиденциальности объекту можно с помощью окна его свойств, вкладка «Мандатный доступ». Если убрать галочку «По умолчанию», то появится возможность в выпадающем списке выбрать нужную метку.

Для каждого пользователя в профиле его учетной записи также устанавливается уровень конфиденциальности от 0 до 7.

Пользователи, имеющие уровень конфиденциальности 0, имеют доступ только к объектам ФС, имеющим метку конфиденциальности 0. Пользователи, имеющие уровень конфиденциальности 1, имеют доступ только к объектам ФС, имеющим метки конфиденциальности 0 и 1. Имеющие уровень конфиденциальности 2 – только к объектам с метками 0, 1, 2. И так далее. Пользователи уровня 7 имеют доступ ко всем объектам.

Назначать категорию конфиденциальности дискам и каталогам, а также устанавливать для пользователей уровень допуска к конфиденциальной информации может только тот пользователь компьютера, который наделен соответствующими полномочиями на администрирование системы защиты.

При входе в ОС пользователь может выбрать уровень доступа, не превышающий установленный для него уровень конфиденциальности. Например, если пользователь имеет уровень конфиденциальности 5, то он может войти в систему с уровнями 0, 1, 2, 3, 4 или 5. Если пользователь выберет уровень доступа, превышающий собственный уровень конфиденциальности, то система защиты выдаст сообщение об ошибке «Мандатный уровень указан неверно». Уровень, с которым пользователь вошел в систему, называется «текущий уровень доступа». Кроме того, пользователь в процессе работы может поднять свой текущий уровень конфиденциальности, но не выше своего максимально. Понизить же текущий уровень можно, только начав новый сеанс работы.

Назначать категорию конфиденциальности дискам и каталогам, а также устанавливать для пользователей уровень допуска к конфиденциальной информации может только тот пользователь компьютера, который наделен соответствующими полномочиями на администрирование системы защиты.

Разграничение доступа к конфиденциальным ресурсам осуществляется следующим образом. Когда пользователь (программа, запущенная пользователем) осуществляет попытку доступа к конфиденциальному ресурсу, система защиты определяет уровень секретности данного объекта. Затем уровень секретности объекта сопоставляется с уровнем допуска к конфиденциальной информации текущего пользователя. Если текущий пользователь не превышает свой уровень допуска, система защиты санкционирует доступ к ресурсу. Иначе система защиты блокирует доступ к объекту.

В системе защиты предусмотрен механизм, позволяющий предотвратить понижение уровня секретности данных. Механизм действует следующим образом.

- При входе в систему пользователь имеет возможность выбрать текущий уровень доступа, не превышающий установленный для него уровень.
- Запись во все объекты, кроме объектов, уровень секретности которых равен текущему уровню доступа пользователя, блокируется (за исключением «разделяемых» папок).

3.4. МЕХАНИЗМЫ ЗАЩИТЫ ОБЪЕКТОВ

Механизм контроля целостности

СЗИ НСД DallasLock 8.0-C включает в свой состав подсистему контроля целостности. Она позволяет контролировать целостность программно-аппаратной среды компьютера, целостность объектов файловой системы и целостность веток реестра.

Процедура контроля целостности осуществляется следующим образом.

- После назначения параметра контроля 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.

При обнаружении нарушения целостности в системе Dallas Lock 8.0-C происходит следующее.

- Блокировка ПК (если у пользователя установлено соответствующее свойство).
- Вывод предупреждения.
- Занесение события в журнал.
- Отправка сообщения на Сервер безопасности (для ПК в Домене безопасности).

У каждого пользователя есть свойство, определяющее действия при выявлении нарушения целостности – либо выдавать предупреждение и продолжать загрузку, либо блокировать загрузку (свойство «Блокировать при нарушении целостности»).

В системе DallasLock 8.0-C проверка целостности может осуществляться:

- в процессе загрузки ПК;
- периодически;
- по заранее составленному расписанию;
- при доступе к объекту (например, при открытии файла) (в этом случае он становится доступным только на чтение);
- по команде администратора (с помощью локальных средств администрирования, либо удаленных).

Механизм регистрации событий

В процессе работы системы DallasLock 8.0-C все события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в системных журналах. Просматривая журналы, можно получить информацию обо всех действиях пользователя, совершенных им на защищенном компьютере. В каждом журнале фиксируются дата, время, имя пользователя, операция, результат и прочие параметры. В СЗИ НСД DallasLock 8.0-C ведется шесть журналов.

- Журнал входов. Фиксируются все входы (или попытки входов – с указанием причины отказа) и выходы пользователей ПК, включая локальный, сетевые и на другие ПК, в том числе терминальный вход и вход для удаленного администрирования.
- Журнал управления учетными записями. Ведется учет всех действий по изменению прав пользователей, созданию и удалению пользователей.
- Журнал ресурсов. Позволяет проследить обращения к объектам ФС и события монтирования/демонтирования устройств, для которых назначен аудит.
- Журнал печати. Заносятся все события, связанные с распечаткой документов на локальных или удаленных принтерах.
- Журнал управления политиками. Дает возможность просмотреть все действия, изменяющие настройку параметров системы защиты.
- Журнал процессов. В журнал заносятся события запуска и завершения процессов.

Система защиты позволяет осуществлять гибкую настройку аудита, выбирать, какие действия пользователя по отношению к каким ресурсам необходимо регистрировать. Кроме того, можно протоколировать все действия, касающиеся администрирования системы защиты.

Использование фильтров позволяет отсеять ненужные данные в журнале так, что они становятся невидимы при просмотре.

Есть возможность экспортировать журналы в другие форматы для последующей обработки.

Настройку режимов регистрации событий может осуществлять только тот пользователь, который наделен соответствующими полномочиями на администрирование системы защиты.

Механизм очистки остаточной информации

СЗИ НСД DallasLock 8.0-C включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Специальные политики определяют количество циклов очистки (1, 2 или 3); производится ли очистка для всех или только для конфиденциальных данных (объектов с уровнем конфиденциальности больше 0).

Подсистема позволяет:

- 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;
- предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого без перезагрузки;
- осуществлять проверку очистки;
- дает возможность задать один, два или три цикла затирания.

Сохранение резервной копии файлов системы защиты

В системе защиты реализован механизм создания и сохранения резервной копии файлов DallasLock 8.0-C. Функция сохранения резервной копии файлов предназначена для ведения нескольких копий программных компонентов средства защиты информации, с возможностью последующей сверки с файлами, используемыми в системе, обнаружения несоответствий (проверяется не только совпадение размера, но и содержимое файлов) и возможностью восстановления.

Поддержка аппаратных средств защиты

Система защиты DallasLock 8.0-C поддерживает работу с аппаратными средствами идентификации. Это позволяет:

- назначать персональные идентификаторы пользователям системы при регистрации для усиленной аутентификации;
- назначать идентификаторы при преобразовании объектов файловой системы, при создании ключевой информации для преобразованного файл-диска;
- назначать аппаратную идентификацию при создании ключа преобразования сменного накопителя.

Система DallasLock 8.0-C позволяет в качестве средства опознавания пользователей системы использовать электронные идентификаторы: USB-флэш-накопители, электронные ключи TouchMemory (iButton), USB-ключи AladdineTokenPro/Java, смарт-карты Aladdine TokenPro/SC, USB-ключи Rutoken (Рутокен) и Rutoken ЭЦП, USB-ключи JaCarta: JaCartaGOST и JaCartaPKI.

Возможность использования в системе защиты DallasLock 8.0-C современных аппаратных идентификаторов предполагает наличие в аппаратной части ПК соответствующего USB-порта или COM-порта.

