Лекция №5

С.А. Краснов

Защита информации от НСД

# Защита информации от НСД

Лекция №5.

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

Тема лекции: Защита информации от НСД.

**Изучаемые вопросы:**

1. Цели, функции и методы защиты информации в АС от НСД.

2. Современные средства защиты информации от НСД. Основные функции средств защиты информации от НСД.

1. **Цели, функции и методы защиты информации в АС от НСД.**

В соответствии с РД «Концепция защиты СВТ и АС от НСД» 30 марта 1992 мы можем выделить основные способы НСД:

1. **Непосредственное обращение к объектам доступа**;

2. **Создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты**;

3. **Модификация средств защиты, позволяющая осуществить НСД**;

4. **Внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД**.

Перед тем, как перейти непосредственно к рассмотрению способов защиты от НСД, определим основные принципы защиты информации:

1. Защита *основывается* на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

2. Защита СВТ *обеспечивается* комплексом программно-технических средств.

3. Защита АС *обеспечивается* комплексом программно-технических средств и поддерживающих их организационных мер.

4. Защита АС *должна обеспечиваться* на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5. Программно-технические средства защиты *не должны* существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

6. Неотъемлемой частью работ по защите является *оценка эффективности* средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.

7. Защита АС *должна предусматривать* контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Цели, функции и методы защиты информации в АС от НСД. Исходя из них, мы можем перейти к задачам защиты информации **(рисунок 1)**:

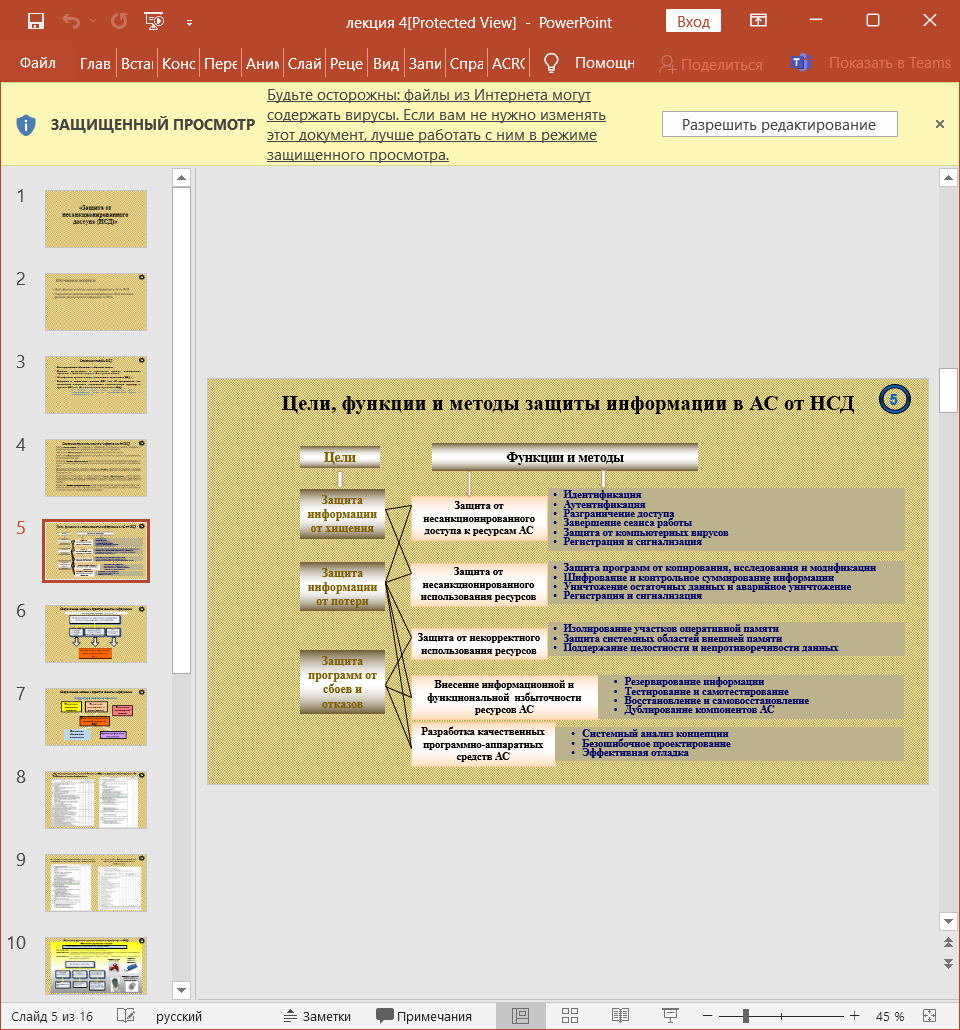


Рисунок 1

Защита от НСД в локальных вычислительных сетях (ЛВС) и отдельных компьютеров, а также в открытых сетях, например, в сети Internet, требует качественного решения **трех базовых задач**:

1. ЗИ на уровне отдельных компьютеров и ЛВС.

2. Защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды.

3. Защиты информации в процессе передачи по открытым каналам связи (через Internet).

Для этих целей проектируются и создаются *программно-аппаратные СЗИ* от несанкционированного доступа, которые в общем случае можно разделить на:

|  |  |  |
| --- | --- | --- |
| **1. СЗИ на уровне отдельных компьютеров и ЛВС** | ЗИ от внутреннего нарушителя | «Secret Net», «Dallas Lock», «Аккорд-АМДЗ», «Спектр-Z», «Панцирь» |
| **2. СЗИ отдельных ПК и ЛВС со стороны внешней среды** | ЗИ от внешнего нарушителя | МЭ, средства антивирусной защиты, средства обнаружения атак, системы анализа защищенности (сканеры безопасности) и др. |
| **3. СЗИ на уровне сети Интернет** | ЗИ в процессе передачи ее по внешним каналам связи | Средства создания VPN – например АПКШ “Континент” |

Все программно-аппаратные средства защиты информации от несанкционированного доступа включают в себя так называемую подсистему управления СЗИ, которая реализуется в рамках *СЗИ от НСД*, условно **состоящей** из следующих подсистем **(Слайд 7)**:

— Подсистемы управления доступом;

— Подсистемы регистрации и учета;

— Криптографической подсистемы;

— Подсистемы обеспечения целостности,

— Подсистемы антивирусной защиты,

— И подсистемы управления СЗИ, предназначенной для эффективного управления вышеназванными подсистемами.

Исходя из *требований* регулятора **функции подсистем СЗИ** зависят от класса АС и представлены в документе: - «РД. АС. Защита от НСД к информации. Классификация АС. Требования по ЗИ».

**Классы защищенности СВТ** представлены в документе: - РД. «СВТ. Защита от НСД к информации показатели защищенности от НСД к информации».

Можно выделить следующие основные *группы механизмов защиты*:

— механизмы управления доступом;

— механизмы регистрации и учета;

— механизмы криптографической защиты;

— механизмы контроля целостности.

Первая **Подсистема управления доступом** является основополагающей для реализации защиты от НСД, т.к. - механизмы защиты данной подсистемы призваны непосредственно противодействовать НСД к информации **(рисунок 2)**.

