Лабораторная работа № 3

ИЗУЧЕНИЕ ОСНОВНЫХ ВОЗМОЖНОСТЕЙ, А ТАК ЖЕ ПРОЦЕССА УСТАНОВКИ И НАСТРОЙКИ АППАРАТНОЙ ЧАСТИ ПРОГРАММНО АППАРАТНОГО КОМПЛЕКСА (ПАК) ЗАЩИТЫ ИНФОРМАЦИИ DALLAS LOCK 8.0

1. Цель и задачи работы

Ознакомится с назначением, основными характеристиками программно-аппаратного комплекса (ПАК) Dallas Lock (DL) 8.0, получить навыки по установке программно-аппаратных средств комплекса.

2. Теоретические положения

Dallas Lock 8.0 [3] представляет собой программно-аппаратную систему защиты персонального компьютера. Система предназначена для исключения несанкционированного доступа к ресурсам компьютера. Для идентификации и аутентификации пользователей используются электронные карты Touch Memory или Proximity.

Dallas Lock 8.0 - это система, обеспечивающая защиту информации на технических средствах, работающих под управлением ОС Windows версии начиная с Windows XP (SP 3) и заканчивая Windows 10, аппаратные интерфейсы которого, позволяют подключить данный комплекс. Данное средство защиты информации соответствует следующим НТД.

«Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности; – «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 3 классу защищенности; – «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля; – «Требования к системам обнаружения вторжений» (документ утвержден приказом ФСТЭК России № 638 от 6 декабря 2011 г.) – по 4 классу защищенности; – «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ; – «Требования к средствам контроля съемных машинных носителей информации» (документ утвержден приказом ФСТЭК России № 87 от 28 июля 2014 г.) – по 4 классу защищенности; Описание применения СЗИ НСД Dallas Lock 8.0-К 6 – «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ; – «Профиль защиты средств контроля отчуждения (переноса) информации со

съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.Н4.ПЗ.

В состав СЗИ входят следующие подсистемы:

– подсистема управления доступом;

– подсистема контроля устройств;

– подсистема преобразования информации;

– подсистема гарантированной зачистки информации;

– подсистема идентификации и аутентификации;

– подсистема регистрации и учёта;

– подсистема администрирования (локального, удаленного и централизованного управления); – подсистема контроля целостности;

– подсистема восстановления после сбоев;

– подсистема межсетевого экранирования;

– подсистема обнаружения вторжений;

– подсистема развертывания

Модули статического шифрования и модуль шифрования данных на дискетах предназначены соответственно для защиты данных пользователя, хранящихся на логических дисках "винчестера" и дискетах. Генерация шифровальных ключей осуществляется на основании личных паролей и электронных карт.

Технические характеристики комплекса

Система запрещает посторонним лицам доступ к ресурсам компьютера.

В качестве средства опознавания пользователей служат электронные идентификаторы Touch Memory фирмы "Dallas Semiconductor Inc." (США) или карты Proximity фирмы HID corporation. Данные приборы имеют малые размеры, очень удобны в применении и надежны в работе.

Благодаря гарантированной неповторяемости ключа, скрытого в идентификаторе, реализован весьма высокий уровень защиты. Число уникальных 48-битовых ключей составляет более 280 триллионов.

Запрос идентификатора при входе на ПЭВМ инициируется из ПЗУ на плате защиты до загрузки операционной системы. Загрузка операционной системы с жесткого диска осуществляется только после предъявления зарегистрированного идентификатора (электронной карты). Поскольку идентификатор запрашивается до обращения к дисководам, возможность загрузки с системной дискеты полностью исключается.

Предусмотрена возможность блокировки клавиатуры во время загрузки компьютера. При этом загрузка предыдущей версии DOS становится невозможной.

Модуль входа в Windows позволяет заменить стандартную процедуру идентификации при входе в систему (ввод имени и пароля) идентификацией по электронной карте.

Перед инсталляцией системы на жесткий диск возможна гибкая настройка аппаратной части путем предварительного выбора адресного пространства ПЗУ

платы защиты в свободной области адресов пользовательских ПЗУ, а также адресов портов для работы с электронной картой.

В системе поддерживается работа до 32 зарегистрированных пользователей на каждом защищенном компьютере. Один пользователь может быть зарегистрирован на нескольких ПЭВМ с разными полномочиями. Данные о пользователях хранятся в энергонезависимой памяти на плате защиты.

