ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 2019 г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 12

Тема: «СЗИ от НСД SECRET NET»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
«____» _____ 201_ г.
протокол № __

Санкт-Петербург
2019

Содержание занятия и время

Вводная часть 10 мин.

Объявление темы, цели и порядка проведения занятия
Проведение текущего контроля в виде тестирования
Выдача раздаточных материалов (уменьшенные копии графических материалов)

Основная часть 75 мин.

1. Классификация и характеристики угроз безопасности информации, связанных с несанкционированным доступом 35 мин.
2. Архитектура, компоненты и защитные механизмы средства защиты информации от несанкционированного доступа Secret Net 40 мин.

Заключительная часть 5 мин.

Контрольные вопросы
Подведение итогов занятия
Задание на самостоятельную работу.

Литература:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – с. 22-42.

2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – с. 192-220.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 – с.21-23, 24-27

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, проектор, экран, телевизор.
2. Приложения (слайды к лекции № 12), видеоролик, раздаточный материал.
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции:

1. Ознакомить обучающихся с угрозами безопасности информации, связанных с НСД в специальных АС и способах и средствах их предотвращения.

2. Сформировать ответственное отношение к выполнению требований по обеспечению информационной безопасности в служебной деятельности.

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Методические приемы:

Использование комплекта слайдов по теме занятия.

Использование раздаточного материла: (уменьшенные копии графических материалов).

Использование примеров из профильных учебных дисциплин.

Проведение систематического текущего контроля обучающихся: индивидуальное тестирование по пройдённому материалу.

В основной части сконцентрировать внимание курсантов на угрозах безопасности информации, связанных с НСД и сертифицированных программно-аппаратных средствах *СЗИ от НСД*.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Сформулируйте определение: Несанкционированный доступ – это…
2. Что применяется для реализации угроз связанных с НСД?
3. Перечислите источники угроз НСД?

4. Сколько групп внутренних нарушителей вы знаете?
5. Сформулируйте определение: Средства защиты от НСД – это…
6. Перечислите защитные подсистемы СЗИ от НСД Secret Net?
7. Что вы понимаете под идентификацией и аутентификацией пользователей?
8. Какие режимы идентификации используются в СЗИ от НСД Secret Net?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

ЛЕКЦИЯ № 12

ВОПРОС № 1. Классификация и характеристики угроз безопасности информации, связанных с НСД.

----------Слайд 4----------

Угроза безопасности информации *- представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее*

Несанкционированный доступ – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации. Также несанкционированным доступом в отдельных случаях называют получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Руководящий документ Гостехкомиссии «Защита от НСД. Термины и определения» (утверждён решением председателя Гостехкомиссии России от 30 марта 1992 г.) трактует определение немного иначе:

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Для реализации угроз связанных с НСД применяются:

1. Программные средства;
2. Программно-аппаратные средства.

----------Слайд 5----------

Перечислим последствия, которые могут возникнуть при НСД:

По ТКУИ:

Нарушение конфиденциальности (*копирование, несанкционированное распространение*);

При НСД:

1. Нарушение конфиденциальности данных (*копирование, несанкционированное распространение*);
2. Нарушение целостности данных (*уничтожение, изменение*)
3. Нарушение доступности данных (*блокирование*).

Примечание: Обратите внимание, что по ТКУИ можно осуществить только нарушения связанные конфиденциальностью данных, а при НСД еще можно нарушить целостность и доступность данных.

----------Слайд 6----------

Перечислим **три основных группы угроз НСД**

1. Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет:
   a. преднамеренных изменений служебных данных;

b. игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации;
c. искажения (модификации) самих данных.

2. Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения;
   a. угрозы удаленного доступа (реализуются с использованием протоколов сетевого взаимодействия);
   b. угрозы непосредственного доступа (осуществляются с использованием программных и программно-аппаратных средств ввода/вывода компьютера).
3. Угрозы внедрения вредоносных программ (программно-математического воздействия).

Рассмотрим **на слайде 7 источники угроз НСД**

1. Нарушитель;
2. Носитель вредоносной программы:
3. Аппаратная закладка.

Типы нарушителей по наличию права доступа:

- **Внешние** *(разведывательные службы государств; криминальные структуры; конкуренты (конкурирующие организации); недобросовестные партнеры; внешние субъекты (физические лица)).*
- **Внутренние** *(сотрудники организации (администраторы, пользователи и лица не имеющие отношения к АС)).*

Далее рассмотрим возможности ***внешних*** нарушителей:

1. НСД к каналам связи (см. **слайд № 8)**;
2. НСД через АРМ, подключенные к интернету (см. **слайд № 9)**;
3. НСД к информации с использованием специальных программных воздействий (см. **слайд № 10)**;
4. НСД через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла оказываются за пределами контролируемой зоны (см. **слайд № 11)**;
5. НСД через ИС партнёров и т.д. (см. **слайд № 12)**.

Далее давайте рассмотрим **категории и возможности внутренних нарушителей (ВН), всего их восемь.**

----------Слайд 13----------

Первая категория ВН – лица, имеющие санкционированный доступ к ИС, но не имеющие доступа к информации (например: системный администратор сегмента сети).