В системе защиты реализовано хранение авторизационной информации в аппаратном идентификаторе, а также определение принадлежности предъявленного аппаратного идентификатора.

ЛАБОРАТОРНАЯ РАБОТА № 1

Цель работы

Изучить программный комплекс защиты информации от несанкционированного доступа «DallasLock 8.0-K»

Настроить для пользователей мандатный доступ и параметры безопасности в соответствии с требованиями по классам 3А (один пользователь), 1В (два пользователя), 1Б (два пользователя) с помощью «DallasLock 8.0-C» и дискреционный доступ и параметры безопасности по классам 2Б (два пользователя), 1Г (два пользователя) с помощью «Dallas-Lock 8.0-K» согласно матрицам доступа.

Для класса 1Г

Пользователь	**PDocs**	**SDocs**	**SSDocs**
User3	R--	RWX	---
User4	R--	---	RWX

Для класса 2Б

Пользователь	**PDocs**	**SDocs**	**SSDocs**
User3	---	R--	RWX
User4	RWX	---	R--

Ход работы

Шаг 1. Создаем пользователя и задаем ему уровень мандатного доступа (по заданию: 1 – конфиденциальные данные).

Шаг 2. Создаем две папки PDocs и SDocs, включаем для них полный аудит и контроль целостности. Для PDocs задаем уровень мандатного доступа: 1 – конфедециальные данные, а для SDocs задаем 2 – персональные данные, чтоб user1 не имел к ней доступа.

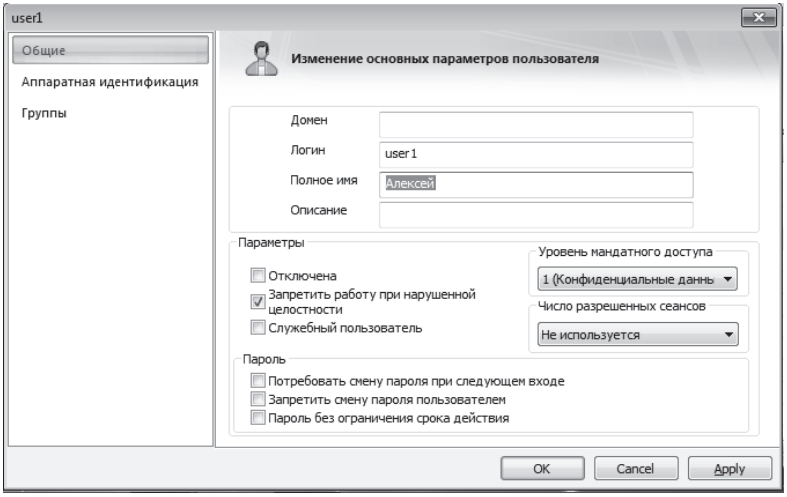

Рис. 1. Создание пользователя user1

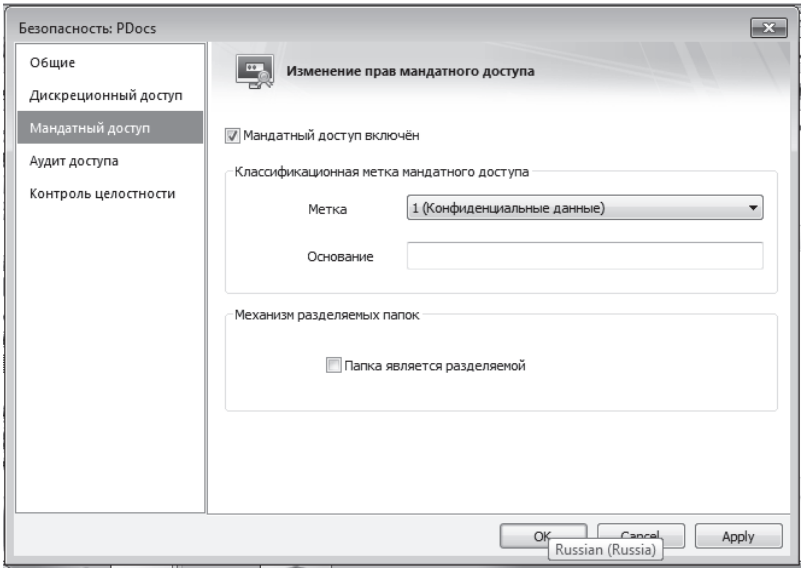

Рис. 2. Создание папки PDocs

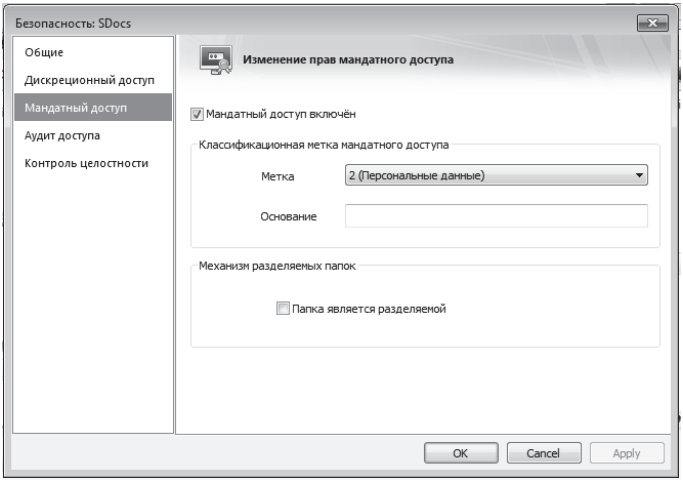

Рис. 3. Создание папки SDocs

Шаг 3. Устанавливаем параметры согласно требованиям по классу 3А.