Обеспечивается ограничение доступа ПОЛЬЗОВАТЕЛЕЙ к компьютеру по времени. Время начала и окончания работы каждого ПОЛЬЗОВАТЕЛЯ на компьютере устанавливается администратором в пределах суток. Интервал времени, в течение которого ПОЛЬЗОВАТЕЛЬ может входить на компьютер со своими правами, может быть установлен от 1 минуты до 23 час. 59 минут (т.е. круглосуточно).

Обеспечено гибкое разграничение доступа ПОЛЬЗОВАТЕЛЯ к файлам и папкам системы. Поддерживаются мандатный и дискреционный способы разграничения доступа. Существует режим защиты уровня секретности данных.

Гарантированное удаление информации обеспечивается при использовании специального инструмента Secure File Deletion. Его функции подобны стандартному инструменту Windows ("Корзина"), но информация, удаляемая с дисков компьютера при помощи Secure File Deletion, затирается нулевым кодом.

При выполнении процедуры входа на компьютер система анализирует электронную карту и личный пароль пользователя. Если произошел отказ в доступе, то данное событие заносится в специальный электронный журнал, при этом фиксируется номер предъявленной карты, имя пользователя, дата и время попытки входа. Ведутся также журналы событий, печати и успешных входов. Электронные журналы доступны только АДМИНИСТРАТОРУ.

Пользователи могут самостоятельно менять личные пароли для входа на компьютер.

Все действия администратора по изменению прав пользователей заносятся в специальный журнал.

Существует возможность временной блокировки компьютера пользователем (например, если ему необходимо ненадолго отлучиться). Блокировка выполняется вручную с помощью стандартной панели безопасности Windows (панель доступна по комбинации клавиш [Ctrl-Alt-Del]). Разблокировка и дальнейшая работа с компьютером возможна только после предъявления электронной карты пользователя, который загружал компьютер последним.

Для усиления защиты конфиденциальной информации, хранящейся на "винчестере" и дискетах пользователей, предусмотрены модули шифрования, работающие в статическом или "прозрачном" режимах. Данные могут шифроваться с использованием нескольких алгоритмов - по выбору пользователя. Шифровальный ключ может формироваться на основе личного пароля или кода личного идентификатора. В "прозрачном" режиме информация шифруется при записи и расшифровывается при чтении со сменного носителя. При этом процесс шифрования незаметен для пользователя.

Модули контроля целостности объектов компьютера обеспечивают:

- контроль изменения файлов пользователя;
- контроль изменения энергонезависимой памяти платы защиты;
- обнаружение создания новых файлов.

Дополнительные сервисные функции предоставляет модуль «Картотека», позволяющий вести учет выданных пользователям электронных карт, а также хранить некоторые данные о самих пользователях.

Системные требования

Система защиты Dallas Lock 8.0 поддерживает 32- и 64-битные версии ОС Windows. Система защиты Dallas Lock 8.0 позволяет защищать информационные ресурсы рабочего пространства Windows To Go операционной системы Windows 8 и Windows 10 на USB - накопителе. Минимальная и оптимальная конфигурация ПК определяется требованиями к версии операционной системы Windows, на которую установлена система защиты Dallas Lock 8.0. Для размещения файлов системы и ее работы требуется не менее 30 Мбайт пространства на системном разделе жесткого диска. Для использования Dallas Lock 8.0 на компьютере в составе ЛВС необходимо настроить сетевой протокол TCP/IP. Для использования аппаратных идентификаторов требуется наличие в аппаратной части ПК соответствующих портов: USB-порта или COM-порта..

Комплект поставки

Программно-аппаратный комплекс Dallas Lock 8.0 поставляется в следующем комплекте:

- диск с программным обеспечением;
- мастер-карта;
- документация по инсталляции и работе с системой: "Руководство администратора";
- набор плат и считывателей (по количеству защищаемых компьютеров).

Установка СЗИ Dallas Lock 8.0

1. Для установки СЗИ НСД Dallas Lock 8.0 необходимо запустить приложение DallasLock8.0C.msi (DallasLock8.0K.msi), которое находится в корневой директории дистрибутива (или выбрать данное действие в меню окна autorun). Если Dallas Lock 8.0 устанавливается на ПК, не оснащенный приводом компакт дисков, а дистрибутив поставляется именно на CD-диске, то можно скопировать с инсталляционного диска на данный ПК необходимый msi-файл любым удобным способом: через ЛВС, USB Flash-накопитель и др.