Возможности:

- иметь доступ к фрагментам информации;
- располагать фрагментами информации о топологии ИС и об используемых коммуникационных протоколах и их сервисах;
- располагать именами и вести выявление паролей зарегистрированных пользователей;
- изменять конфигурацию технических средств ИС, вносить в нее программно-аппаратные закладки.

Вторая категория ВН – зарегистрированные пользователи, осуществляющие ограниченный доступ к ресурсам ИС с рабочего места

Возможности:

- знает по меньшей мере одно легальное имя доступа;
- обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству информации;
- располагает конфиденциальными данными, к которым имеет доступ.

Третья категория ВН – Зарегистрированные пользователи, осуществляющие удаленный доступ к информации по локальным и (или) распределенным информационным системам

Возможности:

- располагает информацией о топологии ИС на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИС;
- имеет возможность прямого (физического) доступа к фрагментам технических средств ИС.

Четвертая категория ВН – зарегистрированные пользователи с полномочиями администратора безопасности сегмента ИС

Возможности:

- обладает полной информацией о системном и прикладном программном обеспечении;
- обладает полной информацией о технических средствах;
- имеет доступ к СЗИ и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИС;
- имеет доступ ко всем техническим средствам сегмента (фрагмента) ИС;

Пятая категория ВН – зарегистрированные пользователи с полномочиями системного администратора ИС

Возможности:

- обладает полной информацией о системном и прикладном программном обеспечении;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

Шестая категория ВН – зарегистрированные пользователи с полномочиями администратора безопасности ИС

Возможности:

- обладает полной информацией об ИС;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИС;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Седьмая категория ВН – программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом объекте

Возможности:

- обладает информацией об алгоритмах и программах обработки информации на ИС;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИС на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты информации, обрабатываемых в ИС.

Восьмая категория ВН – разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИС

Возможности:

- обладает возможностями внесения закладок в технические средства на всех стадиях жизненного цикла;
- может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и ЗИ.

----------Слайд 14----------

Далее рассмотрим **носитель вредоносной программы** как источник угроз НСД в АС. Носители разделяются на две составляющие:

✓ аппаратный элемент компьютера (*опт. диск, дискета 3.1/2", флэш накопители*);

✓ программный контейнер (*пакеты передаваемых по компьютерной сети сообщений; файлы (текстовые, графические, исполняемые))*;

Приведем еще несколько примеров носителей вредоносной программы как программного элемента компьютера (Аппаратные кейлоггеры). Слайд № 15-17.

----------Слайд 18----------

Давайте рассмотрим теперь **угрозы непосредственного доступа**, которые позволяют обеспечить следующие возможности злоумышленнику:

- возможность перехвата управления загрузкой операционной системы и получение прав доверенного пользователя;
- возможность выполнения НСД путем вызова штатных программ операционной системы или запуска специально разработанных программ, реализующих такие действия;
- доступ в среду функционирования прикладных программ;
- непосредственный доступ к информации пользователя.

----------Слайд 19----------

Классифицировать **угрозы по условиям реализации** можно следующим образом. **Выделим три группы угроз:**

1. **Угрозы, реализуемые в ходе загрузки операционной системы**
   - ✓ перехват паролей;
   - ✓ модификация программного обеспечения базовой системы ввода-вывода (BIOS);
   - ✓ перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду.

Примечание: *Чаще всего реализуются с использованием отчуждаемых носителей информации.*

----------Слайд 20-21----------

2. Угрозы, реализуемые после загрузки операционной среды

- непосредственный НСД к информации с использованием:
  - ✓ стандартных функций операционной системы
  - ✓ прикладных программ общего пользования
  - ✓ специально созданных для выполнения НСД программ:
    - *программы просмотра и модификации реестра;*
    - *программы поиска текстов в текстовых файлах по ключевым словам и их копирования;*
    - *специальные программы просмотра и копирования записей в базах данных;*
    - *программы быстрого просмотра графических файлов, их редактирования или копирования;*
    - *программы поддержки возможностей реконфигурации программной среды (настройки ИС в интересах нарушителя).*

----------Слайд 22----------

3. Включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.

Большая часть таких угроз - это угрозы внедрения вредоносных программ**.**

----------Слайд 23----------

Далее рассмотрим **угрозы внедрения вредоносных программ (программно-математические воздействия).**

Программно-математическое воздействие – это воздействие с помощью вредоносных программ.

Вредоносная программа – некоторая самостоятельная программа способная выполнять следующие функции:

- скрывать признаки своего присутствия;
- самодублироваться, ассоциировать себя с другими программами;
- разрушать код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя деструктивные функции;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа;
- искажать, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации.

----------Слайд 24----------

Классификация угроз при ПМВ

Угрозы, реализация которых требует внедрения программных компонентов на компьютере-жертве:

- компьютерные вирусы
- черви
- троянские программы
- потенциально опасное ПО – рекламные утилиты и т.д.

Угрозы, реализация которых внедрения программных компонентов не требует:

- спам
- фишинг
- внешняя, применительно к компьютеру, реклама
- хакинг

----------Слайд 25-27----------

Пути проникновения:
Вирусов;
Троянов;
Червей.

