Презентация по курсовой работе на тему: «Анализ программно-аппаратных средств»

Выполнил:

студент 4 курса ,группы 100502-ЗИСа-о18

Примак А.М.

Проверил:

ассистент каф.ИБ Цигулев И.Н

Введение

Используя различные методы и средства информационной сетевой защиты, невозможно достичь абсолютно идеальной безопасности сети. Средств защиты не бывает слишком много, однако с ростом уровня защищенности той или иной сети возникают и, как правило, определенные неудобства в ее использовании, ограничения и трудности для пользователей. Поэтому, часто необходимо выбрать оптимальный вариант защиты сети, который бы не создавал больших трудностей в пользовании сетью и одновременно обеспечивал достойный уровень защиты информации. Подчас создание такого оптимального решения безопасности является очень сложным.

Таким образом, актуальность анализа программно-аппаратных средств проблемы обуславливается тем, что технологии компьютерных систем и сетей развиваются слишком быстро. Появляются новые угрозы безопасности информации. Соответственно, такую информацию нужно защищать.

Цель курсовой - изучение и анализ программно-аппаратных средств защиты информации.

В соответствии с поставленной целью были определены следующие задачи курсовой:

- рассмотреть основные угрозы в сфере защиты информации, и привести их классификацию;
- охарактеризовать программно-аппаратные средства защиты информации и классифицировать их;
- проанализировать возможности аппаратных и программных средств защиты информации, выявить их достоинства и недостатки;

Глава 1. Угрозы в сфере защиты информации и их классификацию

1. Анализ угроз информационной безопасности
2. Основные методы реализации угроз информационной безопасности
3. Уязвимость компьютерных сетей
4. Способы и средства защиты информации

1.1 Анализ угроз информационной безопасности

Широкое внедрение информационных технологий в нашу жизнь привело к появлению новых угроз безопасности информации.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Общая классификация угроз безопасности

Угрозы безопасности			
Естественные		Искусственные	
Природные	Технические	Непреднамеренные	Преднамеренные

1.2Основные методы реализации угроз информационной безопасности

К основным направлениям реализации злоумышленником информационных угроз относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства системы программных или технических механизмов, нарушающих её предполагаемую структуру и функции.

Распределение методов реализации угроз информационной безопасности по уровням

Уровень доступа к информации	Основные методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза нарушения доступности
Носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации; перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Средств взаимодействия с носителем	Получение информации о программно-аппаратной среде; получение детальной информации о функциях, выполняемых системой; получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам системы; совершение пользователем несанкционированных действий; несанкционированное копирование программного обеспечения; перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные; установка и использование нештатного программного обеспечения; заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент системы; обход механизмов защиты
Представления информации	Определение способа представления информации	Визуальное наблюдение; раскрытие представления информации (дешифрование)	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка.
Содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации.

1.3 Уязвимость компьютерных сетей

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

- перехват информации - целостность информации сохраняется, но её конфиденциальность нарушена;
- модификация информации - исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от чужого имени (этот вид обмана принято называть спуфингом) или Web - сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

Специфика компьютерных сетей, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Также уязвимость информации зависит от вредоносного программного обеспечения. Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Уязвимость компьютерных сетей

Выделяют следующие аспекты вредоносного программного обеспечения:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющая разрушительную функцию, используется для:

- внедрения другого вредоносного программного обеспечения;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы - код, обладающий способностью к распространению путем внедрения в другие программы;
- черви - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по сети и их выполнение (для активизации вируса требуется запуск зараженной программы)

1.4 Способы и средства защиты информации

Для предотвращения вышеперечисленных угроз существуют различные способы защиты информации. Помимо естественных способов выявления и своевременного устранения причин, используют следующие специальные способы защиты информации от нарушений работоспособности компьютерных систем:

- внесение структурной, временной информации и функциональной избыточности компьютерных ресурсов;
- защита от некорректного использования ресурсов компьютерной системы;
- выявление и своевременное устранение ошибок на этапе разработки программно-аппаратных средств

Способы и средства защиты информации

Основным видом угроз целостности и конфиденциальности информации является преднамеренные угрозы. Их можно разделить на 2 группы:

- угрозы, которые реализуются с постоянным участием человека;
- после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без участия человека.