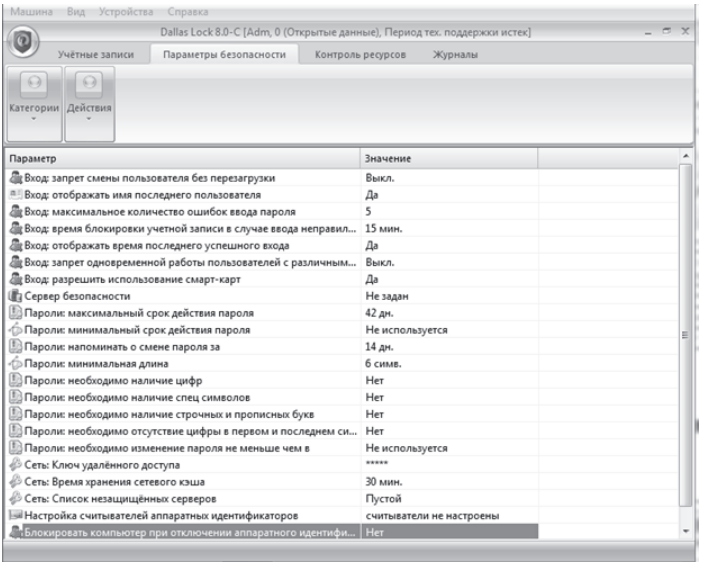

Рис. 4. Параметры безопасности входа для класса 3А

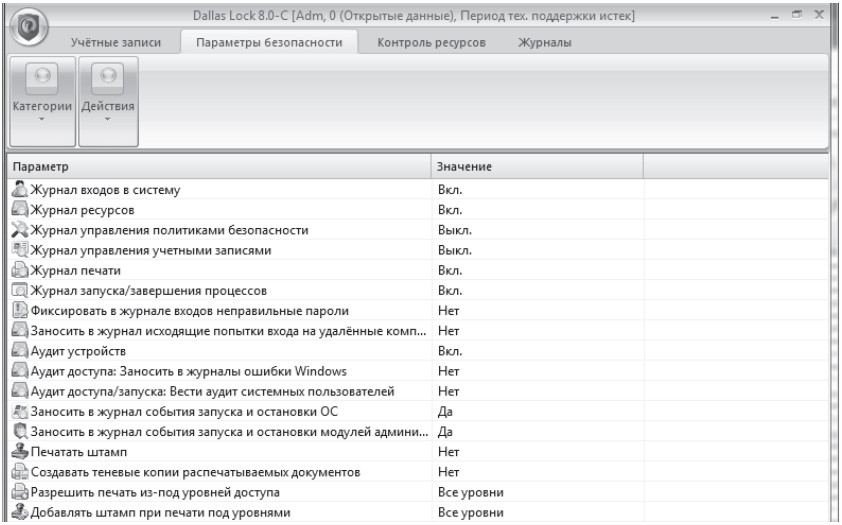

Рис. 5. Параметры подсистемы регистрации и учета для класса 3А

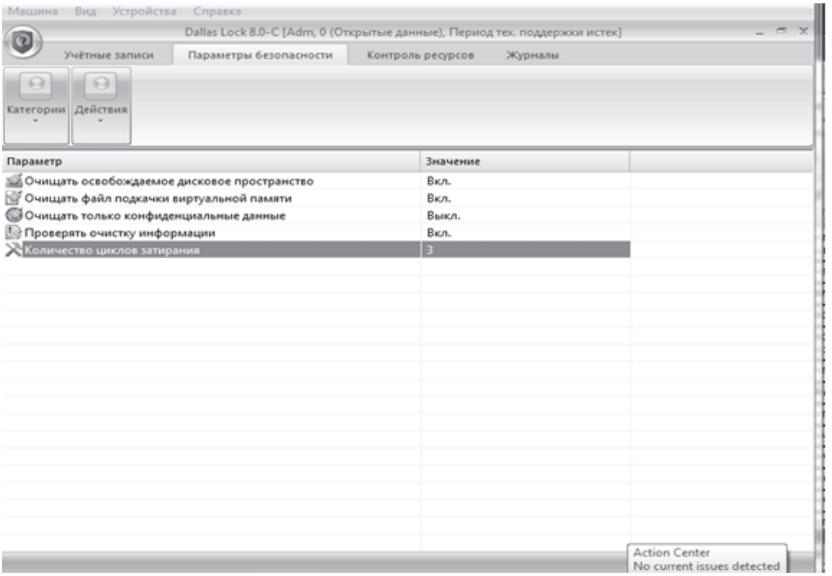

Рис. 6. Очистка освобождаемых областей для класса 3А

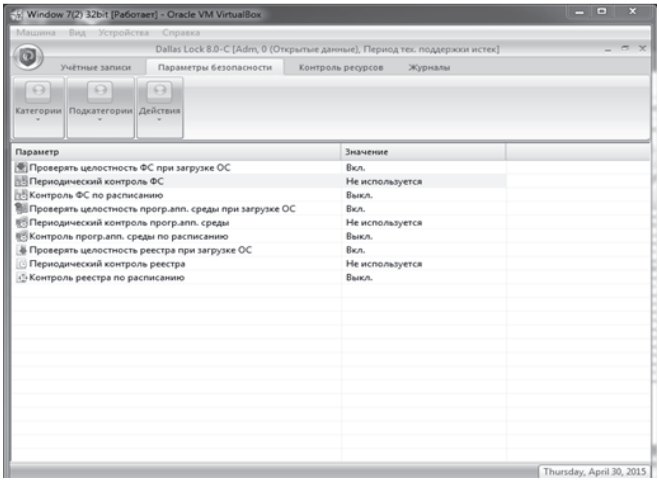

Рис. 7. Очистка освобождаемых областей

Для запуска автоматического тестирования функционала необходимо в оболочке администратора нажать кнопу основного меню и в списке функций выбрать пункт «Тестирование функционала СЗИ».

Затем нажать кнопку «Запустить» и ждать окончания тестирования.

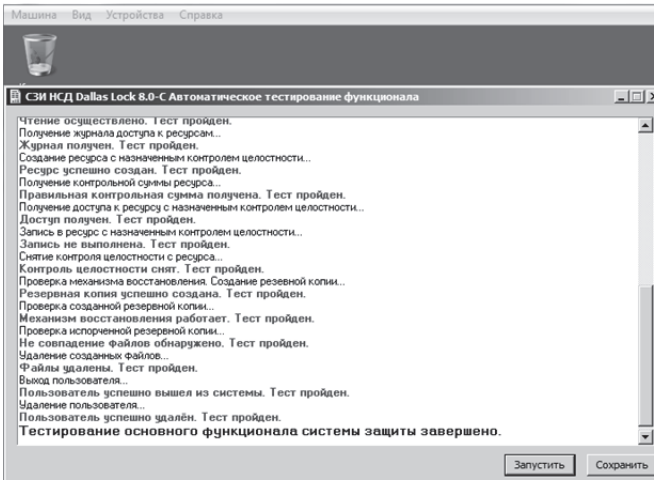

Рис. 8. Запуск тестирования функционала СЗИ

Способов восстановления несколько: с помощью загрузочного диска и в ручном режиме.

Аварийное восстановление с помощью загрузочного диска

После завершения восстановления преобразованных областей дисков (для этого нужно после ввода PIN-кода нажать F2, чтобы появился пункт «Аварийное восстановление», и затем нажать Enter), если такие были, необходимо загрузиться со специального диска восстановления СЗИ НСД DallasLock 8.0. Для получения данного диска необходимо обратиться к разработчику.

В появившемся меню загрузочного диска необходимо выбрать пункт «Аварийное восстановление».

После загрузки в консоли аварийного восстановления будут предложены команды:

- **DLOFF** – аварийное отключение DallasLock в Windows;
- **DLMBROFF** – отключение загрузчика DallasLock;
- **RESTART** – перезагрузка;
- **HELP** – справка.

Если был активирован модуль доверенной загрузки, то командой DLMBROFF его необходимо отключить. После чего система выведет сообщение о том, что в MBR установлен оригинальный загрузчик.

Далее необходимо отключить саму систему защиты DallasLock 8.0 командой DLOFF. После этого система выведет сообщение о том, что система защиты аварийно отключена.

Далее необходимо ввести команду RESTART для перезагрузки компьютера. После перезагрузки система защиты DallasLock 8.0 будет отключена. Далее для корректного отключения системы защиты необходимо внести изменения в реестр.

Сделать это можно, воспользовавшись специальной утилитой 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.

После запуска данной утилиты с правами администратора и команды завершения снятия СЗИ НСД DallasLock 8.0 будет предложено перезагрузиться. Также в процессе снятия системы защиты будет предложено оставить или удалить системную папку DLLOCK80 с хранящимися в ней журналами и другими конфигурационными файлами.

После перезагрузки система защиты DallasLock 8.0 будет удалена с компьютера, теперь можно снова запустить ее установку.

Аварийное восстановление в ручном режиме

Для аварийного отключения системы защиты DallasLock 8.0 в ОС WindowsVista/2008/7/2008R2/8/2012/8.1/2012R2 необходимо получить доступ к файловой системе.

Для этого можно воспользоваться в том числе платформой восстановления WindowsRecoveryEnvironment (WinRE), которая является «преемником» консоли восстановления для предыдущих версий ОС.

WinRE может быть загружена с установочного диска операционной системы. Но можно воспользоваться встроенным инструментом восстановления, не требующим загрузки с CD. Для этого необходимо запустить меню дополнительных вариантов загрузки (перед началом загрузки ОС нажать F8 на клавиатуре).

