***Лекция 30.***

**Методы и средства защиты сетей и межсетевой информации**

***План:***

***1. Методы и средства защиты информации***

***2. Средства защиты информации в сети Интернет***

***3. Защита межсетевой информации***

***Ключевые слова:*** *технические средства, программное обеспечение, несанкционированный доступ к информации, организационно-правовые методы, инженерно-технические методы, физические, программные, аппаратные, криптографические средства и методы, ЭЦП, VPN, протоколы PPTP, SKIP, IPSec, SSL, TSL, SOCKS, ESP, AH, межсетевые экраны*

**Методы и средства защиты информации**

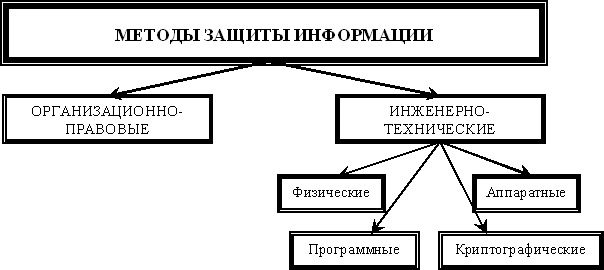
Компьютерные преступления чрезвычайно многогранные и сложные явления.

Объектами таких преступных посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты или программное обеспечение и базы данных, для которых технические средства являются окружением; компьютер может выступать как предмет посягательств или как инструмент.

Виды компьютерных преступлений чрезвычайно многообразны. Это и несанкционированный доступ к информации, хранящейся в компьютере, и ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, и разработка и распространение компьютерных вирусов, и хищение компьютерной информации.

Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

Среди всего набора методов защиты информации выделяют следующие:



Классификация методов защиты информации в компьютерных системах

К методам и средствам организационной защиты информации относятся *организационно-технические* и *организационно-правовые мероприятия*, проводимые в процессе создания и эксплуатации компьютерных сетей для обеспечения защиты информации.

Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будут размещаться компьютеры; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности компьютерной системы.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей.

*Инженерно-техническая защита* – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности.

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

1. *физические средства*, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;

2*. аппаратные средства* – приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств – обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;

3. *программные средства*, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбор, накопление, хранение, обработка и передача) данных;

4. *криптографические средства* – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на компьютере с использованием разнообразных методов шифрования.

**2. Средства защиты информации в сети Интернет**

Средства защиты информации в Интернете бывают:

* *техническими и технологическими*:
  + физическими – устройствами и системами, создающими препятствия на пути злоумышленников или дестабилизирующих факторов, сюда относятся и двери, замки и т.д.;
  + аппаратными – устройствами, встраиваемыми в ИС специально для защиты информации (могут создавать препятствия или шифровать данные);
  + программными – специализированным программным обеспечением, реализующим функции создания препятствий действиям злоумышленников, шифрующими данные или распределяющим уровни доступа;
* *законодательными* – правовыми инструментами, стандартами (на уровне предприятия это могут быть нормативы, права доступа и т.д.;
* *организационными*, в том числе сложившаяся практика обработки информации.

К организационным методам защиты информации от ее последующего распространения в сети можно назвать:

* ограничение публикуемого контента в социальных сетях (путешествия, обстановку своего жилья, ФИО друзей, даты дней рождения, номера телефонов и другую контактную информацию);
* использование сотрудниками специально созданных и не связанных с корпоративными аккаунтами личных аккаунтов;
* контроль предоставления персональной информации в банках, налоговых органах, на вокзалах, в авиа/железнодорожных кассах;
* контроль публикуемой на бейджах линейного персонала информации о работниках – достаточно должности и имени (зная ФИО сотрудника несложно найти его профиль в социальных сетях, т.е. однозначно идентифицировать личность);
* уничтожение бумажных носителей информации (бланков, отчетов), содержащих конфиденциальные данные;
* ограничение использования корпоративных аккаунтов, email для прохождения регистрации и авторизации в социальных сетях, на сайтах, в мобильных приложениях;
* предоставление взвешенной информации о сотрудниках, организации на сайте, в социальных сетях (официальных страницах, группах).

*Технологии защиты информации в сетях*

Основным способом защиты передаваемых данных является их шифрование.

Стойкость шифра зависит от сложности используемого алгоритма. Криптографические (математические) методы шифрования защищены от любых типов угроз, кроме физического доступа к носителям информации (с ключом шифрования).

Если передаваемые данные не являются секретными, а требуется лишь подтверждение их подлинности (подлинности подписей), то используется электронная цифровая подпись (ЭЦП). Подписанный ЭЦП электронный документ не защищен от несанкционированного доступа, однако не может быть изменен без сигнализации об этом.

**3. Защита межсетевой информации**

Одним из методов защиты межсетевой информации является технология виртуальных частных сетей (Virtual Private Network — VPN).