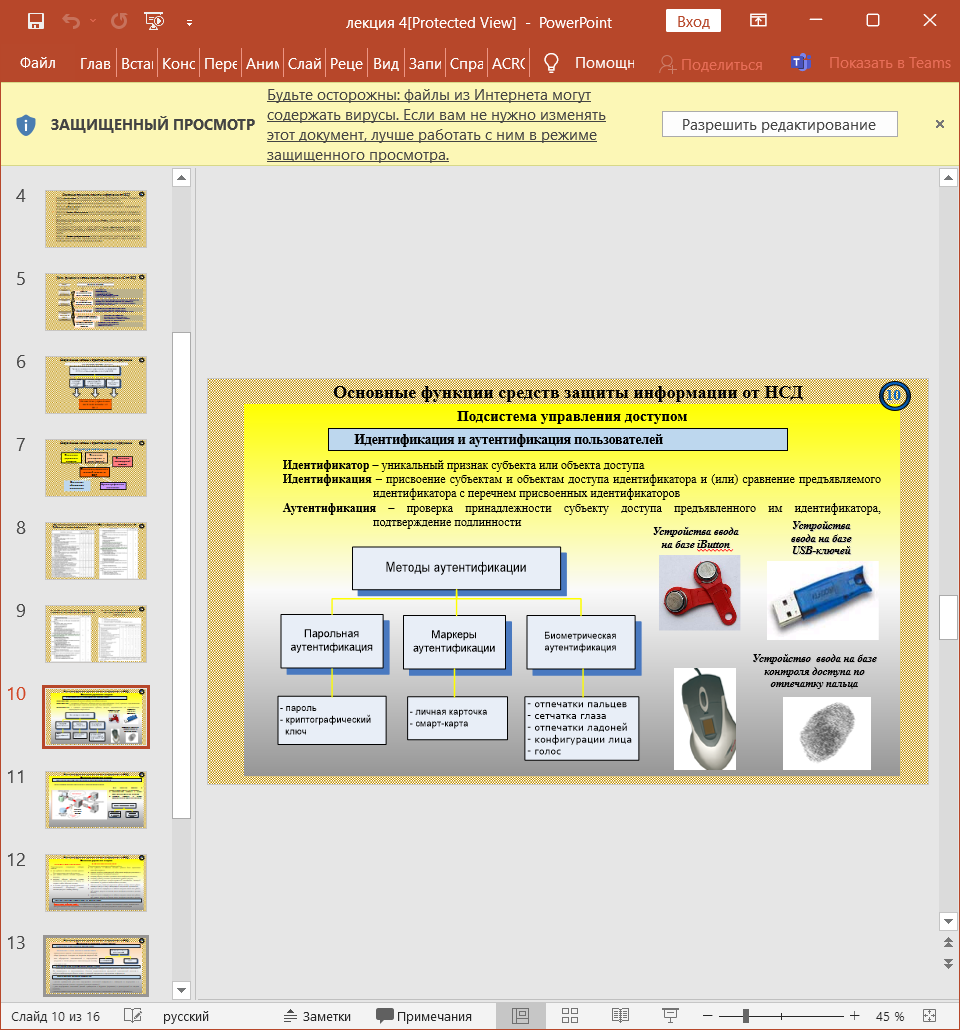


Рисунок 2

*Остальные же группы механизмов защиты* реализуются в предположении, что механизмы защиты первой группы могут быть преодолены злоумышленником.

**Идентификатор** присваивается пользователю, процессу или программно-аппаратному компоненту **(рисунок 2)**.

**Идентификация** позволяет субъекту назвать себя (сообщить свое «имя»).

**Аутентификация** бывает односторонней и двусторонней. Благодаря ей вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

*Методы аутентификации:*

* нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т.п.);
* нечто, чем он владеет (личную карточку, смарт-карта, устройства touch-memory, бейдж или иное устройство аналогичного назначения, IP-адрес, MAC-адрес);
* нечто, что есть часть его самого (голос, отпечатки пальцев, снимок сетчатки глаза и т.п., то есть свои биометрические характеристики).

Таким образом, *методами аутентификации* пользователей являются: **(рисунок 2)**

* Парольная аутентификация – простота и привычность;
* Маркеры аутентификации - не смогут предотвратить атаку с использованием уязвимых мест, поскольку они рассчитаны на правильный вход пользователя;
* Биометрическая аутентификация.

*Биометрические системы* - еще один механизм аутентификации, значительно уменьшающий вероятность угадывания пароля.

Биометрия представляет собой совокупность автоматизированных методов *идентификации* и/или *аутентификации* людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности *отпечатков пальцев*, *сетчатки* и *роговицы* глаз, *геометрия руки и лица* и т.п. К поведенческим характеристикам относятся *динамика подписи* (ручной), *стиль работы с клавиатурой*. На стыке физиологии и поведения находятся анализ *особенностей голоса* и *распознавание речи*.

Каждый подход предполагает использование определенного устройства для идентификации человеческих характеристик. Обычно эти устройства довольно сложны, чтобы исключить попытки обмана. Например, при снятии отпечатков пальцев несколько раз проверяются температура и пульс.

**(Слайд 11)** Далее система защиты должна постоянно контролировать правомерность доступа пользователя к компьютерным ресурсам. Для этого при попытке доступа любого пользователя к какому-либо ресурсу система защиты должна проанализировать его полномочия, находящиеся в своей БД, и разрешить доступ только в случае их соответствия **(Схема 1)**.

*Управление доступом (разграничение доступа) пользователей* – процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам.

*Логическое управление доступом*, реализуемое после идентификации и аутентификации пользователей, - это один из основных способов, призванный обеспечить конфиденциальность, целостность и подлинность информационных объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей.

Подсистема разграничения доступа к компьютерным ресурсам реализует *концепцию единого диспетчера доступа*, являющегося посредником при всех обращениях субъектов к объектам **(рисунок 3)**.

