Лабораторная работа № 3. Системы обеспечения информационной безопасности от НСД. DallasLock.

* 1. **Назначение и возможности системы DALLAS LOCK 8.0-K**

1. **Общее описание системы**

Система защиты информации от несанкционированного доступа (Далее – СЗИ от НСД) «Dallas Lock 8.0-K» предназначена для защиты персонального компьютера:

* от доступа к информации в нарушение должностных полномочий сотрудников;
* от доступа к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения;
* от доступа к информации в объеме, превышающем необходимый для выполнения служебных обязанностей.

Использование СЗИ НСД Dallas Lock 8.0-K в проектах по защите информации ограниченного доступа (конфиденциальная информация, в том числе персональные данные) позволяет привести автоматизированные системы в соответствие требованиям законов Российской Федерации, стандартов и руководящих документов.

Система Dallas Lock 8.0-K представляет собой программный комплекс средств защиты информации в автоматизированных системах на базе персональных компьютеров.

СЗИ НСД Dallas Lock 8.0-K обеспечивает защиту информации от несанкционированного доступа на ПЭВМ в ЛВС через локальный, сетевой и терминальный входы. Также обеспечивает разграничение полномочий пользователей по доступу к файловой системе и другим ресурсам компьютера. Разграничения касаются всех пользователей – локальных, сетевых, доменных, терминальных.

В системе реализована возможность подключения современных аппаратных идентификаторов.

Система защиты может функционировать на автономных персональных компьютерах или на компьютерах в составе локальной вычислительной сети.

**1.2 1 Структура и составные модули**

Система защиты Dallas Lock 8.0-K состоит из следующих основных компонентов:

1. **Драйвер защиты.** Является ядром системы защиты и выполняет основныефункции СЗИ НСД. Обеспечивает дискреционный режим контроля доступа к объектам файловой системы. 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 файловой системы и компьютера. Драйвер осуществляет полную проверку правомочности и корректности администрирования СЗИ НСД, независимо от проверок, осуществляемых в подсистеме администрирования СЗИ НСД.
2. **Подсистема внедрения в интерфейс** *windows explorer*(«проводник»).

Обеспечивает отображение пунктов меню, нужных для настройки СЗИ НСД, в контекстном меню объектов файловой системы.

1. **Подсистема локального администрирования.** Обеспечивает все возможностипо управлению СЗИ НСД, аудиту и настройке системы, просмотру, фильтрации и очистке записей журналов.
2. **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 дискреционного доступа. Контроль доступа наименованных субъектов к наименованным объектам (файлам, программам, томам и т.д.). Для каждой пары субъект – объект задается перечисление допустимых прав;

подсистему аппаратной идентификации. Осуществляет работу с различными типами аппаратных идентификаторов.

**5. Подсистема регистрации и учета.** Включает:

подсистему аудита. Обеспечивает ведение и настройку 6-ти категорий событий;

подсистему зачистки остаточной информации.

1. **Подсистема обеспечения целостности.** Обеспечивает целостность программ иданных, периодическое тестирование СЗИ НСД, наличие средств восстановления СЗИ НСД.
2. **Подсистема преобразования информации.** Обеспечивает кодирование идекодирование данных в файлах-контейнерах.
3. **Подсистема централизованного управления.** Основные компоненты:

модуль «Сервер безопасности». Позволяет объединять защищенные компьютеры

* домен безопасности для централизованного управления; модуль «Менеджер серверов безопасности». Позволяет объединить несколько

Серверов безопасности в единую логическую единицу «Лес безопасности». С помощью этого модуля становиться возможным централизованный сбор журналов со всех Серверов безопасности и применение политик.

**1.3 Возможности**

Система защиты информации Dallas Lock 8.0-K предоставляет следующие возможности:

1. СЗИ НСД Dallas Lock 8.0-K запрещает посторонним лицам доступ к ресурсам ПЭВМ 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 объектам файловой системы, доступ к сети, сменным накопителям, аппаратным ресурсам. Для облегчения администрирования возможно объединение пользователей в группы. Контролируются права доступа для локальных, доменных, сетевых и терминальных пользователей.
2. Система Dallas Lock 8.0-K позволяет в качестве средства опознавания пользователей системы использовать электронные идентификаторы:

USB-Flash-накопители;

электронные ключи Touch Memory (iButton); USB-ключи Aladdin eToken Pro/Java;

смарт-карты Aladdin eToken Pro/SC;

USB-ключи Rutoken (Рутокен) и Rutoken ЭЦП.

