Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Факультет ____Заочного обучения_____

Отчет по учебной практике

Тип учебной практики практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности

студента ___ курса группы _____

_____

(фамилия, имя, отчество)

Место практики: Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики», кафедра МСИБ, г. Самара, ул. Л. Толстого д. 23.

Сроки прохождения практики _____

Руководитель практики от университета зам. декана ФЗО, к.т.н._
(должность, ученая степень, ученое звание,
Бельская Наталья Михайловна
фамилия, имя, отчество)

Самара, 2020г.

Содержание

Введение……...…3
1. Назначение программно-аппаратной защиты……4
2. Способы защиты оборудования программной защиты…….……....6
Заключение……..…16
Список литературы……17

Введение

По мере формирования и усложнения средств, методов и форм автоматизации процессов обработки информации повышается уязвимость защиты информации.

Основными факторами, способствующими повышению этой уязвимости, являются: резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации; резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных; усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального времени и др.

Программные средства защиты информации — это специальные программы и программные комплексы, предназначенные для защиты информации в информационной системе.

Программные средства включают программы для идентификации пользователей, контроля доступа, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и другие. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Недостатки – использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

1. Назначение программно-аппаратной защиты

Программно-аппаратная защита используется для защиты программного обеспечения от несанкционированного (неавторизованного) доступа и нелегального использования. Защитный механизм программным образом опрашивает специальное устройство, используемое в качестве ключа, и работает только в его присутствии. Таким образом, механизм программно-аппаратной защиты содержит две составляющие:

1) аппаратное устройство (аппаратная часть);

2) программный модуль (программная часть).

Поэтому обычно говорят о системах программно-аппаратной защиты.

Очевидно, что стоимость такого механизма превышает стоимость программной защиты, причем стоимость аппаратной части, как правило, превышает стоимость программной части. По этой причине программно-аппаратная защита считается привилегией корпоративных заказчиков, так как для индивидуального пользователя часто неприемлема с экономической точки зрения.

Обратим внимание на то, что, по существу, программно-аппаратная защита не является защитой программ от нелегального распространения и использования. Не станет заказчик программы оплачивать дорогую аппаратуру только ради соблюдения авторских прав разработчика. Но если программный продукт снабжен модулем, предназначенным для защиты от несанкционированного доступа *к данным и информации* пользователя, то заказчик, как правило, готов платить за аппаратуру, повышающую надежность такой защиты.

Система защиты от несанкционированного доступа к данным реализована таким образом, что осуществляет проверку легальности пользователя при работе с программным обеспечением и тем самым косвенно препятствует и незаконному использованию программы.

Кроме того, современные аппаратные устройства (ключи), помимо

информации о законном пользователе, могут содержать также информацию о программном продукте. А системы программно-аппаратной защиты, кроме аутентификации пользователя, могут производить аутентификацию приложения.

Поэтому системы программно-аппаратной защиты от несанкционированного доступа могут служить в то же время и для защиты авторских прав разработчиков программ.

Системы программно-аппаратной защиты широко используются на практике и многими пользователями признаются надежным средством.

Построение системы обеспечения безопасности информации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- экономическая эффективность;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

2. Способы защиты оборудования программной защиты

1.Защита от несанкционированного доступа:

Рассмотрим основные моменты защиты информации от несанкционированного доступа. Речь идет о таком порядке работы, при котором:

1) доступ к информации имеет только тот пользователь, который имеет разрешение; будем называть такого пользователя законным;

2) каждый законный пользователь работает только со своей информацией и не имеет доступа к информации другого законного пользователя;

3) каждый законный пользователь может выполнять только те операции, которые ему разрешено выполнять.

Для организации такого порядка работы прежде всего необходимо обеспечить распознавание законного пользователя. Этот процесс часто называют авторизацией пользователя.

Авторизация пользователя включает три этапа:

1. Идентификация пользователя.
2. Аутентификация пользователя.
3. Непосредственно авторизация пользователя.

Идентификация пользователя (identification) — это, с одной стороны, присвоение пользователю идентификатора - некоторого уникального признака (или нескольких); с другой стороны, процесс, во время которого пользователь указывает присвоенный ему идентификатор.

Другими словами, идентификация — это процесс, при котором пользователь называет себя.

Аутентификация пользователя (от англ. autentication - установление подлинности) - установление подлинности пользователя на основе сравнения с эталонным идентификатором.

Авторизация пользователя - установление прав пользователя.

Авторизованный пользователь (авторизованное лицо) - пользователь (лицо), который получил определенные права на работу с информацией.

В процессе авторизации для законного пользователя определяются права пользователя, то есть определяются данные, с которыми ему разрешено работать; операции, которые ему разрешено выполнять и т.п.