Необходимо выбрать «Устранение неполадок компьютера» (Repair YourComputer). 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).

После получения доступа к файловой системе необходимо подменить системные файлы.

После получения доступа к файловой системе необходимо произвести отключение модуля интерактивного входа путем переименования и копирования файлов с помощью команд:

- 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*

После подмены системных файлов необходимо очистить реестр.

* Если файлы dllives.dll и livessp.dll отсутствуют – некритично.

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 операционной системы, 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.

Изменить значение на «0» параметра Disabled по пути:

для Windows Vista/2008/7/2008R2:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Authentication\ Credential Providers\{6f45dc1e-5384-457a-bc13-2cd81b0d28ed},

для Windows 8/8.1/2012/2012R2:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Authentication\ Credential Providers\ {60b78e88-ead8-445c-9cfd-0b87f74ea6cd}.

Удалить ветку реестра {9123E0C2-FF5E-4b38-BAB9-E2FA800 D2548} по пути:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\ Authentication\Credential Providers.

Полностью удалить из реестра следующие разделы:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dl Crypt,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dl Disk,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DlFlt,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dl HwCtrl

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 (удобно сделать это не для каждого ключа, а для ветки Root).

Изменить значение ключа UpperFilters в ветке:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Clas s\{4D36E967-E325-11CE-BFC1-08002BE10318}: вместо «DlDiskPart-Mgr» следует оставить «PartMgr».

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).

После выполнения вышеописанных 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.

Настроить для пользователей мандатный доступ и параметры безопасности согласно требованиям по классу 1В с помощью «DallasLock 8.0-C».

Шаг 1. Создаем второго пользователя и задаем ему уровень мандатного доступа 0 – открытые данные

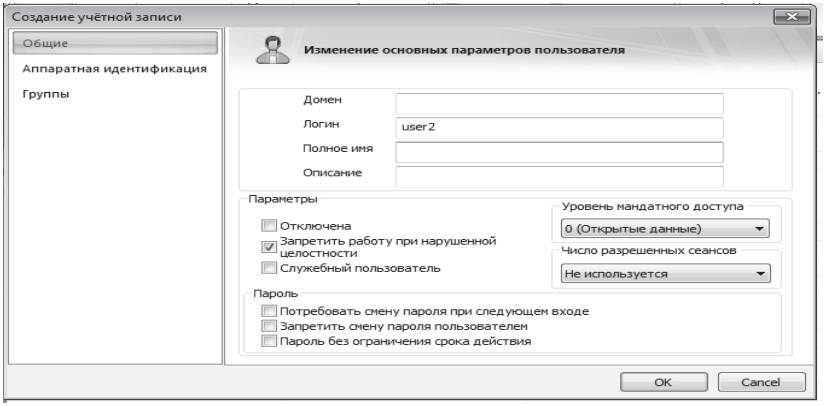

Рис. 9. Создание пользователя user2

Шаг 2. Создаем третью папку Docs, включаем для нее полный аудит и контроль целостности и задаем ей уровень мандатного доступа 0 – открытые данные, чтобы user2 имел к ней доступ и не имел доступа к остальным.

Таким образом, user1 имеет доступ к папкам PDocs и Docs, user2 имеет доступ к Docs, к SDocs у них нет доступа.

Шаг 3. Устанавливаем параметры согласно требованиям по классу 1В.

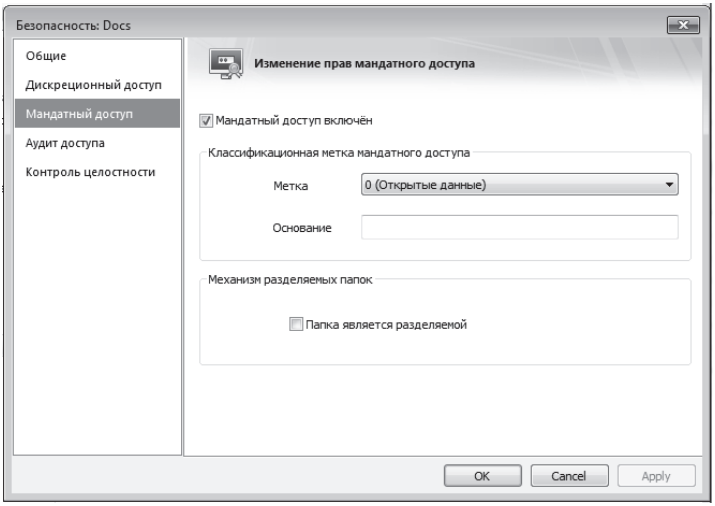

Рис. 10. Создание папки Docs

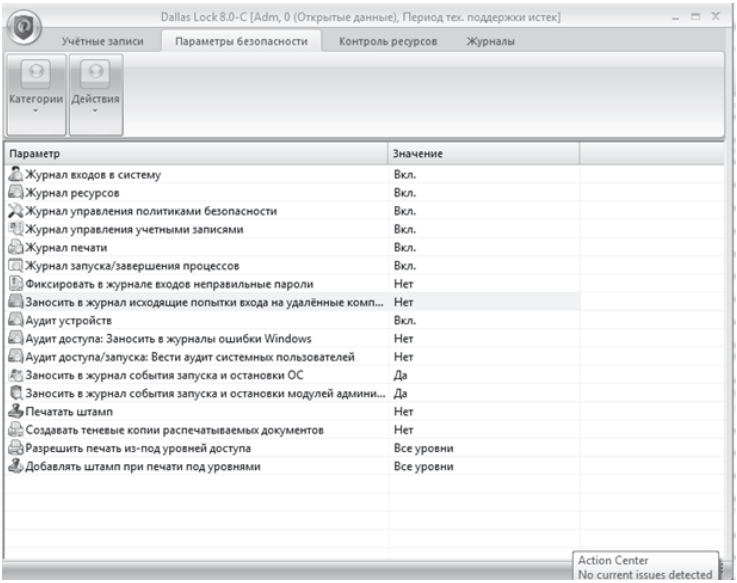

Рис. 11. Параметры регистрации и учета для класса 1В

Сигнализация попыток нарушения защиты работает автоматически.
Остальные параметры, как у класса 3А (пункт 2, шаг 3).

Настроить для пользователей мандатный доступ и параметры безопасности согласно требованиям по классу 1Б с помощью «DallasLock 8.0-С».

Шаг 1. Задаем обоим пользователям уровень мандатного доступа 1 – конфеденциальные данные.

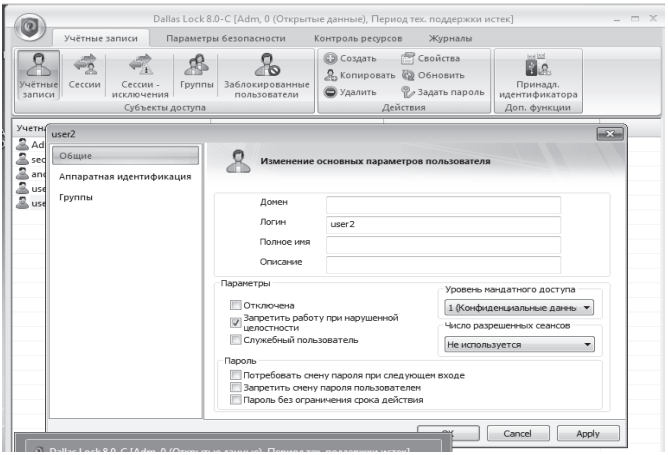

Рис. 12. Изменение уровня мандатного доступа для user2

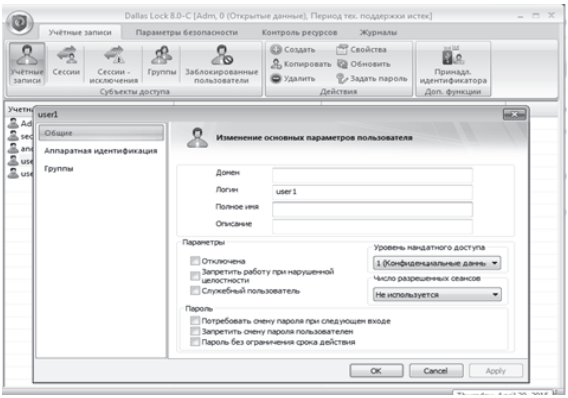

Рис. 13. Уровень мандатного доступа для user1

Шаг 2. Создадим еще две папки SSDocs с мандатным доступом 4 – совершенно секретно и 5LDocs с пятым уровнем доступа и включим для них полный аудит и контроль целостности.