----------Слайд 28----------

Сценарий атаки

----------Слайд 29----------

Выводы по первому вопросу

I. Изучили классификацию, характеристики и источники угроз безопасности информации, связанных с НСД;

II. Разобрали основные способы реализации угроз безопасности информации, связанных с НСД.

----------Слайд 30----------

ВОПРОС № 2. Архитектура, компоненты и защитные механизмы средства защиты от несанкционированного доступа Secret Net.

----------Слайд 31----------

Средства защиты от несанкционированного доступа (СЗИ от НСД) - программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.

Предназначены для решения следующих задач:

- Защита конфиденциальной информации;
- Защита от проникновения и несанкционированных действий злоумышленника внутри системы;
- Выполнение требований и рекомендаций по защите конечных точек.

При защите от НСД должны осуществляться три основных способа обеспечения безопасности:

1. Разграничение и контроль доступа;
2. Контроль целостности программно-аппаратной среды;
3. Регистрация и учет событий.

----------Слайд 32----------

Перечислим основные СЗИ от НСД занимающих данный сектор рынка в настоящее время.

----------Слайд 33----------

Система «Secret Net 7» предназначена для защиты от НСД рабочих станций и серверов на уровне данных, приложений, операционной системы и периферийных устройств, функционирующих под управление операционных систем MS Windows 10/8/7/Vista/XP и Windows Server.

Требования к аппаратному и программному обеспечению

Клиент:

Компонент "Secret Net 7" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32– и 64– разрядные версии ОС с установленными пакетами обновлений не нижеуказанных):

• Windows8/8.1;

• Windows7SP1;

• WindowsVistaSP2;

• WindowsXPProfessionalSP3/XP Professionalx64 EditionSP2;

• WindowsServer2012/Server2012R2;

• WindowsServer2008SP2/Server2008R2SP1;

• WindowsServer2003SP2/Server2003R2SP2.

Сервер:

Компонент “Secret Net 7 – Сервер безопасности” устанавливается на компьютеры, работающие под управление следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не нижу указанных):

- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1;
- Windows Server 2003 SP2/Server 2003 R2 SP2.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Оперативная память	4 ГБ	8 ГБ
Жесткий диск (свободное пространство)	10 ГБ	50 ГБ
Высокопроизводительный жесткий диск (свободное пространство)	100 ГБ	100 ГБ

Сертификаты ФСТЭК и Минобороны России для SN 7.6:

✓ СВТ 3/НДВ 2;

✓ для защиты АС до 1Б включительно (гостайна с грифом «совершенно секретно»).

Последняя версия Secret Net Studio 8.5 имеет действующий сертификат:

• 5 класс защищенности СВТ
• 4 уровень контроля НДВ
• 4 класс защиты СКН
• 4 класс защиты САВЗ
• 4 класс защиты СОВ
• 4 класс защиты МЭ тип “В”

Продукт сертифицирован для защиты:

• значимых объектов критической информационной инфраструктуры (КИИ) до 1категории включительно;
• государственных информационных систем (ГИС) до К1 включительно;
• информационных систем персональных данных (ИСПДн) до У31 включительно;
• автоматизированных систем управления технологическими процессами (АСУ ТП) до К1 включительно.

----------Слайд 34----------

Давайте далее рассмотрим концепцию разработчиков СЗИ ОТ НСД:

Угрозы информационным системам		
Угрозы данным	**Угрозы системе**	**Угрозы сети**
• Утечки данных; • Вымогательство за расшифровку; • Кража данных.	• Заражение вредоносным ПО; • Закрепление в системе; • Несанкционированный доступ к данным; • Несанкционированное изменение прикладного ПО.	• Горизонтальное распространение злоумышленника; • Перехват трафика; • Распространение червей.
Угрозы средствам защиты		
• Отключение пользователем • Отключение злоумышленником • Ограничение функциональности		

Защита от угроз		
Защита данных	**Защита системы**	**Защита сети**
Самозащита и контроль целостности		

----------Слайд 35----------

Архитектура и средства управления

Вы узнаете:

Об общей архитектуре СЗИ от НСД Secret Net;

• О вариантах функционирования системы Secret Net (сетевой и автономный вариант);

• О назначении, принципах функционирования основных компонент системы и их взаимодействии;