2.Идентификация пользователя

Идентификация пользователя может быть основана:

- на знании некоторой секретной информации (пароль, код);

- на владении некоторым специальным предметом или устройством (магнитная карточка, электронный ключ);

- на биометрических характеристиках (отпечатки пальцев, сетчатка глаза, спектральный состав голоса и т.п.).

Системы, основанные на знании некоторой секретной информации:

К такого рода системам относятся прежде всего программные механизмы парольной защиты, которые были уже рассмотрены выше. Кроме того, заметим, что системы, основанные на владении некоторым специальным предметом или устройством (магнитная карточка, электронный ключ), как правило, предполагают также знание пользователем некоторой секретной информации.

Системы, основанные на владении некоторым специальным предметом или устройством:

Традиционно в качестве таких устройств применялись магнитные карточки. Система защиты снабжалась устройством чтения персональной информации (уникального кода пользователя), записанной на магнитной карточке. Заметим, что с точки зрения защиты от несанкционированного доступа такие системы обладают малой степенью надежности, так как магнитная карточка может быть легко подделана (например, скопирована на специальном оборудовании).

Уникальный код пользователя хранится и на так называемой Proximity-карте, снабженной радиопередатчиком. Специальный считыватель постоянно излучает электромагнитную энергию. При попадании карты в электромагнитное поле, карта посылает считывателю свой код, который

затем система сравнивает с эталоном.

Наибольшее распространение получили системы защиты, использующие смарт-карты (SmartCard - интеллектуальная карта). В памяти смарт-карты также хранится эталонная информация для аутентификации пользователя, но в отличие от традиционной магнитной карточки, смарт-карта содержит микропроцессор, который позволяет производить некоторые преобразования уникального кода пользователя или некоторые другие действия.

Многие специалисты технологии защиты, основанные на использовании смарт-карт, считают прогрессивными, поэтому уделяют большое внимание их развитию.

Параллельно с развитием смарткарт-технологий усиленными темпами развиваются сегодня технологии, основанные на использовании электронных ключей. Такие технологии являются наиболее интересными с точки зрения защиты прав разработчиков программного обеспечения, поэтому ниже рассмотрим их подробнее.

Системы, основанные на биометрических характеристиках

Системы используют уникальные индивидуальные особенности строения человеческого тела для идентификации личности. В состав систем входят специальные считывающие устройства, генерирующие эталонные идентификаторы пользователей, а также устройства или программное обеспечение, анализирующее предъявленный образец и сравнивающее его с хранящимся эталоном.

В настоящее время разработаны разнообразные устройства, позволяющие идентифицировать личность на основе биометрических характеристик. Рассмотрим некоторые примеры.

Устройства считывания отпечатков пальцев идентифицируют личность по форме и числу деталей - точек начала и конца линий на пальце.

Сканеры сетчатки глаза сканируют образцы сетчатки глаза пользователя, сосредоточиваясь на уникальных кровеносных сосудах. С

помощью инфракрасного излучения с яркостью лампочки новогодней елки берутся данные по 300 точкам в области сетчатки глаза, и собранная информация преобразуется в число.

Устройства верификации голоса строят математическую модель вокального диапазона говорящего и используют ее для сравнения с образцом голоса (цена такого устройства колеблется от 1.000 до 1.500 долларов). Разработчики таких систем уделяют внимание решению проблеме обмана таких систем с помощью магнитофонов.

Устройства считывания геометрии руки используют свет для построения трехмерного изображения руки человека, проверяя такие характеристики, как длина и ширина пальцев и толщина руки (цена такого устройства приблизительно около 3.500 долларов).

Очевидно, что биометрические системы сложно реализуются, требуют хранения объемных баз данных, надежных технологий распознавания образов и дорогостоящей считывающей аппаратуры. Поэтому применяются такие системы защиты от несанкционированного доступа в основном в учреждениях, требующих особого контроля за доступом к секретной информации.

3.Аутентификация пользователя:

Аутентификация пользователя обычно реализуется по одной из двух схем: простая PIN-аутентификация или защищенная PIN-аутентификация. Обе схемы основаны на установлении подлинности пользователя посредством сравнения PIN-кода пользователя (PIN - Personal identification number, персональный идентификационный номер) с эталоном.

При простой PIN-аутентификации PIN-код просто посылается в ключ (смарт-карту); ключ (смарт-карта) сравнивает его с эталоном, который хранится в его (ее) памяти, и принимает решение о дальнейшей работе.

Процесс защищенной PIN-аутентификации реализуется по следующей схеме:

- защищенное приложение посылает запрос ключу (смарт-карте) на PIN-аутентификацию;

- ключ (смарт-карта) возвращает случайное 64-разрядное число;

- приложение складывает это число по модулю 2 с PIN-кодом, который ввел владелец ключа (смарт-карты), зашифровывает его DES-алгоритмом на специальном ключе аутентификации и посылает результат ключу (смарт-карте);

- ключ (смарт-карта) осуществляет обратные преобразования и сравнивает результат с тем, что хранится в его (ее) памяти.