После запуска программы установки необходимо выполнять действия по подсказкам программы. На каждом шаге инсталляции предоставляется возможность отмены инсталляции с возвратом сделанных изменений. Для этого служит кнопка «Отмена». Выполнение следующего шага инсталляции выполняется с помощью кнопки «Далее».

2. При установке системы защиты на компьютере с установленной ОС Vista и выше после запуска приложения, на экране будет выведено окно для подтверждения операции (рис. 1).

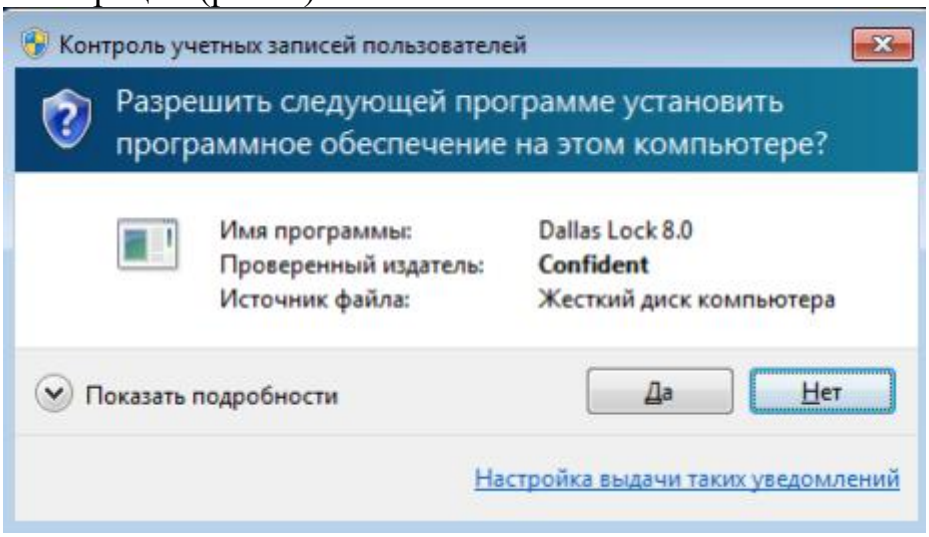

Рис.1. Разрешение на установку программы в ОС

После подтверждения запустится программа установки СЗИ НСД Dallas Lock 8.0 (рис. 2).

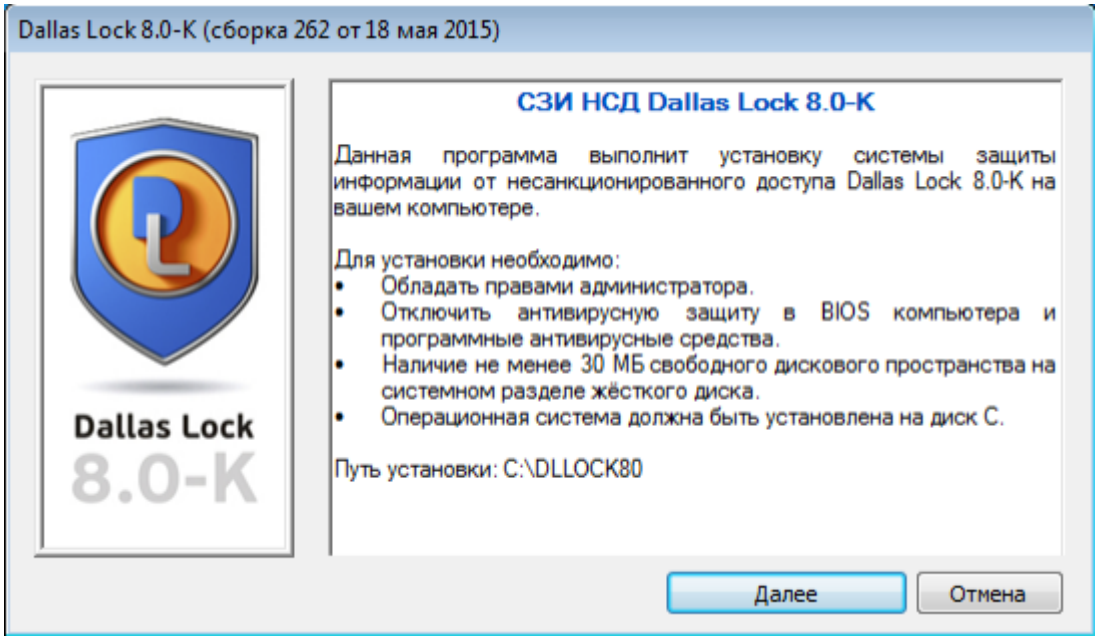

Рис. 2. Окно установки СЗИ

3. Для установки необходимо нажать кнопку «Далее», после чего программа установки приступит к инсталляции. На данном этапе программа установки попросит осуществить ввод параметров установки (рис. 3).