Задачи по защите от угроз каждого вида одинаковы:

- запрещение несанкционированного доступа к ресурсам;
- невозможность несанкционированного использования ресурсов при осуществлении доступа;
- своевременное обнаружение факта несанкционированного доступа. Устранение их причин и последствий

Глава 2. Анализ программно-аппаратных средства защиты информации

1. Общие сведения о программно-аппаратных средствах защиты информации
2. Сравнение программно-аппаратных средств на примере популярных программно-аппаратных комплексов и средств защиты информации от НСД
3. Сравнение программно-аппаратных средств на примере популярных средств криптографической защиты информации

2.1Общие сведения о программно-аппаратных средствах защиты информации

Программно-аппаратные средства защиты информации – вся система обработки информации или часть ее физических компонентов с размещенными программами и данными. Программы при этом размещаются таким образом, чтобы их несанкционированное изменение было невозможным в ходе исполнения. Программы и данные, размещенные на ПЗУ с электронным программированием, допускающим стирание, рассматриваются как программное обеспечение.

К программным и программно-аппаратным средствам защиты информации относятся:

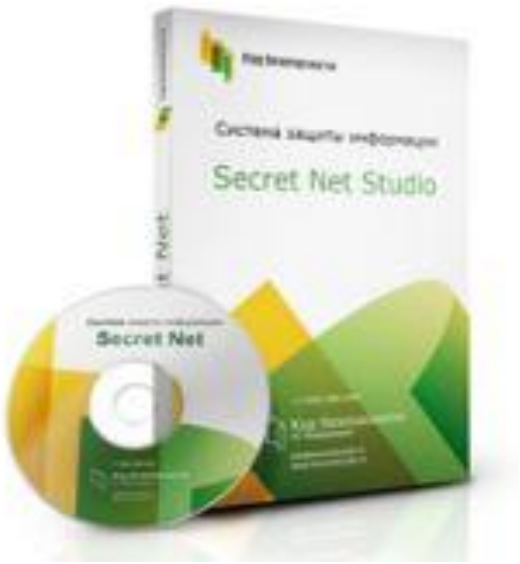
- средства криптографической защиты информации;
- антивирусные программы;
- средства идентификации и аутентификации пользователей;
- средства управления доступом;
- средства протоколирования и аудита;
- средства экранирования.

2.2 Сравнение программно-аппаратных средств на примере популярных программно-аппаратных комплексов и средств защиты информации от НСД

В настоящее время среди основных игроков рынка сертифицированных программно-аппаратных средств защиты информации (СЗИ) можно выделить следующие продукты:

- СЗИ Secret Net Studio и ПАК «Соболь» («Код Безопасности»)
- СЗИ Dallas Lock и средство доверенной загрузки (СДЗ) Dallas Lock (компания «Конфидент»)
- СЗИ «Аккорд» (компания ОКБ САПР)
- СЗИ «Блокхост-сеть 4»(«Газинформсервис»)
- СЗИ Панцырь+ (НПП «Безопасные информационные технологии»)
- ПАК Diamond WPN/FW (компания ТСС)
- СЗИ«Страж NT 4.0» (компания «Рубинтех»)

Выберем несколько популярных программно-аппаратных средств защиты информации и сравним их между собой, что бы лучше понимать их нынешние возможности. Далее рассмотрим что из себя представляют и из каких компонентов состоят СЗИ Secret Net Studio и СЗИ Dallas Lock 8.0-K.



Secret Net Studio представляет из себя комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

Ключевые особенности:

- Независимый от ОС контроль внутренних механизмов СЗИ и драйверов;
- Автоматизированная настройка механизмов для выполнения требований регуляторов;
- Удобные графические инструменты мониторинга состояния компьютеров в защищаемой системе;

- Комплексная защита на пяти уровнях: защита данных, приложений, сетевого взаимодействия, операционной системы и подключаемых устройств;
- Интеграция независимых от ОС защитных механизмов для повышения общего уровня защищенности рабочих станций и серверов;
- Создание централизованных политик безопасности и их наследование в распределенных инфраструктурах;
- Поддержка иерархии и резервирования серверов безопасности в распределенных инфраструктурах.

В состав клиента системы Secret Net Studio входят следующие функциональные компоненты:

- основные программные службы, модули и защитные подсистемы (базовая защита);
- дополнительно подключаемые функциональные компоненты, условно разделенные на следующие группы:
  — локальная защита;
  — сетевая защита;
  — шифрование трафика.

Базовая защита

В базовую защиту входят следующие программные службы, модули и защитные подсистемы:

- ядро;
- агент;
- средства локального управления;
- подсистема локальной аутентификации;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой

Шифрование трафика (VPN клиент)

Подсистема шифрования трафика обеспечивает безопасную передачу данных через общедоступные незащищенные сети. Для организации передачи данных используется технология "виртуальной частной сети», реализуемая аппаратно-программным комплексом шифрования "Континент".

