**Тема № 2: Методы и средства защиты информации от НСД.**

**Тема лекции: Защита от НСД на примере развертывания СЗИ Secret Net и АПМДЗ «Соболь».**

**Учебные вопросы:**

1. Назначение и особенности СЗИ от НСД Secret Net.
2. Реализуемые функции защиты СЗИ от НСД Secret Net.

Программно-аппаратный комплекс Secret Net, получивший новое название – Secret Net Studio, предназначен для защиты информации от несанкционированного доступа в ЛВС, функционирующих под управлением ОС Microsoft Windows: для АРМ – Windows 7, а для серверов – Windows Server. Аппаратную составляющую комплекса обеспечивает электронный замок «Соболь».

Обеспечивает построение защищенных АС до класса 1Б включительно по требованиям РД АС.

Secret Net обладает следующими важными достоинствами:

* двухуровневое описание состояния системы защиты, позволяющее создать уровень “как должно быть”, формально описывающий положения принятой в организации политики безопасности, и уровень “как есть на самом деле”, отражающий реально действующие настройки средств защиты для ресурсов корпоративной сети (компьютеров, пользователей, устройств и т.д.);
* создание объектов управления доступом, отображающих реальные объекты предметной области (например, “сотрудник”, “задача, решаемая сотрудником”, “автоматизированное рабочее место” “помещение, в котором расположено автоматизированное рабочее место” и другие объекты);
* документоориентированный подход к управлению системой защиты, который позволяет управлять доступом к ресурсам при помощи формализованных электронных документов (заявок), а также контролировать состояние информационной безопасности корпоративной сети с помощью типовых отчетных документов, принятых в организации (формуляры АРМ, формуляры задач, перечни пользователей и их полномочий, перечни нарушений и т.п.);
* смешанное управление безопасностью, обеспечивающее централизованное управление основными настройками системы, сбором, обработкой и анализом сведений от всех средств защиты, используемых в корпоративной сети, а также децентрализованное изменение необходимых настроек системы защиты на местах с последующим отображением этих изменений в центральной базе данных;
* привлечение к созданию формального описания политики безопасности различных категорий пользователей корпоративной сети (специалистов управлений автоматизации, разработчиков прикладных систем, др. сотрудников);
* использование на серверах и рабочих станциях активных агентов, позволяющих обеспечить смешанное управление безопасностью и формирование контура “как есть”, а также синхронизацию изменений, происходящих как в центральной базе данных системы защиты, так и в локальных базах данных на рабочих местах;
* модульность и наращиваемость системы. Эти свойства упрощают ввод системы защиты в эксплуатацию и поэтапную активизацию возможностей системы путем подключения дополнительных компонент.

В качестве аппаратных средств в Secret Net используются:

* электронный замок «Соболь» - аппаратно-программный модуль доверенной загрузки, обеспечивающий доверенную загрузку ОС и модулей защиты и защиту от несанкционированной начальной загрузки нештатной ОС с внешних носителей;
* электронные идентификаторы (Рутокен, iButton и др.), которые обеспечивают двухфакторную аутентификацию пользователей при их доступе в АС (для класса 1Б допускается использовать только iButton).

Secret Net содержит все необходимые механизмы защиты информации от несанкционированного доступа:

* доверенная загрузка (защита от загрузки с внешних носителей);
* идентификация и аутентификация пользователей;
* разграничение доступа пользователей к информации и ресурсам автоматизированной системы;
* контроль печати конфиденциальной информации;
* избирательное (дискреционное) и полномочное (мандатное) управление доступом;
* контроль целостности программ и данных;
* гарантированное уничтожение данных;
* контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик;
* централизованное управление системой защиты, оперативный мониторинг, аудит безопасности;
* защита терминальных сессий при использовании АРМ как «тонких клиентов» при доступе к терминальному сервису (серверу).