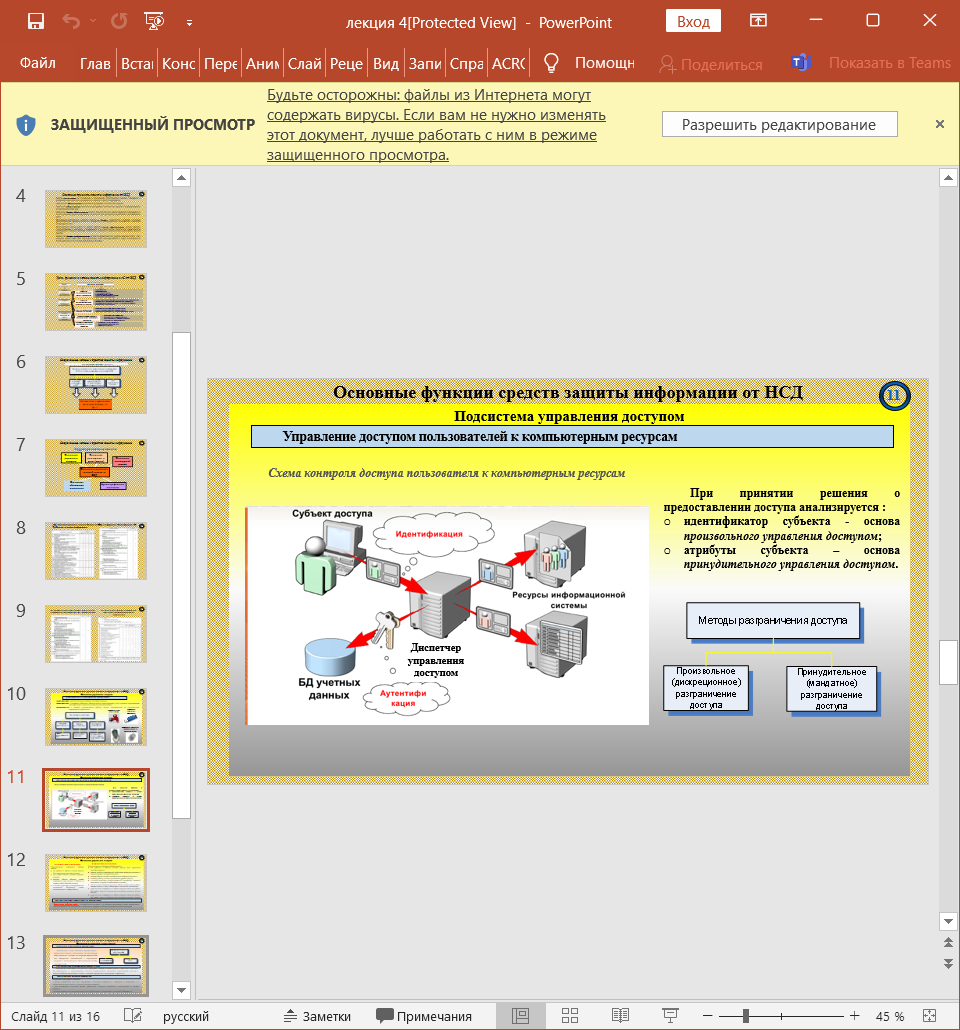


Рисунок 3

Диспетчер доступа должен выполнять следующие *функции*:

* проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты (правил разграничения доступа);
* при необходимости регистрировать факт доступа и его параметры в системном журнале регистрации.

При принятии решения о предоставлении доступа обычно анализируется следующая информация **(рисунок 3)**:

* идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.).
* атрибуты субъекта (метка безопасности, группа пользователя и т.п.).

Если при попытке доступа пользователя к компьютерным ресурсам подсистема разграничения определяет *факт несоответствия запроса на доступ пользовательским полномочиям*, то доступ блокируется, и могут предусматриваться следующие санкции за попытку НСД:

* предупреждение пользователя;
* отключение пользователя от вычислительной системы на некоторое время;
* полное отключение пользователя от системы до проведения административной проверки;
* подача сигнала службе безопасности о попытке несанкционированного доступа с отключением пользователя от системы;
* регистрация попытки несанкционированного доступа.

Основными методами разграничения доступа пользователей являются:

**Произвольное или дискреционное управление доступом** - это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту. Владельцем объекта, как правило, считается пользователь, создавший данный объект.

При **принудительном разграничении доступа** компьютерные ресурсы разделяются на группы в соответствии с *уровнями* секретности и *категориями* информации, к которым они относятся. В качестве уровней секретности могут быть выделены следующие:

• «несекретно»;

• «для служебного использования»;

• «секретно».

Категории образуют неупорядоченный набор, например - бухгалтерские документы, кадровые, производственные и т.д. Их назначение - описать предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по видам, что способствует лучшей защищенности.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются **метки безопасности**. Метка субъекта, называемая еще мандатом, задает:

• максимальный уровень секретности информации, доступ к которой ему разрешен;

• категории информации, к которой он допущен.