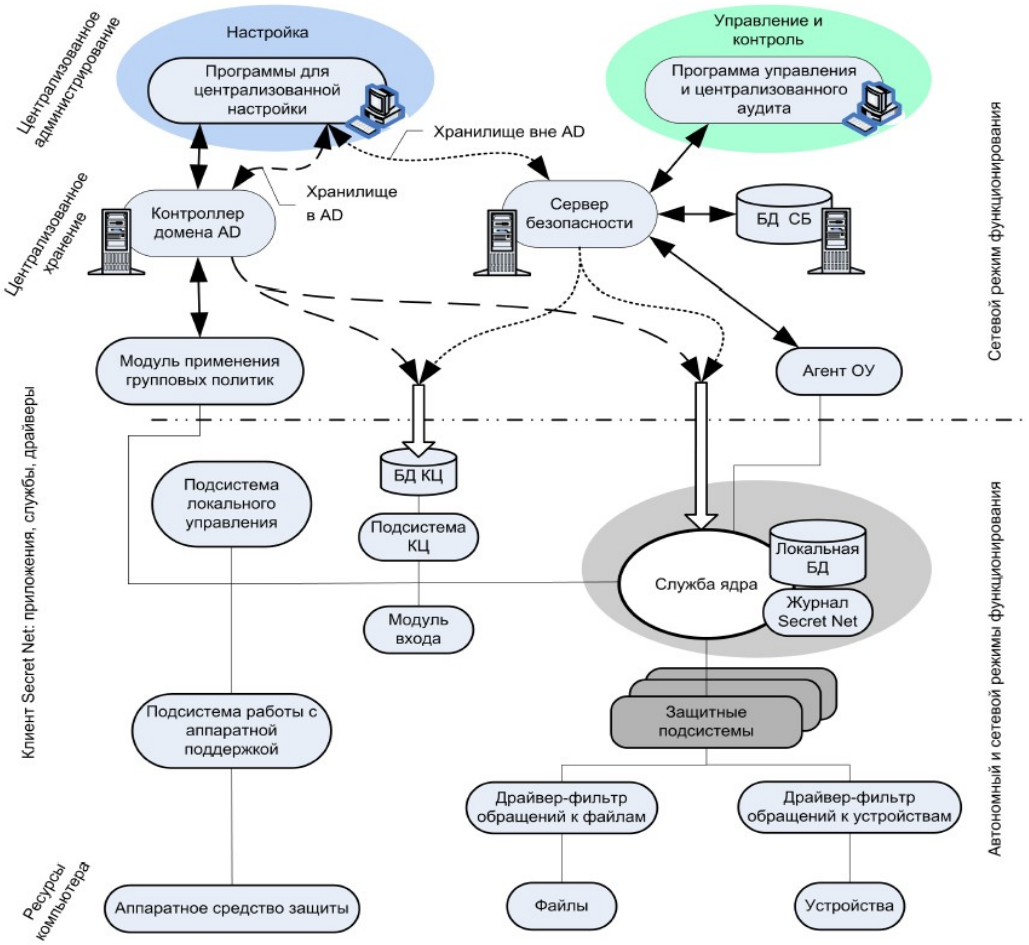
Общая архитектура

Основные возможности комплекса **«Secret Net»:**

- идентификация пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty, Proximity и т.п.);
- аутентификация по паролю длиной до 16 символов;
- поддержка автоматической смены пароля пользователя по истечении заданного интервала времени;
- аппаратная поддержка защиты от несанкционированной загрузки ОС с гибкого диска и CD-ROM диска;
- разграничение доступа пользователей к ресурсам компьютера с помощью механизмов дискреционного и мандатного управления доступом;
- создание для любого пользователя ограниченной замкнутой среды программного обеспечения (списка разрешенных для запуска программ);
- управление временем работы всех пользователей;
- возможность объединения пользователей в группы для упрощения управления их доступом к совместно используемым ресурсам;

- регистрация действий пользователя в системном журнале;
- поддержка для каждого пользователя индивидуальных файлов Config.sys и Autoexec.bat;
- защита компьютера от проникновения и размножения вредоносных программ;
- контроль целостности средств защиты, среды выполнения программ и самих прикладных программ;
- гибкие средства администрирования системы защиты с использованием механизма привилегий, позволяющего распределить административные функции между различными пользователями компьютера.

Обобщенная структурная схема взаимодействия основных компонентов системы Secret Net представлена на следующем рисунке.



Основные подсистемы клиента Secret Net

Клиент системы Secret Net включает следующие основные компоненты и подсистемы:

- служба ядра;
- подсистема локального управления;
- защитные подсистемы;
- модуль входа;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой.

Ядро

Служба ядра автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Она осуществляет управление подсистемами и компонентами и обеспечивает их взаимодействие.

Ядро выполняет следующие функции:

• обеспечивает обмен данными между компонентами клиента и обработку поступающих команд;

• обеспечивает доступ других компонентов системы к информации, хранящейся в локальной базе данных Secret Net;

• обрабатывает поступающую информацию о событиях, происходящих на компьютере и связанных с безопасностью системы, и регистрирует их в журнале Secret Net.

Подсистема локального управления

Подсистема локального управления обеспечивает:

• управление объектами защиты (устройствами, файлами, каталогами);

• управление параметрами пользователей и защитных механизмов;

• взаимодействие с локальной БД Secret Net;

• формирование заданий на контроль целостности;

• просмотр локальных журналов.

----------Слайд 36----------

Защитные подсистемы

Со службой ядра взаимодействуют следующие защитные подсистемы:

• **Замкнутая программная среда** – предотвращает запуск неразрешенного программного обеспечения (ПО).

• **Затирание данных** – обеспечивает затирание содержимого удаленных файлов.

• **Защита дисков** – обеспечивает защиту информации на локальных дисках при несанкционированной загрузке компьютера.

• **Разграничение доступа к устройствам** — обеспечивает разграничение доступа к заданным устройствам компьютера (портам, USB-устройствам, локальным дискам и др.).

• **Теневое копирование** – сохраняет в специальном хранилище копии выводимых данных (например, файлов).

• **Полномочное управление доступом** – обеспечивает хранение категорий конфиденциальности ресурсов, разграничение доступа к этим ресурсам и контроль потоков конфиденциальной информации в системе.