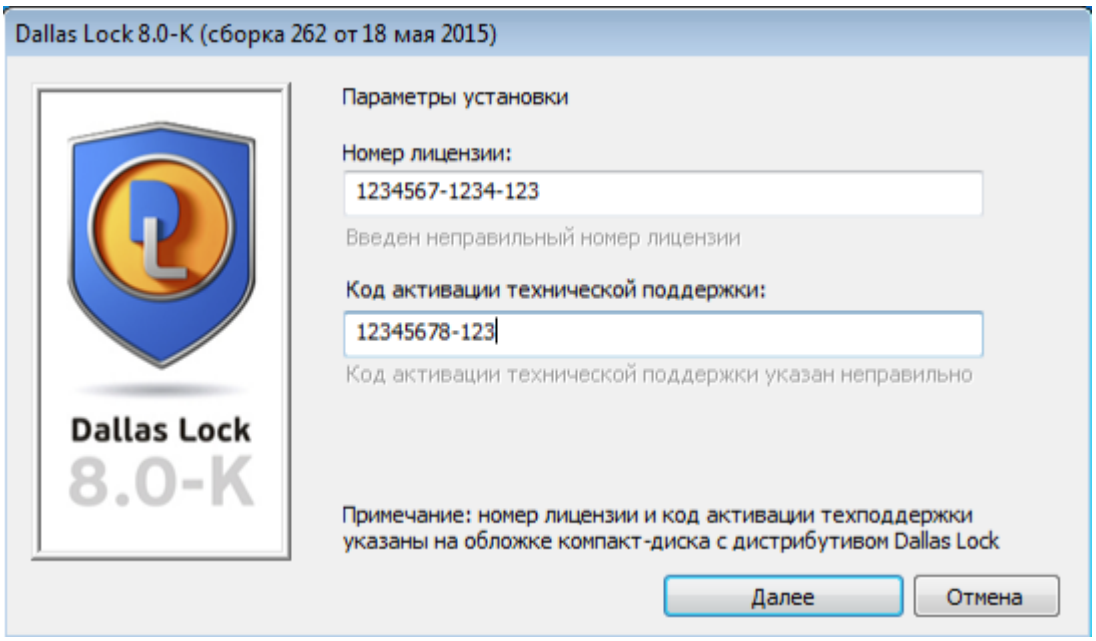

Рис. 3. Ввод параметров СЗИ

4. Для защиты от нелегального использования продукта необходимо ввести номер лицензии Dallas Lock 8.0 и код технической поддержки, которые указаны на обложке компакт-диска с дистрибутивом в соответствующих полях. Следует обратить внимание, что номер лицензии может либо активировать модуль «Межсетевой экран», либо оставлять его неактивным (в зависимости от приобретенного изделия). После этого необходимо нажать кнопку «Далее».

5. В том случае, когда необходимо ввести компьютер в Домен безопасности в процессе установки системы, то в соответствующие поля необходимо ввести имя Сервера безопасности и его ключ доступа. Если этого не сделать на этапе установки, то компьютер не будет введен в Домен безопасности, но это можно будет сделать и после установки СЗИ НСД.