Локальная защита

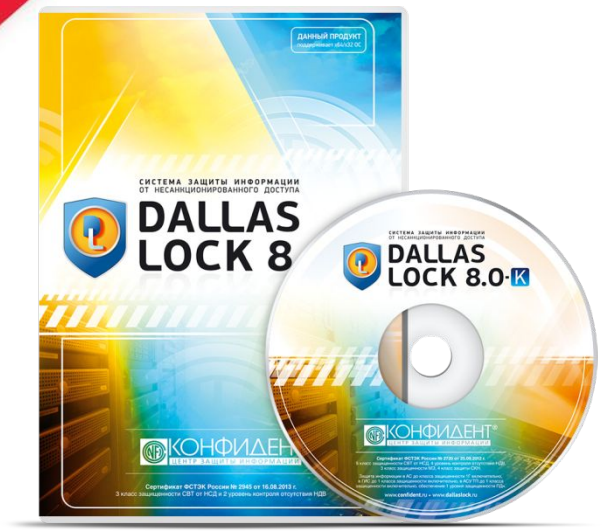
К группе локальной защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- контроль устройств;
- контроль печати;
- замкнутая программная среда;
- полномочное управление доступом;
- дискреционное управление доступом к ресурсам файловой системы;
- затирание данных;
- защита информации на локальных дисках;
- шифрование данных в криптоконтейнерах.

Сетевая защита

К группе сетевой защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- межсетевой экран;
- авторизация сетевых соединений.



Dallas Lock 8.0 представляет собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов.

Система защиты Dallas Lock 8.0 состоит из следующих основных компонентов:

- Программное ядро (Драйвер защиты).
- Подсистема администрирования.
- Подсистема управления доступом.
- Подсистема регистрации и учета.
- Подсистема идентификации и аутентификации.
- Подсистема гарантированной зачистки информации.
- Подсистема преобразования информации.
- Подсистема контроля устройств.
- Подсистема межсетевого экранирования.
- Подсистема обнаружения вторжений.
- Подсистема контроля целостности.
- Подсистема восстановления после сбоев.
- Подсистема развертывания (установочные модули).
- Подсистема централизованного контроля конфигураций.
- Подсистема резервного копирования.

Сравнение классов защищенности СЗИ от НСД Secret Net Studio и Dallas Lock 8.0-К

	Secret Net Studio	Dallas Lock 8.0-К
Сертификат соответствия	**ФСТЭК России** №3745 от 16 мая 2017г Действителен до 16 мая 2025 г.	**ФСТЭК России** №2720 от 25 сентября 2012г Действителен до 25 сентября 2021 г.
Класс защищенности СВТ	5 класс защищенности СВТ	5 класс защищенности СВТ
Класс защиты МЭ	ИТ.МЭ.В4.ПЗ	ИТ.МЭ.В4.ПЗ
Класс защиты СОВ	ИТ.СОВ.У4.ПЗ	ИТ.СОВ.У4.ПЗ
Класс защиты СКН	ИТ.СКН.П4.П3	ИТ.СКН.П4.ПЗ
Уровень контроля отсутствия НДВ	УД 4	УД 4
САВЗ	4 класс защиты САВЗ	—
Класс АС	1Г	1Г
Класс защищенности ГИС / АСУ ТП Уровень защищенности ПДн Категория значимых объектов КИИ	до 1 вкл.	до 1 вкл.

Secret Net Studio и Dallas Lock 8.0-К примерно равны по характеристикам, вопрос о применении конкретного средства решается либо на основе различий архитектуры СЗИ и требования к наличию аппаратной части, либо на основе экономической выгодности продукта в конкретной компании.

2.3Сравнение программно-аппаратных средств на примере популярных средств криптографической защиты информации

Средствами криптографической защиты информации (СКЗИ) называют специальные программы для шифрования данных. СКЗИ используют в разных сферах, например, для доверенного хранения документов или передачи информации по защищенным каналам связи.

Рассмотрим самые используемые СКЗИ двух разработчиков — КриптоПро и ViPNet.

ViPNet CSP 4 — российский криптопровайдер, сертифицированный ФСБ России как средство криптографической защиты информации (СКЗИ) и электронной подписи.

ViPNet CSP 4 позволяет:

- Создавать ключи электронной подписи, формировать и проверять ЭП по ГОСТ Р 34.10-2012.
- Хэшировать данные по ГОСТ Р 34.11-2012
- Шифровать и производить имитозащиту данных по ГОСТ 28147-89, ГОСТ 34.12-2018, ГОСТ 34.13-2018
- Создавать защищенные TLS-соединения (только для Windows)
- Формировать CMS-сообщения, включая расширение CAdES-BES;
- Формировать транспортные ключевые контейнеры.

КриптоПро CSP 5.0 — новое поколение криптопровайдера, развивающее три основные продуктовые линейки компании КриптоПро: КриптоПро CSP (классические токены и другие пассивные хранилища секретных ключей), КриптоПро ФКН CSP/Рутокен CSP (неизвлекаемые ключи на токенах с защищенным обменом сообщениями) и КриптоПро DSS (ключи в облаке).

