ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ «ВОРОБЬЁВЫ ГОРЫ»
ОТДЕЛЕНИЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ КОЛЛЕДЖ ПРОФЕССИОНАЛЬНЫХ ТЕХНОЛОГИЙ»

КУРСОВАЯ РАБОТА

Тема: «Программные способы организации защиты данных в корпоративных информационных системах»

Студента 2 Курса Группы ИС-21
Дневной формы обучения
Специальности 09.02.04
Информационные системы(по отраслям)
Замула Ярослав Дмитриевич
Руководитель КР: Постовой Николай Гаврилович

Москва,2018

Актуальность

С каждым годом растёт количество и качество возможно опасных и вредоносных программ. В связи с этим возникает потребность в постоянно улучшающихся и модернизирующихся средствах защиты.

Цель исследования

Выявление программных способов организации защиты данных в корпоративных информационных системах.

Объект исследования

Программы для защиты данных(4systems)

Предмет исследования

Совокупность инженерно-технических Dallas Lock 8.0-С

Гипотеза

Гипотеза: Защита корпоративных данных будет осуществляться эффективно при наличии правильно установленной системы защиты Dallas Lock 8.0-С.

Задача исследования :

Обнаружение угрозы защиты

8.0-С.

Цель теоретического исследования

Выявление угроз и последующие устранение проблем безопасности.

Методы исследования

Анализ научной литературы, систематизация и интеграция теоретических знаний и практических навыков.

Как понять что в сети находится посторонний?

Определить, что сервер подвергается атаке злоумышленников возможно, это будет видно по следующим признакам:

- Нестабильная работа, блокировка VPS.
- Отсутствует доступ к root или правам пользователя.
- Существенное увеличение трафика на сервере.
- Появление следов рассылки спама с VPS.
- Неестественная сетевая активность.

Обнаружение причин, которые способствовали взлому сервера:

- Несоответствующая конфигурация программного обеспечения (ПО) сервера.
- Некачественно придуманные или утерянные пароли для root-доступа.
- Уязвимое (не обновленное) ПО.

Способы защиты данных

Программные средства защиты

Аппаратные средства защиты

Основные возможности СЗИ от НСД Dallas Lock 8.0-C:

- Запрет/разрешение последовательных и параллельных портов
- возможность блокировки файлов по расширению
- наличие функций автоматизации создания замкнутой программной среды (режим обучения, мягкий режим);деленным типам накопителей информации)
- гарантированная очистка остаточной информации с возможностью выбора количества циклов затирания
- система контроля целостности параметров компьютера

Общее описание Dallas Lock 8.0

TESSIS КОНФИДЕНТ

Сертификат совместимости

SafeNet eToken – Dallas Lock 8.0

Настоящим сертификатом компании ЗАО «Сертифицированные информационные системы» и ООО «Конфидент» подтверждают корректность совместной работы электронных ключей SafeNet eToken с системой защиты информации Dallas Lock 8.0 редакций «К» и «С».

Сертификат подготовлен на основании результатов испытаний, проведенных компаниями ЗАО «Сертифицированные информационные системы» и ООО «Конфидент».

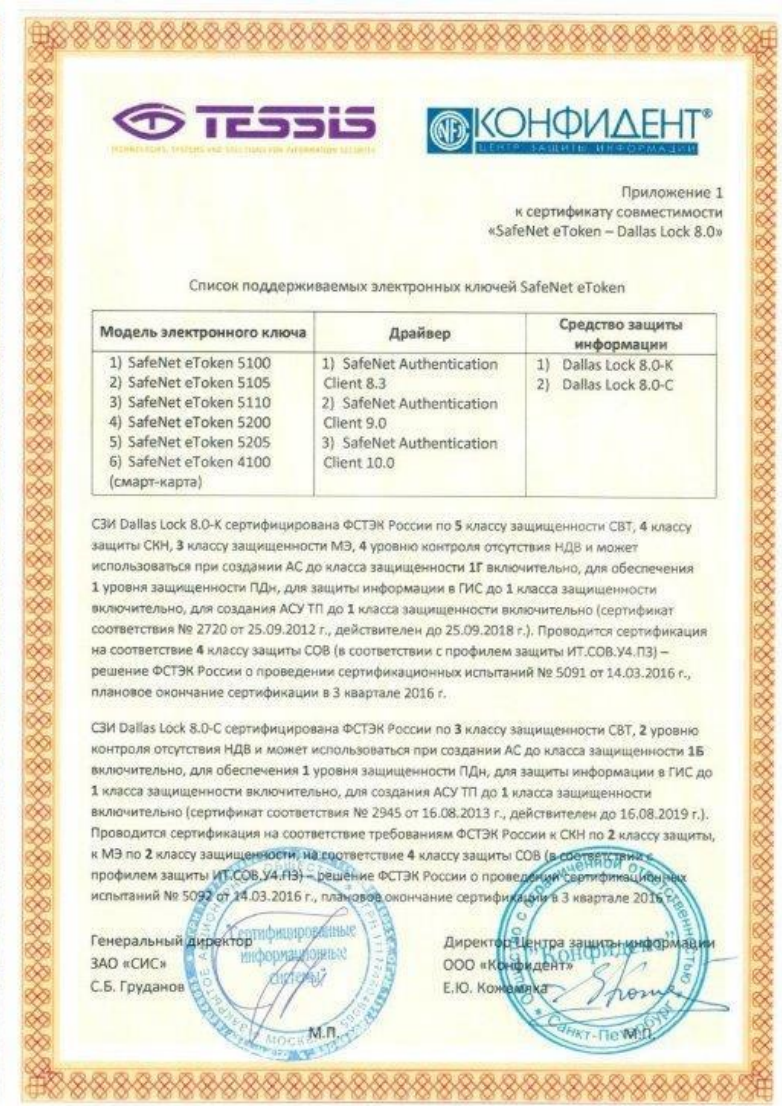
Таблица совместимости электронных ключей SafeNet eToken с «Dallas Lock» приведена в Приложении 1 к настоящему сертификату.