• **Контроль печати** – обеспечивает контроль вывода документов на печать (в том числе и конфиденциальных).

----------Слайд 37----------

Политика разграничения прав доступа

Прозрачная политика прав доступа с использованием меток конфиденциальности

• Работа с конфиденциальными данными возможна только в соответствующей сессии (*например: сессия гостайны*);

• Информация не может быть скопирована в документ или хранилище более низкого уровня допуска;

• Строгий запрет на вывод, изменение, удаление информации неавторизованными лицами.

Права доступа распространяются на все ресурсы системы

• Выдача прав SN в соответствии с корпоративными ролями/уровнями допуска.

Многофакторная аутентификация

• Задание политики сложности паролей
• Вход по идентификатору/смарт-карте
• Совместный режим работы с ПАК «Соболь».

----------Слайд 38----------

МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

Метки назначаются на:
Сессии пользователя;
Ресурсы системы;
Файлы и каталоги.

СЗИ от НСД позволяет обеспечить защиту:

1. При входе в систему (**Контроль доступа в систему**) прохождение процедуры идентификации, аутентификации, авторизации.
2. При обращении к файлам, директориям и NTFS-потокам **(Контроль доступа к файлам, директориям и NTFS-потокам —** обеспечивает хранение категорий конфиденциальности ресурсов, разграничение доступа к этим ресурсам и контроль потоков конфиденциальной информации в системе.**)**
3. При обращении к устройствам (**Контроль устройств** — обеспечивает разграничение доступа к заданным устройствам компьютера (портам, USB-устройствам, локальным дискам и др.).
4.) При обращении к печатающим устройствам (**Контроль печати** — обеспечивает контроль вывода документов на печать (в том числе и конфиденциальных).

Избирательное управление доступом

Избирательное разграничение доступа к локальным ресурсам компьютера осуществляется на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа. Управление доступом к локальным ресурсам файловой системы осуществляется с помощью стандартных средств управления ОС Windows в программе "Проводник". Дополнительно в Secret Net реализованы механизмы разграничения доступа к устройствам (дискам, портам и другим устройствам) и принтерам, управление которыми осуществляется с помощью средств управления политиками в специальном разделе параметров Secret Net.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, формируемых и поддерживаемых в актуальном состоянии механизмом контроля подключения и изменения устройств.

Система Secret Net предоставляет следующие возможности для разграничения доступа пользователей к устройствам:

• установка стандартных разрешений и запретов на выполнение операций с устройствами;

• назначение устройствам категорий конфиденциальности или допустимых уровней конфиденциальности сессий пользователей для управления доступом с использованием механизма полномочного разграничения доступа.

Возможности по разграничению доступа зависят от типов устройств. Разграничение доступа пользователей не осуществляется полностью или частично для устройств, имеющих особую специфику использования или необходимых для функционирования компьютера. Например, не ограничивается доступ к процессору и оперативной памяти, отсутствуют некоторые возможности разграничения доступа для портов ввода/вывода.

Полномочное разграничение доступа

Механизм полномочного разграничения доступа (называемый также механизм полномочного управления доступом) обеспечивает:

• разграничение доступа пользователей к информации, которой назначена категория конфиденциальности (конфиденциальная информация);

• контроль подключения и использования устройств с назначенными категориями конфиденциальности;

• контроль потоков конфиденциальной информации в системе;

• контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;

• контроль печати конфиденциальных документов.

По умолчанию в системе предусмотрены следующие категории конфиденциальности: "неконфиденциально" (для общедоступной информации), "конфиденциально" и "строго конфиденциально". При необходимости можно увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации. Максимально возможное количество категорий – 16.

Категорию конфиденциальности можно назначить для следующих ресурсов:

• локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;

• каталоги и файлы на дисках с файловой системой NTFS.

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска. Если уровень допуска пользователя ниже, чем категория конфиденциальности ресурса, система блокирует доступ к этому ресурсу. После получения доступа к конфиденциальной информации уровень конфиденциальности программы (процесса) повышается до категории конфиденциальности ресурса, чтобы все сохраняемые данные имели эту категорию конфиденциальности.

Полномочное разграничение доступа на уровне устройств осуществляется следующим образом. Если устройство подключается во время сеанса работы пользователя, уровень допуска которого ниже, чем категория конфиденциальности устройства, система блокирует подключение устройства. При подключении такого устройства до начала сеанса работы пользователя – запрещается вход пользователя в систему. В режиме контроля потоков уровень конфиденциальности сессии пользователя должен соответствовать заданным категориям

конфиденциальности всех подключенных устройств.

----------Слайд 39-40----------

ДОПОЛНИТЕЛЬНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ

Шифрование контейнеров

• Данные на жестком диске и съемных носителях хранятся в зашифрованном контейнере;

• Для пользователя контейнер отображается как подключаемый локальный диск.

Контроль целостности данных

• Расчет контрольных сумм от данных и сравнение с эталонным значением;

• Администратор Сервера Безопасности оперативно получает уведомление о нарушении целостности информации.

Создание теневых копий

• При копировании информации на съемные носители, а также отправке документов на печать.

Гарантированное удаление данных

• Уничтожение конфиденциальной информации без возможности последующего восстановления специализированными средствами.