1. Для решения проблемы «простых паролей» система имеет гибкие настройки сложности паролей. Можно задать минимальную длину пароля, необходимость обязательного наличия в пароле цифр, специальных символов, строчных и прописных букв, степень отличия нового пароля от старого.
2. Используется дискреционный принцип контроля доступа. Он обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) 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 (открытие, запись, чтение, удаление, переименование, запуск, копирование).
3. Возможно ограничение круга доступных для пользователя объектов файловой системы (дисков, папок и файлов под FAT и NTFS). Применяется полностью независимый от ОС механизм.
4. В СЗИ НСД Dallas Lock 8.0-K реализована система контроля целостности параметров компьютера. Она обеспечивает:

контроль целостности программно-аппаратной среды при загрузке компьютера; контроль целостности файлов при загрузке компьютера; контроль целостности ресурсов файловой системы и программно-аппаратной

среды по расписанию;

контроль целостности ресурсов файловой системы и программно-аппаратной среды через заданные интервалы времени (периодический контроль);

блокировку загрузки компьютера при выявлении изменений.

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

* 1. СЗИ НСД Dallas Lock 8.0-K включает подсистему очистки остаточной информации, которая гарантирует предотвращение восстановления удаленных данных. Подсистема позволяет:

принудительно зачищать определенные файлы и папки, используя соответствующий пункт в контекстном меню проводника (windows explorer);

с помощью политики «Запрет смены пользователя без перезагрузки», можно предотвращать возможность завершения сеанса работы одного пользователя и начала работы другого (это гарантирует освобождение используемых областей оперативной памяти).

* 1. В СЗИ НСД Dallas Lock 8.0-K реализовано ведение 6 электронных журналов, в которых фиксируются действия пользователей:

журнал входов. В журнал заносятся все входы (или попытки входов с указанием причины отказа) и выходы пользователей ПЭВМ, включая как локальные, так и сетевые, в том числе терминальные входы и входы для удаленного администрирования;

журнал доступа к ресурсам. В журнал заносятся обращения к объектам файловой системы, для которых назначен аудит. Можно гибко настраивать для каждого объекта, какие события нужно заносить в журнал, а какие нет;

журнал запуска процессов. В журнал заносятся события запуска и завершения процессов;

журнал управления политиками безопасности. В журнал заносятся все события связанные с изменением конфигурации СЗИ НСД. Так же в этот журнал заносятся события запуска/завершения модулей администрирования и события запуска/завершения работы системы;

журнал управления учетными записями. В журнал заносятся все события связанные с созданием или удалением пользователей, изменением их параметров;

журнал печати. В журнал заносятся все события, связанные с распечаткой документов на локальных или сетевых принтерах.

Для облегчения работы с журналами есть возможность фильтрации записей по определенному признаку и экспортирования журналов в различные форматы. При переполнении журнала, его содержимое автоматически компрессируется и помещается в специальную папку, доступ к которой есть, в том числе, и через средства удаленного администрирования. Этим обеспечивается непрерывность ведения журналов.

* 1. Для защиты данных при хранении их на внешних носителях либо при передаче по различным каналам связи есть возможность преобразования данных в файл-контейнер.
* качестве ключа преобразования используется пароль и по желанию пользователя, аппаратный идентификатор. Распаковать такой контейнер можно на любом компьютере, защищенном Dallas Lock 7.7 или Dallas Lock 8.0-K, при условии знания пароля и наличии аппаратного идентификатора, используемых при преобразовании. Возможно использование встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, например, сертифицированного «КриптоПро».
  1. Для предотвращения утечки информации с использованием сменных накопителей (таких как USB-Flash Drive, дискета, внешний жесткий диск и прочие) система позволяет разграничивать доступ, как к отдельным типам накопителей, так и к конкретным экземплярам.
  2. Система позволяет настраивать «Замкнутую программную среду» (режим, в котором пользователь может запускать только программы, определенные администратором).