Дата: 12.08.2016

№ЮС-0008

Генеральный директор
ЗАО «СИС»
С.Б. Груданов
М.П.

Директор Центра защиты информации
ООО «Конфидент»
Е.Ю. Кожемяка
М.П.



TESSIS КОНФИДЕНТ

Приложение 1
к сертификату совместимости
«SafeNet eToken – Dallas Lock 8.0»

Список поддерживаемых электронных ключей SafeNet eToken

Модель электронного ключа	Драйвер	Средство защиты информации
1) SafeNet eToken 5100 2) SafeNet eToken 5105 3) SafeNet eToken 5110 4) SafeNet eToken 5200 5) SafeNet eToken 5205 6) SafeNet eToken 4100 (смарт-карта)	1) SafeNet Authentication Client 8.3 2) SafeNet Authentication Client 9.0 3) SafeNet Authentication Client 10.0	1) Dallas Lock 8.0-K 2) Dallas Lock 8.0-C

СЗИ Dallas Lock 8.0-К сертифицирована ФСТЭК России по **5** классу защищенности СВТ, **4** классу защиты СКН, **3** классу защищенности МЭ, **4** уровню контроля отсутствия НДВ и может использоваться при создании АС до класса защищенности **1Г** включительно, для обеспечения **1** уровня защищенности ПДн, для защиты информации в ГИС до **1** класса защищенности включительно, для создания АСУ ТП до **1** класса защищенности включительно (сертификат соответствия № 2720 от 25.09.2012 г., действителен до 25.09.2018 г.). Проводится сертификация на соответствие **4** классу защиты СОВ (в соответствии с профилем защиты ИТ.СОВ.У4.ПЗ) – решение ФСТЭК России о проведении сертификационных испытаний № 5091 от 14.03.2016 г., плановое окончание сертификации в 3 квартале 2016 г.

СЗИ Dallas Lock 8.0-С сертифицирована ФСТЭК России по **3** классу защищенности СВТ, **2** уровню контроля отсутствия НДВ и может использоваться при создании АС до класса защищенности **1Б** включительно, для обеспечения **1** уровня защищенности ПДн, для защиты информации в ГИС до **1** класса защищенности включительно, для создания АСУ ТП до **1** класса защищенности включительно (сертификат соответствия № 2945 от 16.08.2013 г., действителен до 16.08.2019 г.). Проводится сертификация на соответствие требованиям ФСТЭК России к СКН по **2** классу защиты, к МЭ по **2** классу защищенности, на соответствие **4** классу защиты СОВ (в соответствии с профилем защиты ИТ.СОВ.У4.ПЗ) – решение ФСТЭК России о проведении сертификационных испытаний № 5092 от 14.03.2016 г., плановое окончание сертификации в 3 квартале 2016 г.

Генеральный директор
ЗАО «СИС»
С.Б. Груданов
М.П.

Директор Центра защиты информации
ООО «Конфидент»
Е.Ю. Кожемяка
М.П.

Выводы по практической части

В презентации к курсовой работе были изложены следующие этапы:

1. Обнаружение взлома сети.
2. Способы защиты данных.
3. Основные возможности Dallas Lock 8.0-C.
4. Требования к аппаратному и программному обеспечению.
5. Общее описание системы защиты Dallas Lock 8.0.

Заключение

В процессе выполнения курсовой работы достигнуты результаты по обнаружению признаков взлома корпоративной базы данных, выбору и установке средства защиты Dallas Lock.

В главе 1 рассмотрены теоретические основы по защите данных, способы обнаружений угроз, анализ и выбор способов решений задачи, а также изложение решения задачи. Анализ показал, что существующий системы защиты недостаточно. Взвези с этим необходимы дополнительные системы защиты Dallas Lock, которые рассмотрены в следующий главе.

В главе 2 были рассмотрены средства защиты информации, требования к аппаратному и программному обеспечению, установка системы защиты Dallas Lock 8.0, установка сервера безопасности Dallas Lock 8.0.

Поставленные задачи по обнаружению угроз и установки системы защиты Dallas Lock 8.0-C, для их предотвращения, решены.

Спасибо за внимание