В случае совпадения считается, что аутентификация прошла успешно и пользователь (приложение) может продолжать работу.

4.Электронные ключи:

Электронный ключ – это некоторое физическое устройство. Электронный ключ может быть выполнен либо на основе специализированного чипа, либо на микросхемах энергонезависимой электрически перепрограммируемой памяти, либо на базе микропроцессоров.

Долгое время такие устройства подсоединялись к разъему параллельного (принтерного) порта компьютера, что ввиду неудобства сдерживало широкое внедрение электронных ключей. Позже появились технологии, позволяющие подсоединять электронные ключи и через последовательные порты.

Новейшие стандарты и технологии (в частности, технология подключения устройств на основе USB-шины - Universal Serial Bus) позволяют иметь дополнительные порты в удобных и легкодоступных местах компьютера и тем самым способствуют широкому применению аппаратных устройств для защиты.

В памяти электронного ключа хранится уникальная информация. Программная часть системы защиты определяет наличие электронного ключа при запуске программы и проверяет правильность содержащейся в ключе информации.

Память электронного ключа, кроме уникальной информации о пользователе (регистрационный номер, пароль, PIN-код), может содержать и другие параметры. Разработчики защиты с целью противодействия незаконному распространению и использованию программного обеспечения включают в электронный ключ информацию о программном обеспечении, например,

- серийный номер программы;
- номер версии;
- дату выпуска (продажи) и др.

При наличии возможности программы работать в демонстрационном режиме (или в режиме блокирования некоторых функций) электронный ключ дополняется информацией о количестве запусков приложения, предельного времени (даты) работы. Заметим, что при этом электронный ключ может служить и для защиты условно бесплатного программного обеспечения.

Замечательное свойство современных электронных ключей - возможность дистанционного перепрограммирования памяти ключа. Технологии дистанционного перепрограммирования памяти ключа используются разработчиками, во-первых, для противодействия незаконному использованию программ, а во-вторых, для улучшения потребительских свойств программного обеспечения.

Сегодня усилия разработчиков, помимо повышения качества основных функций программного обеспечения и увеличения надежности защиты, направлены и на повышение потребительских свойств продукта: простоту установки и настройки, удобство администрирования, гибкость применения и т.п. Дистанционное перепрограммирование памяти ключа позволяет разработчику с максимальной степенью удобства для конечного пользователя сопровождать программное обеспечение. Например, вместе с новой версией продукта пользователь получает и специальный модуль, который производит модификацию поля номера версии в памяти электронного ключа. Модуль защиты всегда производит сравнение номера

версии программы с соответствующим полем. Такой механизм препятствует нелегальному использованию программы: нарушитель не сможет воспользоваться незаконно полученной копией новой версии продукта без перепрограммирования памяти электронного ключа.

Удобен для пользователя и перевод программного обеспечения из работы в демонстрационном режиме на режим полного функционирования. После оплаты пользователь также получает специальный модуль, модифицирующий поле памяти электронного ключа, ответственного за такой перевод. При этом пользователь освобождается от необходимости переустановки и/или перенастройки приложения.

Некоторые разработчики предлагают использование памяти электронного ключа и для управления правами доступа. В зависимости от уникальной информации о пользователе и специальных полей в памяти ключа, пользователю доступны те или иные функции программы. Перепрограммирование памяти ключа позволяет открыть/закрыть доступ к некоторым функциям.

Электронные ключи обеспечивают также лицензирование в сетях.

Лицензия - это оговоренные при покупке программного продукта права на использование программы.

Разработчики сетевого программного обеспечения стремятся получить доход с каждой копии программы, установленной на рабочую станцию локальной сети. При этом возникают проблемы. Так как пользователи программного обеспечения в локальной сети, оплатив стоимость одной копии, стремятся не платить за использование программы на дополнительных рабочих станциях. Кроме того, у пользователей есть возможность установить лицензионную копию на сервере и использовать ее с любой рабочей станции. В этих случаях разработчики получают неадекватную прибыль от реализации программного продукта.

Традиционно эта проблема решается с помощью специальных программ - администраторов лицензий (licence manager). Подчеркнем, что

при использовании таких программ контроль за легальным использованием программного продукта возлагается на администраторов сетей и часто не защищен от обмана. Поэтому для гарантированного решения проблемы защиты авторских прав разработчиков сетевого программного обеспечения необходимо, чтобы контроль за легальным использованием продукта производил сам разработчик.