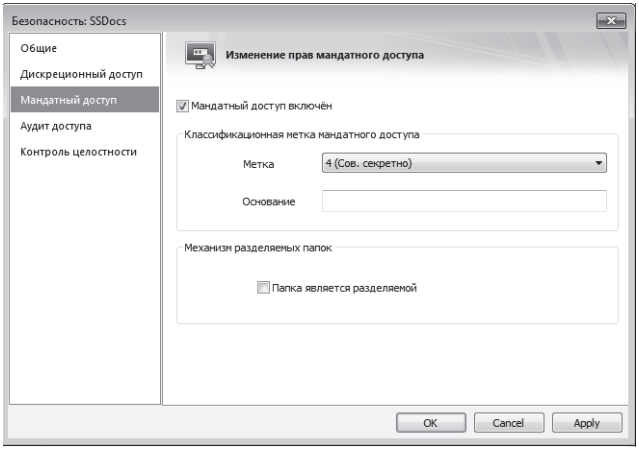

Рис. 14. Создание папки SSDocs

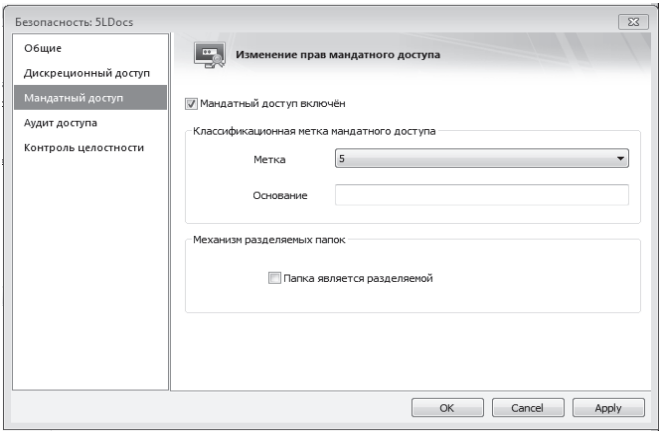

Рис. 15. Создание папки 5LDocs

Таким образом, оба пользователя имеют доступ к папкам Docs, PDocs и не имеют к SDocs, SSDocs, 5LDocs.

Шаг 3. Устанавливаем параметры согласно требованиям по классу 1Б.

Для шифрования информации необходимо выбрать в контекстном меню соответствующего файла или папки пункт «DL8.0: Закодировать».

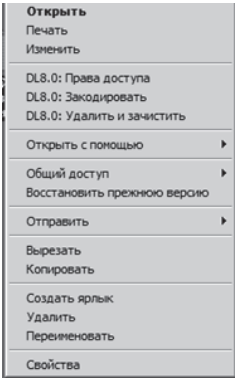

Рис. 16. Меню
для кодирования

На экране появится окно модуля преобразования объекта ФС, в котором необходимо указать данные и параметры

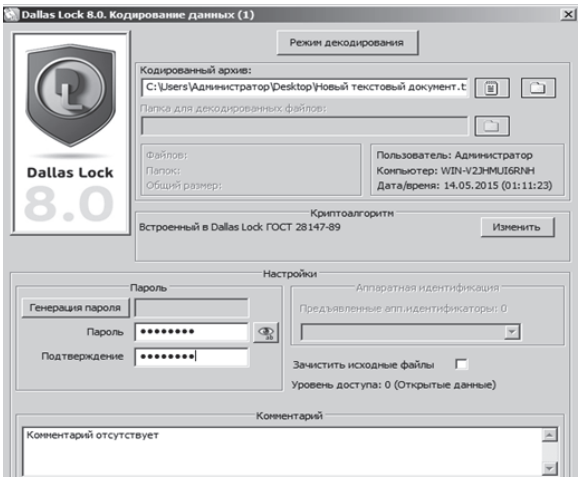

Рис. 17. Кодирование файла

Файл-контейнер с расширением *.dlcf появится в указанной папке.

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: Закодировать». Будущий файл-контейнер будет содержать все выбранные файлы. При этом имя и путь к будущему файлу-контейнеру будут по умолчанию состоять из имени первого из несколько выбранных файлов. Преобразование завершится сообщениями системы с указанием количества файлов.

Декодировать объект ФС можно, кликнув на него два раза, введя пароль, указав путь и нажав кнопку «Декодировать». Также при декодировании можно удалить и зачистить объект ФС.

Остальные параметры как у 1В (пункт 3, шаг 3).

Настроить для пользователей дискреционный доступ и параметры безопасности в соответствии с требованиями по классу 1Г с помощью «DallasLock 8.0-K» согласно матрице доступа:

Пользователь	**PDocs**	**SDocs**	**SSDocs**
User3	R--	RWX	---
User4	R--	---	RWX

Шаг 1. Создаем пользователей и папки.

Шаг 2. Для каждой папки устанавливаем дискреционный доступ для пользователей согласно матрице.