Secret Net 7 построен по архитектурам «клиент – сервер» и «агент – менеджер». Использование этих архитектур позволяет централизованно управлять безопасностью большого количества компьютеров, принимать и обрабатывать информацию о происходящих событиях за счет следующих механизмов:

* регистрация событий рабочих станций;
* контроль действий сотрудников и администраторов;
* контроль потоков конфиденциальной информации;
* механизм отчетов.

Secret Net может быть успешно развернут в сложной доменной сети с большим количеством сегментов.

Возможности:

Система централизованного управления.

Оперативный мониторинг и аудит.

Мониторинг.

Аудит.

***Архитектура системы Secret Net***

*Состав и назначение подсистем*

Система Secret Net состоит из трех основных частей (рис.1):



Рисунок 1 – Архитектура системы Secret Net

Общая схема размещения частей системы Secret Net на рабочих станциях и серверах автоматизированной системы (рис. 2).



Рисунок 2 – Размещение составных частей Secret Net на компьютерах АС

*Состав серверной части Secret Net рис. 3.*



Рисунок 3 - Компоненты серверной части системы Secret Net

Состав подсистемы управления представлен на рисунке ниже (Рис. 4).



Рисунок 4 - Состав подсистемы управления

События, происходящие в информационной системе, регистрируются в ряде журналов (Таблица 1):

Таблица 1 - Журналы регистрации событий

| **Название журнала** | **Содержание** |
| --- | --- |
| Журнал заданий встречной синхронизации | Содержит записи, необходимые для изменения базы данных системы защиты при обратной синхронизации |
| Журнал событий | Содержит записи обо всех событиях, произошедших на защищаемых рабочих станциях и серверах |
| Журнал событий НСД | Содержит записи о событиях НСД, произошедших на защищаемых рабочих станциях и серверах |
| Системный журнал | Содержит записи, регистрирующие внутренние события сервера безопасности |
| Журнал событий аудита | Содержит регистрационные записи об управляющих действиях администраторов разных уровней |

На рисунке (Рисунок 5) представлена схема размещения и взаимодействия компонент и подсистем, входящих в состав клиентской части системы Secret Net.



Рисунок 5- Компоненты клиентской части системы Secret Net

На рисунке ниже (Рис. 6) представлена схема размещения и взаимодействия модулей и компонент, входящих в состав подсистемы идентификации.



Рисунок 6 - Компоненты подсистемы идентификации

Подсистема контроля целостности, программу расчета, пакеты контроля целостности (Рисунок 7).



Рисунок 7 - Компоненты подсистемы контроля целостности

На рисунке ниже (Рисунке 8) представлена подсистема полномочного управления доступом.



Рисунок 8 - Компоненты подсистемы полномочного управления доступом

***В.2. Реализуемые функции защиты***

*Защита от несанкционированного входа в систему*

Внешняя защита предназначена для предотвращения доступа посторонних пользователей к защищенному компьютеру. (Рисунок 9):



Рисунок 9 - Средства внешней защиты компьютера

*Механизм идентификации и аутентификации пользователей*

*Функция временной блокировки компьютера*

*Функция программной защиты от загрузки с внешнего носителя*

*Аппаратные средства внешней защиты*

В системе Secret Net предусмотрена аппаратная поддержка внешней защиты. Она обеспечивается электронным замком «Соболь». Аппаратные средства внешней защиты обеспечивают: защиту от загрузки операционной системы со съемных носителей и проникновения в систему, минуя внешнюю защиту, а также идентификацию пользователя с помощью аппаратных средств идентификации (iButton, RuToken и др.).Режимы работы с аппаратными средствами идентификации представлены в таблице ниже (Таблица 2).