Замкнутая программная среда

• предотвращает запуск неразрешенного программного обеспечения (ПО).

Защита дисков

• обеспечивает защиту информации на локальных дисках при несанкционированной загрузке компьютера.

----------Слайд 41----------

ЭШЕЛОНИРОВАННАЯ ЗАЩИТА SECRET NET

ЭТАП ПРОНИКНОВЕНИЯ

Задачи:

• Защита от несанкционированного входа в систему;
• Защита от проникновения во внутреннюю сеть;
• Через атаку на сетевой сервис;
• Через атаку с помощью USB устройства.

Механизмы Secret Net:

• Система обнаружения и предотвращения вторжений (СОВ);
• Контроль устройств;
• Идентификация, аутентификация.

Система обнаружения и предотвращения вторжений

• Защищает от проникновения злоумышленника во внутреннюю сеть организации через внешние каналы.

Контроль устройств

• Запрещает использование неавторизованных съемных носителей информации, предотвращая занесение вредоносного ПО в систему с зараженных устройств.

----------Слайд 42----------

Идентификация и аутентификации пользователей

Модуль входа

Совместно с ОС Windows модуль входа в систему обеспечивает:

• обработку входа пользователя в систему (проверка возможности входа, оповещение остальных модулей о начале или завершении работы пользователя);
• блокировку работы пользователя;
• функциональный контроль работоспособности системы;
• загрузку данных с персональных идентификаторов пользователя;
• усиленную аутентификацию пользователя при входе в систему.

----------Слайд 43----------

Механизм защиты входа в систему

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся следующие средства:

• средства для идентификации и аутентификации пользователей;
• средства блокировки компьютера;
• аппаратные средства защиты от загрузки ОС со съемных носителей.

----------Слайд 44----------

В системе Secret Net идентификация пользователей может выполняться в следующих режимах:

• "По имени" – пользователь может войти в систему, выполнив ввод имени и пароля или используя аппаратные средства, стандартные для ОСWindows;

• "Смешанный" – пользователь может войти в систему, выполнив ввод имени и пароля, а также использовать персональный идентификатор, поддерживаемый системой Secret Net;

• "Только по идентификатору" – каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net.

Усилить защиту компьютеров можно с помощью следующих режимов:

• режим разрешения интерактивного входа только для доменных пользователей – в этом режиме блокируется вход в систему локальных пользователей (под локальными учетными записями);

• режим запрета вторичного входа в систему – в этом режиме блокируется запуск команд и сетевых подключений с вводом учетных данных другого пользователя (не выполнившего интерактивный вход в систему).

----------Слайд 45----------

Блокировка компьютера

Средства блокировки компьютера предназначены для предотвращения несанкционированного использования компьютера. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора.

Блокировка при неудачных попытках входа в систему

Для пользователей могут быть установлены ограничения на количество неудачных попыток входа в систему. В дополнение к стандартным возможностям ОС Windows (блокировка учетной записи пользователя после определенного числа попыток ввода неправильного пароля) система Secret Net контролирует неудачные попытки аутентификации пользователя по ключевой информации.

Если в режиме усиленной аутентификации пользователь определенное количество раз предъявляет неверную ключевую информацию, система блокирует компьютер. Разблокирование компьютера осуществляется администратором. Счетчик неудачных попыток обнуляется при удачном входе пользователя или после разблокирования компьютера.

Временная блокировка компьютера

Режим временной блокировки включается в следующих случаях:

• если пользователь выполнил действие для включения блокировки;

• если истек заданный интервал неактивности (простоя) компьютера.

Блокировка компьютера при работе защитных подсистем

Блокировка компьютера предусмотрена и в алгоритмах работы защитных подсистем. Такой тип блокировки используется в следующих ситуациях:

• при нарушении функциональной целостности системы Secret Net;

• при нарушении аппаратной конфигурации компьютера (попытки подключения неразрешенных устройств и изменения параметров устройств);

• при нарушении целостности контролируемых объектов.

Блокировка компьютера администратором оперативного управления

В сетевом режиме функционирования блокировка и разблокирование защищаемого компьютера могут осуществляться удаленно по команде пользователя программы оперативного управления.

----------Слайд 46----------

Программно-аппаратный комплекс «Соболь»

Подсистема обеспечивает взаимодействие с устройствами аппаратной поддержки системы Secret Net и состоит из следующих компонентов:

1. Модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
2. Модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
3. Драйверы устройств аппаратной поддержки (если они необходимы).

ПАК "Соболь" 4.2 Возможности:

• Идентификация и аутентификация пользователей до загрузки ОС.
• Идентификация и аутентификация во время входа пользователя после загрузки ОС.
• Идентификация и аутентификация во время входа пользователя с удаленного компьютера.
• Запрет загрузки ОС со съемных носителей (аппаратно-программный модуль доверенной загрузки).
• Усиленный контроль целостности на рабочих станциях и серверах до загрузки ОС.
• Снятие временной блокировки компьютера.
• Хранение в идентификаторе пароля и криптографического ключа.

Поддерживаемые идентификаторы:

1. USB-ключ Guardant ID, JaCarta-2 PKI/ГОСТ, Rutoken ЭЦП и Rutoken Lite.
2. Смарт-карты Рутокен ЭЦП SC и Рутокен Lite и более ранние версии.
4. Персональная электронная карта(ПЭК).