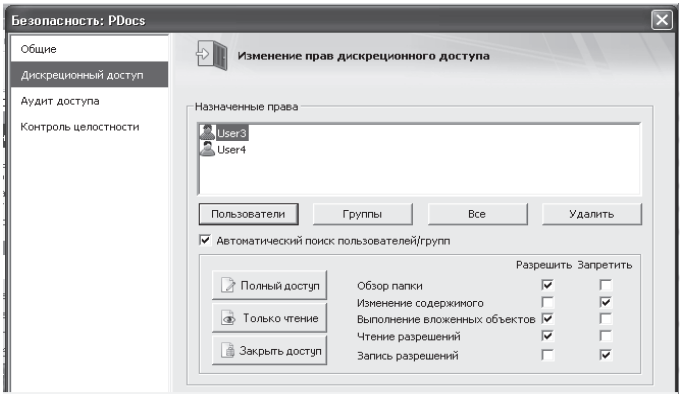

Рис. 18. Дискреционный доступ к PDocs для user3

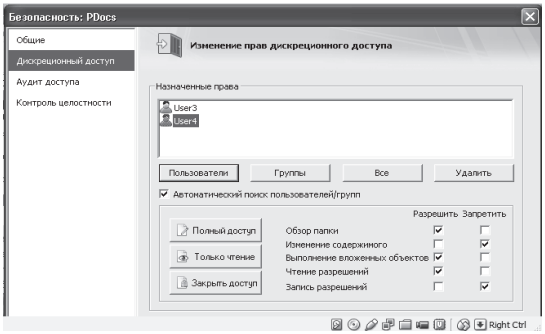

Рис. 19. Дискреционный доступ кPDocs для user4

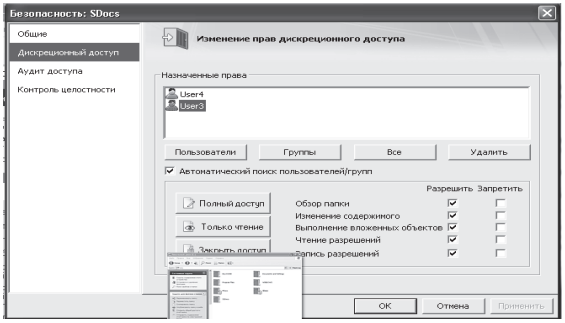

Рис. 20. Дискреционный доступ к SDocs для user3

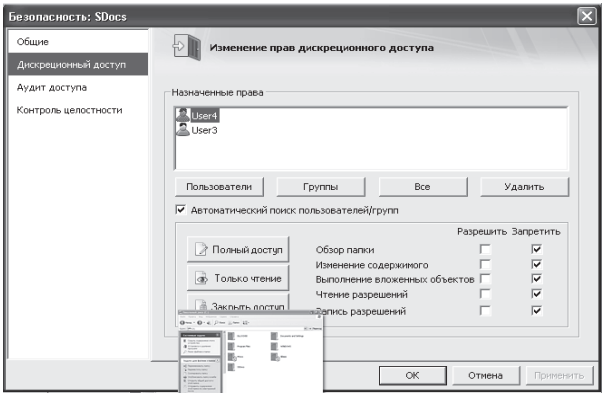

Рис. 21. Дискреционный доступ к SDocs для user4

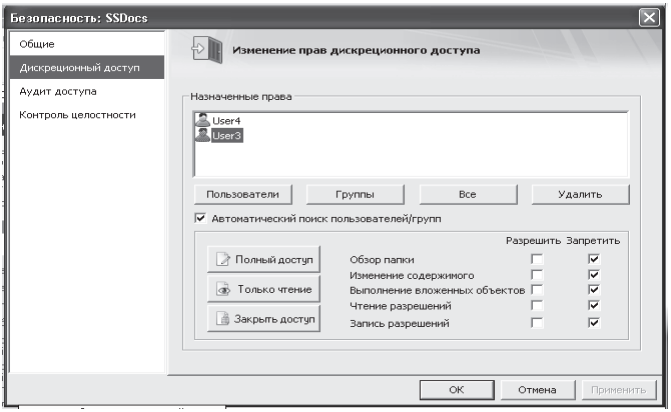

Рис. 22. Дискреционный доступ к SSDocs для user3

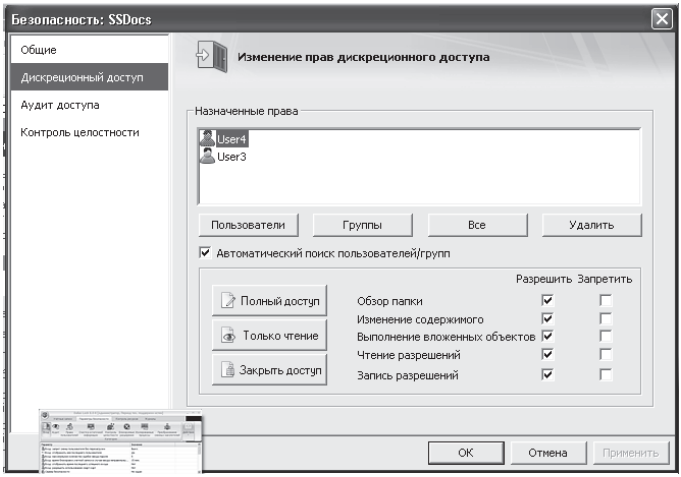

Рис. 23. Дискреционный доступ к SSDocs для user4

Шаг 3. Устанавливаем дискреционный доступ для пользователей для всех глобальных параметров.

Аналогично, как на рис. 24, – для остальных глобальных параметров.

Шаг 4. Устанавливаем параметры согласно требованиям по классу 1Г.

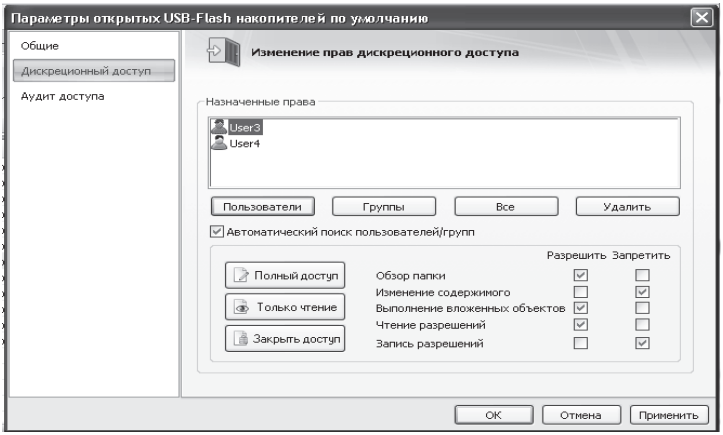

Рис. 24. Дискреционный доступ к USB-Flash
в глобальных параметрах накопителям для пользователей

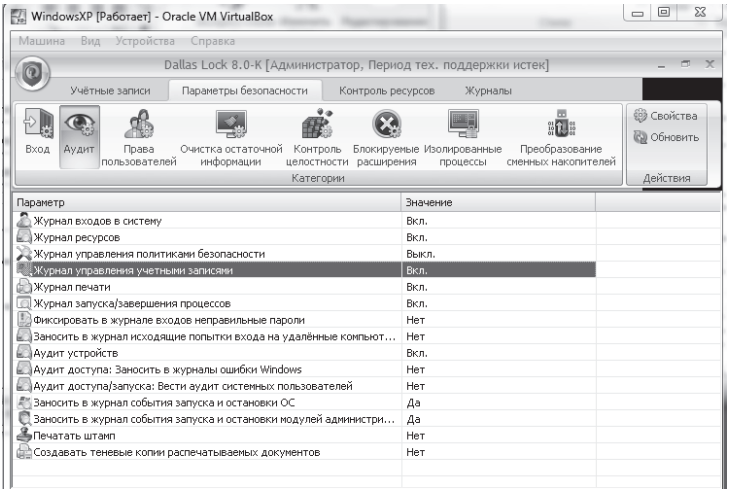

Рис. 25. Параметры регистрации и учета

Остальные параметры как у 1В (пункт 3, шаг 3).

Настроить для пользователей дискреционный доступ и параметры безопасности в соответствии с требованиями по классу 2Б с помощью «DallasLock 8.0-K» согласно матрице доступа:

Пользователь	**PDocs**	**SDocs**	**SSDocs**
User3	---	R--	RWX
User4	RWX	---	R--

Шаг 1. Создаем пользователей и папки.

Шаг 2. Для каждой папки устанавливаем дискреционный доступ для пользователей согласно матрице.