Для этого можно в памяти электронного ключа в отдельных, защищенных от записи полях, хранить счетчик лицензий, а также максимальное число пользователей лицензируемого приложения. Очевидно, что система, использующая такой электронный ключ, позволяет контролировать и ограничивать число станций, работающих (одновременно) с защищенной программой.

5.Современные электронные ключи

Первоочередной причиной, сдерживающей использование программно-аппаратной защиты, является высокая стоимость дополнительных аппаратных устройств. Обычно это дорогие считывающие устройства, так называемые ридеры (reader). Поэтому успех на рынке систем программно-аппаратной защиты обеспечен тем производителям, электронные ключи которых являются более удобными и дешевыми.

В январе 1999 года израильской компанией Aladdin Knowledge Systems была запатентована технология eToken USB (для нового поколения компьютеров с периферийной шиной USB) на основе концептуально нового электронного ключа eToken[2]. Электронный ключ eToken предназначен для безопасного хранения паролей, ключей шифрования, а также для защиты программного обеспечения и данных от несанкционированного использования. Устройство eToken USB представляет собой миниатюрный брелок (размер - 52x16x8 мм, вес 5 г.) с энергонезависимой (до 8 Кб) памятью, допускающей перезапись (не менее 100 тыс. раз). Ключ eToken является компромиссом между традиционным электронным ключом и смарт-картой. Для получения

доступа к защищенному объекту пользователю достаточно вставить ключ eToken в USB-порт и набрать на клавиатуре личный код.

Электронный ключ eToken базируется на встроенной аппаратной системе аутентификации пользователей. Для аутентификации пользователей используется защищенная PIN-аутентификация.

Разработчику защиты предоставляется комплект разработчика - Developer's Kit. В комплект разработчика входит программное обеспечение, которое позволяет организовать различные механизмы защиты.

6.Способы взлома программно-аппаратной защиты

На практике в основном применяются два способа взлома программно-аппаратной защиты:

1. Отключение (взлом) программной части защиты.
2. Эмулирование электронного ключа.

Первый способ взлома заключается в удалении (модификации) из защищенного приложения полностью или частично кодов, связанных с механизмом защиты. Например, иногда достаточно удалить из программы команды опроса электронного ключа и/или команды сравнения с эталоном. Очевидно, что большинство из рассмотренных выше методов взлома программной защиты могут быть использованы для взлома программной части программно-аппаратной защиты.

Эмулирование электронного ключа - это способ взлома путем эмулирования программными или аппаратными средствами работы электронного ключа.

Эмулятор - программа, выполняющая функции, обычно реализуемые некоторым внешним устройством.

Программа-эмулятор реализована таким образом, что возвращает защищенному приложению «правильные» ответы на все обращения к электронному ключу. В результате получается электронный ключ, реализованный только на программном уровне.

Для защиты от эмуляции электронного ключа рекомендуется

использовать хаотический порядок обмена информацией между защищенным приложением и электронным ключом.

Обычно эмулятор взаимодействует с защищенным приложением либо через точку входа API вызова ключа, либо подменой драйвера работы с ключом. Для противодействия эмуляции через точку входа рекомендуется контролировать целостность соответствующего фрагмента программы и/или зашифровать его. Специалисты рекомендуют наряду с явными обращениями к ключу реализовывать и скрытые вызовы.

Для противодействия эмуляции с помощью подмены драйвера работы с ключом специалисты также рекомендуют контролировать целостность драйвера, например, с помощью электронной цифровой подписи.

Заметим, что реализация эмулятора электронного ключа достаточно сложна, поэтому доступна только высококвалифицированным специалистам.

Интересное решение для защиты от эмуляции электронного ключа и защиты программ с его помощью предлагает компания Актив. Программно-аппаратный комплекс защиты Guardant Stealth использует аппаратные алгоритмы преобразования данных, серьезно усложняющие разработку эмулятора ключа. Электронные ключи Guardant Stealth содержат микроконтроллеры (прозрачные для пользователя), производящие вычисления по одному из нескольких оригинальных высоко сложных алгоритмов (ключ может содержать до 18 таких алгоритмов). Микроконтроллер возвращает защищенному приложению преобразованную с помощью аппаратного алгоритма входную информацию.

Заключение

Быстро развивающиеся компьютерные информационные технологии вносят заметные изменения в нашу жизнь. Информация стала товаром, который можно приобрести, продать, обменять. При этом стоимость информации часто в сотни раз превосходит стоимость компьютерной системы, в которой она хранится.

От степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей. Такова плата за усложнение и повсеместное распространение автоматизированных систем обработки информации.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя

Список литературы

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
3. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.
4. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2017. - 159 с.
5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
6. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.1 / С.В. Запечинков. - М.: ГЛТ, 2006. - 536 с.
7. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.2 / С.В. Запечинков. - М.: ГЛТ, 2008. - 558 с.