Таблица 2 - Режимы работы с аппаратными средствами идентификации

| **Режим** | **Описание** |
| --- | --- |
| Мягкий | Любой пользователь может войти в систему двумя способами:  1) предъявив персональный идентификатор,  2) указав свое имя |
| Обычный | Определенным пользователям вход в систему разрешен только при предъявлении персонального идентификатора; остальные пользователи могут войти в систему двумя способами:  1) предъявив персональный идентификатор,  2) указав свое имя |
| Усиленный | Определенные пользователи могут войти в систему двумя способами:  1) предъявив персональный идентификатор,  2) указав свое имя; остальным пользователям вход в систему разрешен только при предъявлении персонального идентификатора |
| Жесткий | Вход в систему любого пользователя разрешен только при предъявлении персонального идентификатора |

*Управление доступом пользователей к ресурсам*

*Объекты управления и защиты*

Все объекты системы Secret Net подразделяются на два основных типа (Рисунок 10).



Рисунок 10 - Объекты системы защиты

В таблице ниже (Таблица 3) приводится перечень ресурсов компьютера, защищаемых средствами системы Secret Net, в соответствии с типом, к которому они принадлежат.

Таблица 3 - Состав защищаемых ресурсов компьютера

| **Тип ресурса** | **Состав** |
| --- | --- |
| Ресурсы файловой системы | Локальные логические диски и размещающиеся на них каталоги и файлы |
| Аппаратные ресурсы | Локальные и сетевые принтеры, коммуникационные порты, физические диски, дисководы, приводы DVD |
| Ресурсы операционной системы | Системные файлы, ключи системного реестра, системное время, диалоги настройки параметров системы |

*Механизмы разграничения доступа*

Система Secret Net включает в свой состав следующие средства разграничения доступа пользователей к ресурсам компьютера:

* механизм избирательного управления доступом;
* механизм полномочного управления доступом;
* механизм замкнутой программной среды.

«Сферы влияния» механизмов разграничения доступа по отношению к различным типам ресурсов компьютера представлены на рисунке (Рис. 11).



Рисунок 11 - Используемые механизмы разграничение доступа к ресурсам

*Механизм избирательного управления доступом*

Система защиты Secret Net использует стандартные механизмы Windows для избирательного управления доступом (Рис. 12). Непосредственное управление осуществляется с помощью диалогов Secret Net. Избирательный доступ на основе предоставления прав и привилегий.



Рисунок 12 - Условия доступа при использовании механизма избирательного управления

*Механизм полномочного управления доступом*

Система Secret Net включает в свой состав средства, позволяющие организовать полномочное (мандатное) управление доступом пользователей к конфиденциальной информации. (Рисунок 13).



Рисунок 13 - Условия допуска к конфиденциальной информации

*Механизм замкнутой программной среды*  (Рисунок 14).



Рисунок 14 - Схема использования замкнутой программной среды

Пользователь не сможет запустить программы, не входящие в этот список, в том числе и с гибких дисков, даже если они ему доступны.

*Средства контроля работы системы защиты*

*Механизм регистрации событий*

*Механизм контроля целостности*

Механизм контроля целостности используется в системе Secret Net для повышения надежности работы системы защиты. Он осуществляет проверку целостности следующих объектов:

* системных программ – ядра и исполняемых файлов системы;
* разрешенных для запуска программ замкнутой программной среды при включенном режиме контроля целостности;
* других файлов, список которых определен администратором системы защиты;
* ключей системного реестра.

Для всех проверяемых объектов составляются пакеты контроля целостности. В пакетах содержатся контрольные суммы проверяемых объектов и полный путь к каждому из них. Контрольные суммы рассчитываются с использованием хеш-функций (в соответствии с ГОСТ Р 34.10 в режиме имитовставки) или по оригинальному (быстрому) алгоритму собственной разработки.

**Встроенные средства предотвращения утечек информации из состава Secret Net 7**

СЗИ НСД Secret Net 7 в закрытой ЛВС за счет встроенных средств обеспечивает реализацию следующих функций предотвращения утечек информации (DLP):

* контроль устройств;
* контроль потоков закрытой информации;
* контроль печати закрытой информации;
* теневое копирование.

**Вопросы?**