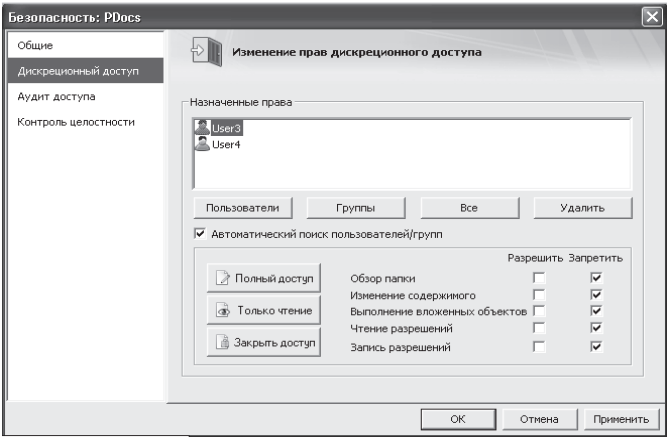

Рис. 26. Дискреционный доступ к PDocs для user3

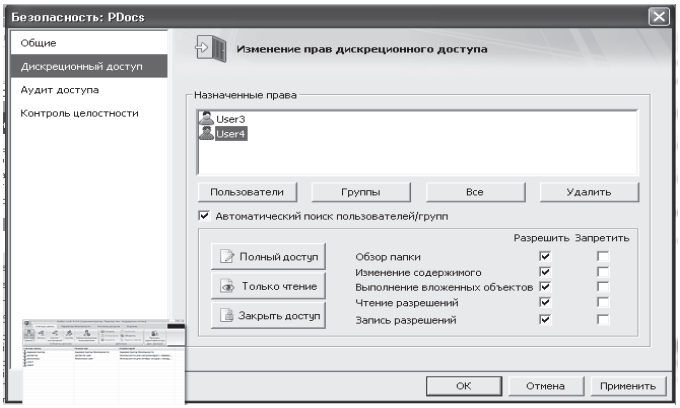

Рис. 27. Дискреционный доступ к PDocs для user4

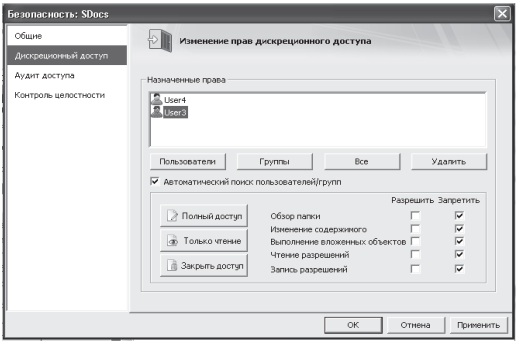

Рис. 28. Дискреционный доступ к SDocs для user3

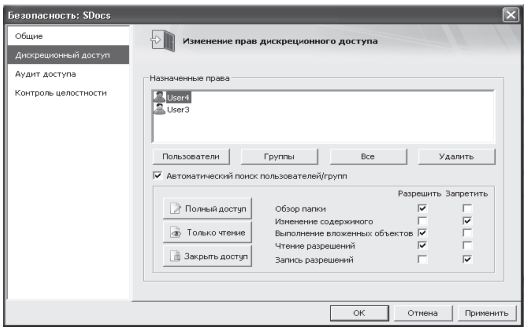

Рис. 29. Дискреционный доступ к SDocs для user4

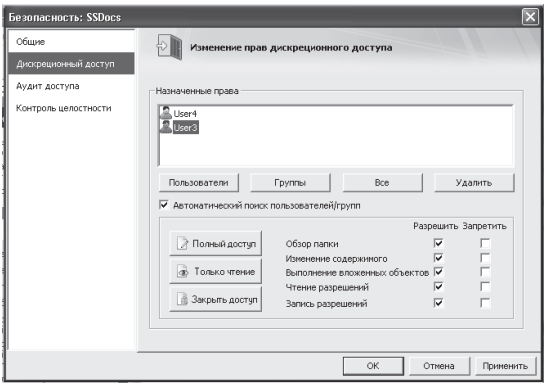

Рис. 30. Дискреционный доступ к SSDocs для user3

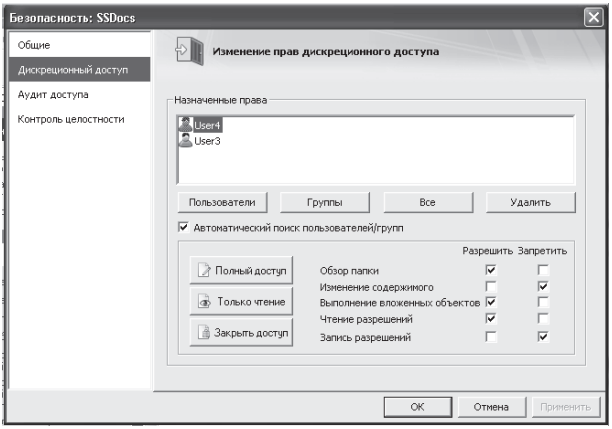

Рис. 31. Дискреционный доступ к SSDocs для user4

Шаг 3. Устанавливаем дискреционный доступ для пользователей для всех глобальных параметров.

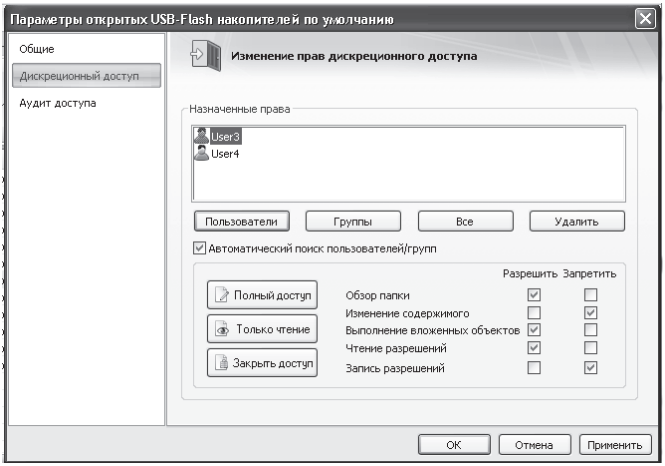

Рис. 32. Дискреционный доступ к USB-Flash в глобальных параметрах накопителям для пользователей

Аналогично, как на рис. 32, – для остальных глобальных параметров.

Шаг 4. Устанавливаем параметры согласно требованиям по классу 2Б.

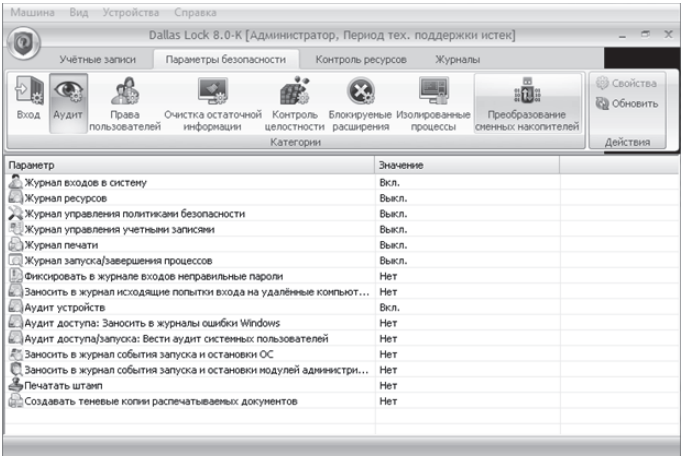

Рис. 33. Параметры подсистемы регистрации и учета для класса 2Б

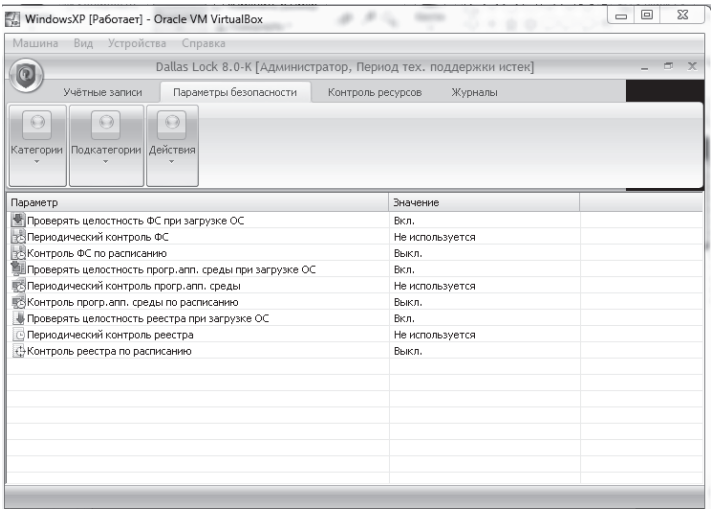

Рис. 34. Параметры подсистемы обеспечения целостности для класса 2Б

Периодическое тестирование СЗИ НСД и восстановление описаны в пункте 2, шаг 3.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Из каких подсистем состоит СЗИ НСД DallasLock 8.0-C?
2. Какие электронные идентификаторы позволяет использовать СЗИ НСД DallasLock 8.0-C?
3. Как реализован механизм мандатного управления доступом?
4. Какие виды отчетов можно получить в СЗИ НСД DallasLock 8.0-C?
5. Какие существуют механизмы защиты объектов?
6. Опишите способы восстановления системы защиты.