----------Слайд 46----------

ЭТАП ВНУТРЕННЕГО РАСПРОСТРАНЕНИЯ

Задачи решаемые СЗИ от НСД:

• Защита от распространения злоумышленника во внутренней сети.
• Защита от перехвата трафика.
• Защита от распространения вирусов во внутренней сети

Механизмы Secret Net:

• Межсетевой экран
• Авторизация сетевых соединений

Фильтрация трафика:

• На основе IP-Адресов и сетевых портов;
• Имени пользователя;
• Приложения;
• Времени.

Виртуальная сегментация сети

• Создание нескольких виртуальных сегментов в одной подсети;
• Шифрование трафика при обмене между машинами виртуального сегмента;
• Взаимная аутентификация машин в рамках одного виртуального сегмента.

Запрет доступа к серверному приложению до тех пор, пока не проведен ряд проверок

• Проверка пользователя;
• Взаимная аутентификация АРМ пользователя и сервера;
• Проверка приложения, которое запрашивает доступ.

----------Слайд 47----------

КОНЕЧНЫЙ ЭТАП АТАКИ

Задачи:

• Защита от заражения вредоносным ПО
• Защита от несанкционированного изменения прикладного ПО
• Защита от закрепления злоумышленника в системе

Механизмы Secret Net:

• Замкнутая программная среда (ЗПС)
• Контроль целостности
• Антивирус
• Паспорт ПО

Замкнутая программная среда – Гарантирует запуск на компьютере только разрешенных приложений/ скриптов из белого списка.

Замкнутая программная среда

Механизм замкнутой программной среды позволяет определить для любого пользователя компьютера индивидуальный перечень программного обеспечения, разрешенного для использования. Система защиты контролирует и обеспечивает запрет использования следующих ресурсов:

• файлы запуска программ и библиотек, не входящие в перечень разрешенных для запуска и не удовлетворяющие определенным условиям;

• сценарии, не входящие в перечень разрешенных для запуска и не зарегистрированные в базе данных.

Примечание.

Сценарий (называемый также скрипт) представляет собой последовательность исполняемых команд и/или действий в текстовом виде. Система Secret Net контролирует выполнение сценариев, созданных по технологии Active Scripts.

Попытки запуска неразрешенных ресурсов фиксируются как события НСД в журнале Secret Net. На этапе настройки механизма составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически на основании сведений об установленных на компьютере программах или по записям журналов, содержащих сведения о запусках программ, библиотек и сценариев. Также предусмотрена возможность ручного формирования списка.

Для файлов, входящих в список, можно включить режим контроля целостности. По этой причине механизм замкнутой программной среды и механизм контроля целостности используют единую модель данных.

Механизм замкнутой программной среды не осуществляет блокировку запускаемых программ, библиотек и сценариев в следующих случаях:

• при наличии у пользователя привилегии "Замкнутая программная среда: Не действует" (по умолчанию привилегия предоставлена администраторам компьютера) – контроль запускаемых пользователем ресурсов не осуществляется;

• при включенном "мягком" режиме работы подсистемы замкнутой программной среды – в этом режиме контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО.

Этот режим обычно используется на этапе настройки механизма.

Механизмы контроля и регистрации

Система Secret Net включает в свой состав следующие средства, позволяющие контролировать ее работу:

• механизм регистрации событий;

• механизм контроля целостности.

Подсистема контроля целостности обеспечивает проверку неизменности ресурсов (каталогов, файлов, ключей и значений реестра) компьютера. Хотя данная подсистема и выполняет контролирующие функции, она не включена в состав защитных подсистем, так как выполняет контроль не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию).

Механизм регистрации событий

В процессе работы системы Secret Net события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале Secret Net. Все записи журнала хранятся в файле на системном диске. Формат данных идентичен формату журнала безопасности ОС Windows.

Предоставляются возможности для настройки перечня регистрируемых событий и параметров хранения журнала. Это позволяет обеспечить оптимальный объем сохраняемых сведений с учетом размера журнала и нагрузки на систему. Механизм контроля целостности

Механизм контроля целостности осуществляет слежение за неизменностью контролируемых объектов. Контроль проводится в автоматическом режиме в соответствии с заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков (последние только при использовании ПАК "Соболь"). Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т. е. на наличие файлов по заданному пути.

В системе предусмотрена возможность выбора времени контроля. В частности, контроль может быть выполнен при загрузке ОС, при входе пользователя в систему, по заранее составленному расписанию. При обнаружении несоответствия могут применяться различные варианты реакции на возникающие ситуации нарушения целостности, например, регистрация события в журнале Secret Net, блокировка компьютера.

Вся информация об объектах, методах, расписаниях контроля сосредоточена в модели данных. Модель данных хранится в локальной базе данных системы Secret Net и представляет собой иерархический список объектов и описание связей между ними. В модели используются следующие категории объектов в порядке от низшего уровня иерархии к высшему: ресурсы, группы ресурсов, задачи, задания и субъекты активности (компьютеры, пользователи, группы компьютеров и пользователей). Модель, включающая в себя объекты всех категорий, между которыми установлены связи, – это подробная инструкция системе Secret Net, определяющая, что и как должно контролироваться.