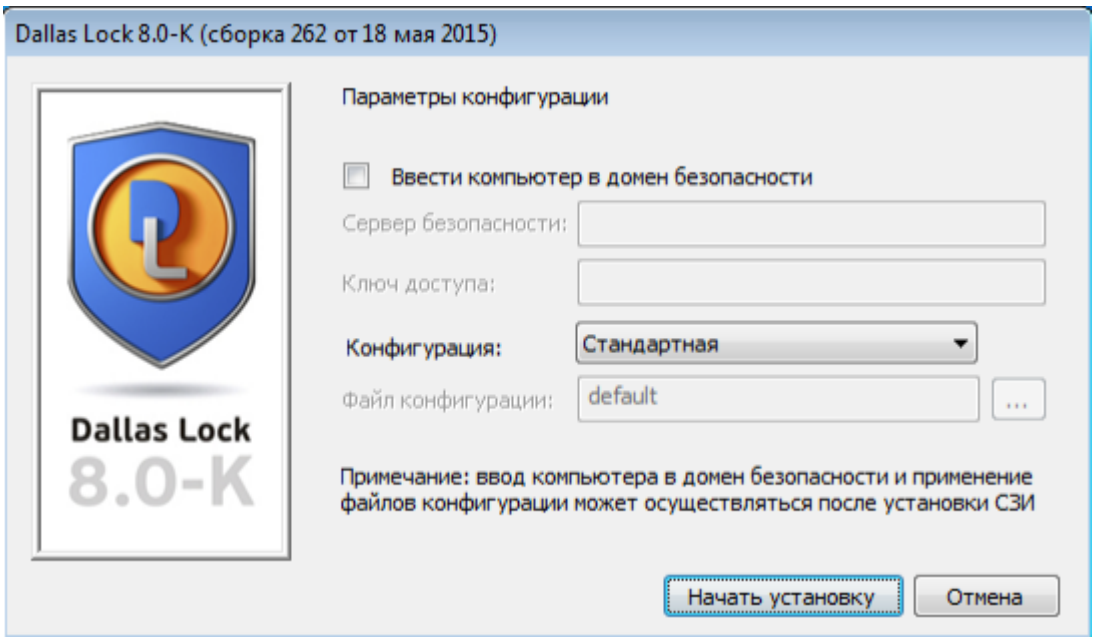

Рис.4. Введение в домен безопасности на этапе установки

6. Указать, если требуется, файл конфигурации, для этого нажать кнопку поиска рядом с полем ввода и в появившемся окне проводник выбрать заранее сохраненный файл.

7. После нажатия кнопки «Далее» процесс установки системы защиты будет завершен. После нажатия кнопки «Перезагрузка» через 30 секунд произойдет автоматическая перезагрузка ПК (рис. 5).

Рис.5. Завершение установки СЗИ

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

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

После установки системы защиты и перезагрузки компьютера в меню «Пуск» появится ярлык оболочки администратора СЗИ НСД Dallas Lock 8.0.

3. Оборудование

Персональный компьютер, работающий под управлением операционной системы Windows, версия которой поддерживается Dallas Lock 8.0; Workstation, плата защиты КТ-33X, комплект установочных дисков DL 8.0, считыватель электронных карт, мастер-карта.

4. Задание на работу

4.1 Ознакомиться с назначением, основными характеристиками и системными требованиями для установки ПАК DL 8.0.

4.2 Под руководством преподавателя произвести установку и настройку аппаратной части ПАК.

5. Порядок выполнения работы

5.1 Ознакомиться с теоретическими сведениями или руководством администратора ПАК DL 8.0.

5.2 Убедиться в соответствии ПЭВМ системным требованиям, предъявляемым для установки ПАК (наличие порта USB, соответствующих адресов в пространстве ввода/вывода, установленной ОС Windows
5.3 Подключить считыватель карт Touch Memory.
5.4 Воспользовавшись установочным диском №1 и мастер-картой, или информацией о лицензионном ключе и компании - правообладателе лицензии из установочного комплекта выполнить инсталляцию программ, обеспечивающих работу платы защиты. Убедиться в отсутствии ошибок.
5.5 Произвести установку СЗИ Dallas Lock 8.0 в соответствии с инструкцией по установке.

6. Оформление отчета

Отчет оформляется в тетради или листах формата А4 и должен содержать:
- название курса, название и номер лабораторной работы;
- цель работы и задание на исследование;
- характеристики ПАК Dallas Lock 8.0;
- данные по настройке адресов на плате КТ;
- код активации и номер лицензии для установки ПАК;
- порядок инсталляции аппаратной части комплекса;
- виды (скриншоты) окон мастера установки СЗИ.

7. Контрольные вопросы

7.1 Каково назначение ПАК Dallas Lock 8.0?
7.2 Какие аппаратные компоненты входят в ПАК Dallas Lock 8.0?
7.3 Какую информацию содержит карта Touch Memory?
7.4 Какие требования предъявляются к аппаратной части компьютера для установки ПАК?
7.5 Расскажите о функциях, выполняемых платой защиты серии КТ.
7.6 Каков порядок установки аппаратных компонентов ПАК Dallas Lock 8.0?
7.7Каков порядок установки программных компонентов ПАК.