ЛАБОРАТОРНАЯ РАБОТА № 2

Цель работы

- Ознакомиться с консолью управления системой защиты информации DallasLock 8.0-C.
- Установить сервер безопасности, добавить в домен клиента и установить для пользователей группы клиента параметры безопасности согласно классу 1Г.

Ход работы

Шаг 1. Устанавливаем сервер безопасности, добавляем клиента XP в домен, создаем для него группу XPusers и выбираем пользователей XPuser1 и XPuser2, которые смогут на нем работать.

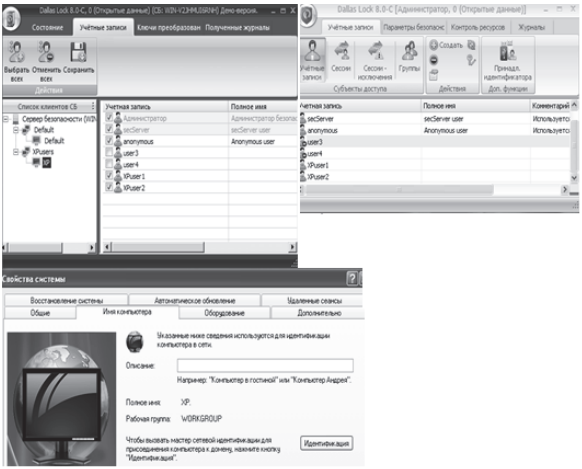

Рис. 37. Установка сервера безопасности, добавление клиента XP в домен безопасности

Шаг 2. Задаем группе XPusers параметры безопасности согласно классу 1Г, сохраняем их и затем синхронизируем.

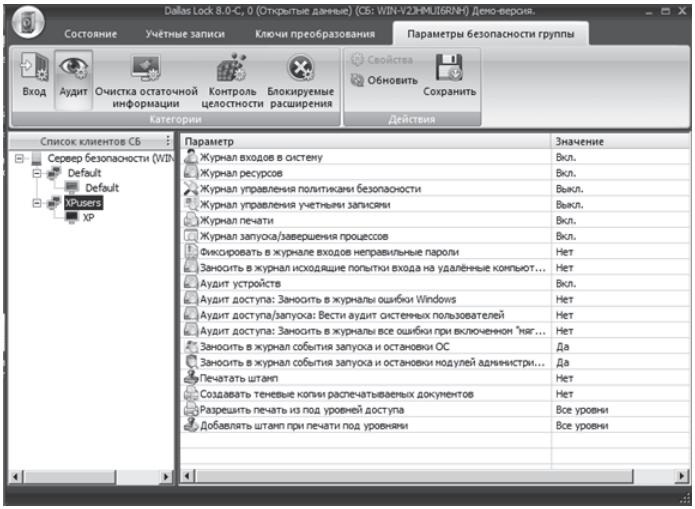

Рис. 39. Параметры подсистемы регистрации и учета для класса 1Г

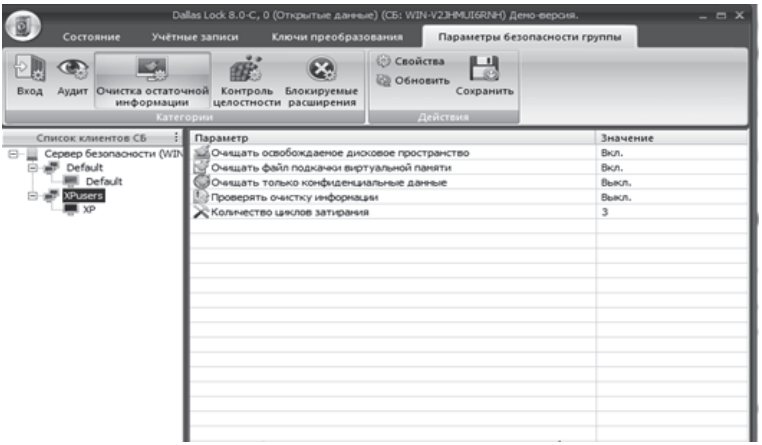

Рис. 40. Очистка освобождаемых областей для класса 1Г

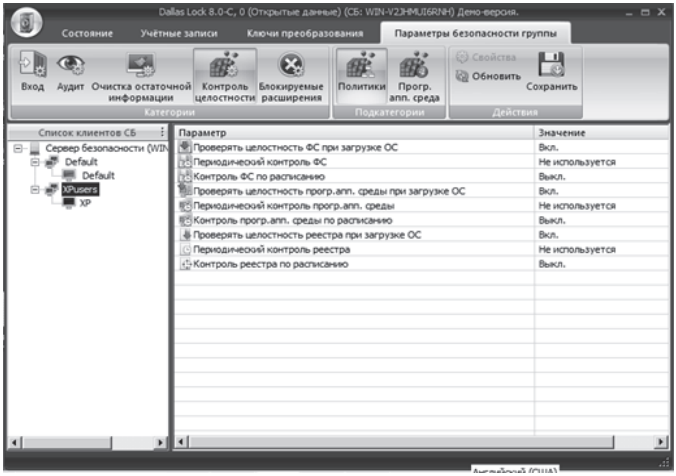

Рис. 41. Параметры подсистемы обеспечения целостности для класса 1Г

Периодическое тестирование СЗИ НСД и восстановление описаны в пункте 2, шаг 3.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Как реализован механизм дискреционного управления доступом?
2. Для чего необходим сервер безопасности СЗИ НСД DallasLock 8.0-C?
3. Какие параметры регистрации и учета можно настроить в СЗИ НСД DallasLock 8.0-C?
4. Где настраиваются параметры безопасности входа в АС с СЗИ НСД DallasLock 8.0-C?
5. Что такое «замкнутая программная среда»?
6. Возможно ли с сервера безопасности настроить локальные параметры безопасности пользователей?

СПИСОК ЛИТЕРАТУРЫ

1. http://www.dallaslock.ru
2. Система защиты информации от несанкционированного доступа Dallas Lock 8.0 – Руководство по эксплуатации – Ru.48957919.501410-02 92 – 2014. – 238 с.

Туманов Сергей Андреевич
Рева Иван Леонидович

**СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ
ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
НА ОСНОВЕ «DallasLock 8.0»**

Учебно-методическое пособие

В авторской редакции

Выпускающий редактор *И.П. Брованова*
Корректор *И.Е. Семенова*
Дизайн обложки *А.В. Ладыжская*
Компьютерная верстка *Н.В. Гаврилова*

Налоговая льгота – Общероссийский классификатор продукции
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

Подписано в печать 25.12.2015. Формат 60 × 84 1/16. Бумага офсетная
Тираж 50 экз. Уч.-изд. л. 3,25. Печ. л. 3,5. Изд. 295. Заказ № 138
Цена договорная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20