* 1. Возможно использование СЗИ НСД Dallas Lock 8.0-K на ноутбуках, виртуальных машинах, серверах (файловых, терминального доступа, контроллерах домена
* т.д.).
  1. При использовании нескольких защищенных СЗИ НСД Dallas Lock 8.0-K компьютеров в ЛВС возможно удаленное администрирование. Средствами удаленного администрирования осуществляется изменение политик безопасности, создание и удаление пользователей, назначение прав доступа к объектам файловой системы, просмотр журналов и управление аудитом и контролем целостности. Процесс удаленного администрирования визуально не отличается от локального администрирования. Модуль удаленного администрирования входит в состав всех поставок, его не требуется приобретать отдельно.
  2. При использовании нескольких защищенных СЗИ НСД Dallas Lock 8.0-K компьютеров в ЛВС возможно централизованное управление ими. Это осуществляется с использованием специального модуля – «Сервер безопасности Dallas Lock». Этот модуль должен быть установлен на отдельный компьютер, защищенный СЗИ НСД Dallas Lock 8.0-К. Остальные компьютеры, введенные под контроль данного Сервера безопасности, станут его клиентами и образуют домен безопасности. С Сервера безопасности станет возможным централизованное управление политиками безопасности, просмотр состояния, автоматический сбор журналов, создание/удаление/редактирование параметров пользователей и другие операции по настройке и управлению клиентами. Кроме того, с помощью модуля «Менеджер серверов безопасности Dallas Lock» есть возможность объединить несколько серверов безопасности в «Лес безопасности» (ЛБ).
  3. СЗИ НСД Dallas Lock 8.0-K содержит подсистему самодиагностики основного функционала СЗИ НСД.
  4. Для удобства администрирования системы, 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 прочие.).
  5. Для проверки соответствия настроек СЗИ НСД есть возможность создания отчетов по назначенным правам и конфигурациям на объекты файловой системы. Данный механизм содержит настройки для выбора типа отчета, параметров необходимых ресурсов, параметров сортировки. Данный отчет может быть создан по завершению настройки СЗИ НСД и, впоследствии, результаты этого отчета могут быть сверены с текущими настройками СЗИ НСД в любой момент, путем сверки сохраненной версии отчета и создания отчета в момент проведения проверки.
  6. Предусматривается ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности.
  7. Для ускорения внедрения СЗИ НСД Dallas Lock 8.0-K в крупных сетях может использоваться механизм удаленной установки средствами cервера безопасности или средствами групповых политик Active Directory.
  8. Для облегчения настройки таких возможностей, как «Замкнутая программная среда» существует «мягкий режим» – режим, при работе в котором при обращении к ресурсу, доступ к которому запрещен, доступ все равно разрешается, но в журнал доступа заносится сообщение об ошибке.

**Задания к лабораторной работе №3**

1. Настроить политику аудита для 2 пользователей, параметры взять у преподавателя.

2. Просмотреть и сохранить журналы аудита. Настроить фильтр на просмотр событий текущей недели, месяца, года.

3. Произвести предоставление полномочий некоторого пользователя другому пользователю, используя функционал Dallas Lock.

4. Настроить контроль целостности для жесткого диска, USB-устройства, папки, файла. Для расчета контрольных сумм использовать встроенные алгоритмы.

5. Удалить и очистить с помощью Dallas Lock информацию о сохраненных журналах.

6. Настроить запрет смены пользователей без перезагрузки.

7. Создать папки, файлы, зашифровать их, используя встроенные криптоалгоритмы.

8. Заблокировать для различных групп пользователей работу с mp3, mpeg, docx, djvu.

9. Создать отчет о правах и конфигурациях Dallas Lock

10. Создать резервную копию файлов СЗИ от НСД Dallas Lock.

11. Протестировать функционал Dallas Lock.