Модель данных является общей для механизмов контроля целостности и замкнутой программной среды.

Антивирусный модуль – Обновляемая база доверенных сигнатур позволяет распознать вредоносную активность.

Паспорт ПО – Инструмент администратора ИБ для выявления новых исполняемых файлов и библиотек.

Дополнительно: Особенности сетевого варианта:

- усиленная идентификация и аутентификация;
- криптографическая защита данных;
- централизованный мониторинг состояния безопасности информационной системы и управление защитными механизмами.

Сетевой вариант «Secret Net» предоставляет администратору безопасности возможность централизованного управления защитными механизмами клиентов «Secret Net», мониторинга состояния безопасности информационной системы, оперативного управления рабочими станциями в случае попыток НСД, централизованной обработки журналов регистрации и генерации отчетов.

Важное место в области систем разграничения доступа занимают аппаратно-программные системы идентификации и аутентификации (СИА), или устройства ввода идентификационных признаков (термин соответствует ГОСТ Р 51241-98), предназначенные для обеспечения защиты от НСД к компьютерам. При использовании СИА доступ пользователя к компьютеру осуществляется только после успешного выполнения процедуры идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности пользователю предъявленного им идентификационного признака осуществляется в процессе аутентификации.

В состав СИА входят аппаратные идентификаторы, устройства ввода-вывода (считыватели, контактные устройства, адаптеры, разъемы системной платы и др.) и соответствующее ПО. Идентификаторы предназначены для хранения уникальных идентификационных признаков. Кроме этого они могут хранить и обрабатывать конфиденциальные данные. Устройства ввода-вывода и ПО осуществляют обмен данными между идентификатором и защищаемым компьютером.

Слабым звеном названных средств является уникальный элемент. Если нарушитель каким-либо образом получил этот самый элемент и предъявил системе защиты, то она воспринимает его, как "своего" и разрешает действовать в рамках того субъекта, секретным элементом которого несанкционированно воспользовались.

Для устранения данных недостатков были разработаны различные механизмы, из которых широкое распространение получили *системы построения защищённых виртуальных сетей (Virtual Private Network, VPN), обнаружения атак и анализа защищенности.*

Задание и методические указания на самостоятельную подготовку

1. Изучить конспект лекций.
2. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – с. 22-42 (*Подготовиться к ПЗ №*5).
3. Войцеховский С.В., Калиниченко С.В.. Архитектура и программное обеспечение современных компьютерных систем и сетей войск ВКО: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – с. 192-220 (*Детальней изучить механизмы защиты Secret Net*).

4. Базовая модель угроз безопасности ПД при их обработке в информационных системах ПД (выписка). ФСТЭК России, 2008. – с. 21-23, 24-27 (*Выписать возможности внутренних нарушителей*).

5. Изучить эксплуатационные документы «Методические рекомендации по настройке СЗИ от НСД Secret Net» (получить у преподавателя на самоподготовке).

Методические рекомендации преподавателю по проведению лекции:

Во вступительной части преподавателю объявить тему, цель учебные вопросы и последовательность проведения занятия, отметить значимость для обучающегося знание угроз безопасности информации, связанных с НСД в специальных АС.

Готовность обучающихся к занятию проверить по наличию у них рекомендованной литературы, рабочих тетрадей с записями, сделанными в них при подготовке к данному занятию, а также в ходе проведения опроса или коллоквиума.

Коллоквиум проводится в письменной форме. По результатам индивидуального опроса преподаватель выставляет оценки в журнал учета учебных занятий. Обучающимся, недостаточно подготовленным к занятию, дать задание по устранению недостатков и установить время повторного ответа, после чего перейти к отработке первого учебного вопроса.

Отработку учебных вопросов проводить в соответствии с планом проведения занятия. В ходе лекции преподавателю контролировать действия обучающихся, добиваясь полного выполнения замысла лекции. В случае возникновения технических неполадок в используемом материально-техническом обеспечении принимать немедленные меры по приведению его в рабочее состояние, привлекая для этого при необходимости, инженера лаборатории.

При проверке ответов на контрольные вопросы оценивать краткость, конкретность и правильность ответов.

Оценку за выполнение занятия выставить в журнал учета учебных занятий записав, при необходимости, замечания, направленные на улучшение подготовки.

В заключительной части подвести итоги занятия, объявить оценки. Напомнить о необходимости иметь в наличии конспект лекции, кто по каким-либо причинам отсутствует на данном занятии; установить для этого дату и время. Объявить тему следующего занятия и дать указания на подготовку к нему. Тема следующего занятия «Общие сведения о компьютерных вирусах».

Методические рекомендации (задания) для слушателей и курсантов:

Для успешного прохождения тестирования необходимо накануне занятия изучить материал предыдущих лекций. В начале занятия будет произведен опрос курсантов по изученному теоретическому материалу в виде тестирования. Продолжительность опроса – до 10 минут.

В ходе лекции конспектировать материал в тетради. На занятиях проявлять активность, помня, что результаты текущего контроля отражаются на возможности освобождения от сдачи промежуточной аттестации.

Старший преподаватель 27 кафедры
подполковник
С.Краснов