Метка объекта определяет степень закрытости и категории, содержащейся в нем информации.

*Создание замкнутой рабочей среды для пользователей*

Немаловажную роль играет создание для каждого пользователя ограниченной виртуальной среды, скрывающей запрещенные ресурсы и не предоставляющей средства доступа к этим ресурсам. С этой целью для рабочих станций достаточно создать замкнутое интерфейсное окружения. В этом случае можно заблокировать доступ к панели управления, системным дискам рабочих станций и установить список только разрешенных программ.

Подсистема регистрации и учета предназначена для регистрации в системных журналах (представляющих собой файлы на внешних носителях информации) различных событий, происходящих в системе.

Говоря о регистрации, часто различают такие понятия, как протоколирование и аудит.

**Протоколирование** предполагает сбор и накопление информации о событиях, происходящих в компьютерной системе, а **аудит** - анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

*При протоколировании сведений* по обращению к компьютерной системе и ее ресурсам рекомендуется фиксировать:

* дата и время поступления запроса (события);
* идентификатор пользователя, от имени которого выдан запрос;
* идентификатор компьютера (терминала), с которого поступил запрос;
* содержание сообщения в составе запроса (действия пользователя);
* реквизиты защиты (полномочия пользователей, пароли, коды, ключи и др.), используемые при выполнении запроса;
* время окончания использования ресурса.

Имея такие сведения в любой момент можно получить статистические данные относительно компьютеров (терминалов), пользователей и программ, запрашивающих доступ, а также сведения о результатах выполнения запросов и характере использования запрашиваемых ресурсов.

*Гарантированное* уничтожение *остаточных данных*

Если важный документ просто выбрасывается в мусорную корзину, то он становится добычей для злоумышленников. Секретные документы нужно разрезать на мелкие части. Канцелярская бумагорезательная машина дает дополнительный уровень защиты, измельчая документ в продольном и поперечном направлении.

Информацию в компьютерных системах можно восстановить после удаления, если она удалена неправильно. Это ОП, внешние накопители. Существуют коммерческие программы, которые стирают данные с магнитных носителей без возможности их восстановления, например, PGP desktop и BCWipe.

*Учёт машинных носителей информации*

Учёт машинных носителей информации предполагает выполнение следующих действий.

К **базовым** функциям *подсистемы обеспечения целостности информации* относятся:

*Контроль целостности программного и информационного окружения*

Эффективный контроль целостности программного и информационно окружения основано на проверке соответствия текущих характеристик информационных объектов их эталонным характеристикам.

Должны быть обеспечена целостность программных средств СЗИ от НСД, а также неизменность программной среды. При этом:

* целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;
* целостность программной среды обеспечивается качеством приемки любых программных средств в АС.

*Резервирование и восстановление информации*

Функции резервирования и восстановления информации, реализуемые в СЗИ от НСД, определяют, каким образом осуществляется резервное копирование данных. Наиболее важными функциями резервирования информации являются:

*1) Частота резервного копирования*

Как правило, конфигурация предусматривает проведение полного резервного копирования данных 1 раз в неделю с дополнительным резервным копированием, проводимым в остальные дни. Дополнительное резервное копирование сохраняет только файлы, изменившиеся с момента последнего резервирования, что сокращает время процедуры и обеспечивает меньший объем пространства на резервном носителе.

*2) Хранение резервных копий*

Необходимо хранить носители с резервными копиями в защищенных местах, которые, тем не менее, должны быть доступны в случае, если потребуется восстановить утерянные данные.

*3) Резервируемая информация*

Не каждый файл на компьютере требует ежедневного резервного копирования. Например, исполняемые системные файлы и файлы конфигурации практически не меняются, поэтому для них не обязательно ежедневное резервирование. Имеет смысл создать резервную копию системных файлов заранее и загружать их с надежного носителя, если требуется переустановить систему.

Файлы данных, в особенности часто изменяющиеся, должны резервироваться регулярно. В большинстве случаев необходимо осуществлять их ежедневное резервное копирование.

*Криптографическая защита хранящейся информации*

Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Это очень простой принцип. Вся сложность заключается в том, как реализуется весь этот процесс.

*Подсистема антивирусной защиты* является неотъемлемой частью системы защиты СЗИ от НСД. При её правильной настройке значительно уменьшается риск воздействия вредоносных программ.

Но никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам.

Вопросы?