КриптоПро CSP 5.0 позволяет:

- Формирование и проверка электронной подписи.
- Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.
- Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS, и IPsec.
- Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений доверенного функционирования.

Сравнение СКЗИ ViPNet CSP 4 и КриптоПро CSP 5.0:

	ViPNet CSP 4	КриптоПро CSP 5.0
Стартовая стоимость	2700 руб. единоразово / пользователь	4350 руб. в год / пользователь
VPN / Виртуальная Частная Сеть	+	-
Брандмауэры	-	-
Контроль доступа	+	+
Мониторинг активности	+	-
Отчетность / Аналитика	-	-
Реакция на угрозы	+	-
Система обнаружения вторжений	+	-
Сканирование уязвимостей	-	-

По функциональным возможностям выигрывает СКЗИ VipNet, но окончательный выбор зависит лишь от поставленных задач и требований к программно-аппаратным средствам. Например КриптоПро CSP подойдет индивидуальным пользователям и командам, которые нуждаются в хранении ключей, а VipNet CSP подойдет компаниям, фирмам и предприятиям, которые хотят надежно защитить рабочее место от внешних и внутренних сетевых атак.

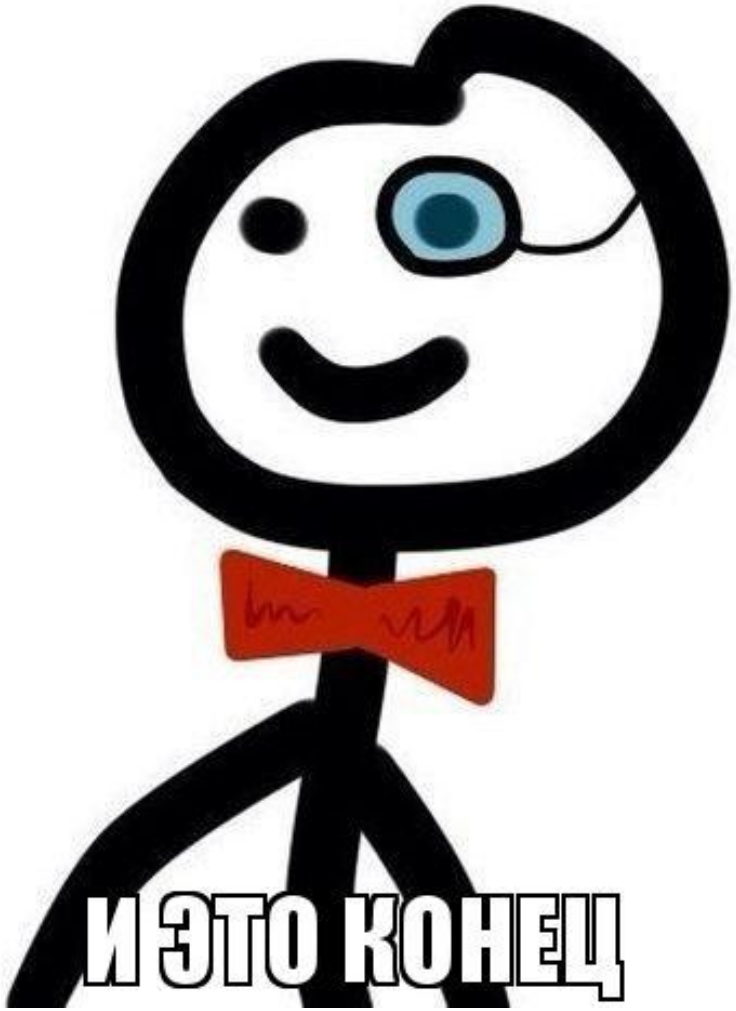
Заключение

Обеспечение защиты информации сейчас становится, важнейшим условием нормального функционирования любой информационной системы. В защите информации сейчас можно выделить три основных и дополняющих друг друга направления:

- постоянное совершенствование технологий и организационно-технических мероприятий технологии обработки информации с целью ее защиты от внешних и внутренних угроз безопасности;
- блокирование несанкционированного доступа к информации при помощи специальных аппаратных средств;
- блокирование несанкционированного доступа к информации при помощи специальных программных средств.

В существующей проблеме защиты информации в сетях, которая становится всё более актуальная, выделяются три основных аспекта уязвимости:

- опасность несанкционированного доступа к информации лицами, для которых она не предназначена;
- возможность искажения либо уничтожения конфиденциальной, ценной информации;
- возможность модификации информации, как случайная, так и умышленная.


И ЭТО КОНЕЦ