Программные средства построения VPN могут обеспечивать защищенную связь между двумя объектами сети на различных уровнях модели взаимодействия открытых систем OSI:

* *канальном*

— с использованием протоколов РРТР (Point to Point Tunnel Protocol), L2TP (Layer 2 Tunnel Protocol), L2F (Layer 2 Forwarding); VPN на канальном уровне обычно используется для соединения удаленного компьютера с одним из серверов ЛВС;

* *сетевом*

— с использованием протоколов SKIP (Simple Key management for Internet Protocol), IPSec (Internetwork Protocol Security); VPN на сетевом уровне могут использоваться как для соединения удаленного компьютера и сервера, так и для соединения двух ЛВС;

* *сеансовом*

— протоколы SSL, TLS (Transport Layer Security), SOCKS; VPN на сеансовом уровне может создаваться поверх VPN на канальном и сетевом уровнях.

Программные средства построения VPN создают так называемый туннель, по которому передаются зашифрованные данные. Построение VPN происходит на основе протокола SKIP.

Заголовок SKIP-пакета является стандартным IP-заголовком, и поэтому защищенный с помощью протокола SKIP пакет будет распространяться и маршрутизироваться стандартными устройствами любой ТСР/1Р-сети.

SKIP шифрует IP-пакеты, ничего не зная о приложениях, пользователях или процессах, их формирующих; он обрабатывает весь трафик, не накладывая никаких ограничений на вышележащее программное обеспечение.

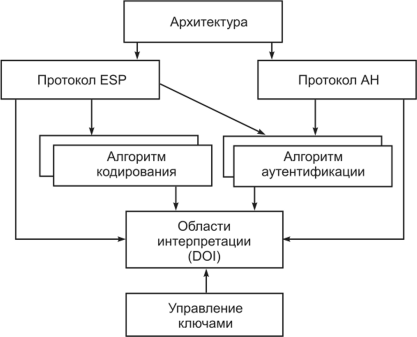
SKIP независим от сеанса: для организации защищенного взаимодействия между парой абонентов не требуется никакого дополнительного информационного обмена и передачи по каналам связи какой-либо открытой информации.

В основе SKIP лежит криптография открытых ключей Диффи — Хеллмана, которой пока в рамках такой сети, как Интернет, нет альтернативы.

Протокол SKIP базируется на открытых ключах, поэтому для подтверждения их подлинности можно использовать цифровые сертификаты, описанные в рекомендации ITU Х.509.

Дополнительная спецификация протокола определяет процедуру обмена информацией о поддерживаемых алгоритмах шифрования для данного узла защищенной сети.

Архитектура протокола IPSec приведена на рисунке.



Протокол заголовка аутентификации (Authentication Header — АН) предназначен для защиты от атак, связанных с несанкционированным изменением содержимого пакета, в том числе от подмены адреса отправителя сетевого уровня.

Протокол инкапсуляции зашифрованных данных (Encapsulated Security Payload — ESP) предназначен для обеспечения конфиденциальности данных.

Необязательная опция аутентификации в этом протоколе может дополнительно обеспечить контроль целостности зашифрованных данных.

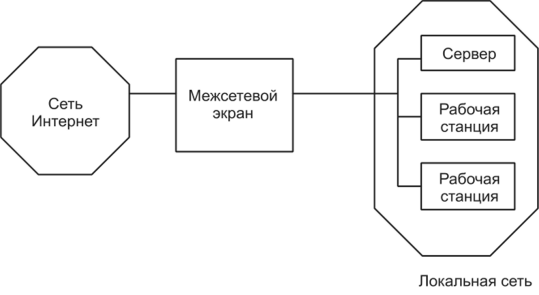
Различают два режима применения ESP и АН (а также их комбинации) — транспортный и туннельный:

* *транспортный режим* используется для защиты поля данных IP-пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета. Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, сведения о руководителях;
* *туннельный режим* предполагает защиту всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются VPN-сервером (например, межсетевым экраном организации) и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифрования межсетевым экраном начального заголовка сетевого уровня исходный пакет направляется получателю.

Среди программно-аппаратных и программных средств обеспечения информационной безопасности при работе в сети Интернет можно выделить межсетевые экраны, средства анализа защищенности (сканеры уязвимостей), системы обнаружения атак и системы контроля содержимого (контент-анализа, content filtering).

Межсетевые экраны (брандмауэры, firewall) реализуют набор правил, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной сети (открытой) в другую (защищенную).

Обычно межсетевые экраны устанавливаются между сетью Интернет и локальной вычислительной сетью организации, хотя могут размещаться и внутри корпоративной сети (в том числе на каждом компьютере — персональные). В зависимости от уровня взаимодействия объектов сети основными разновидностями межсетевых экранов являются фильтрующие маршрутизаторы, шлюзы сеансового уровня и шлюзы прикладного уровня.



**Контрольные вопросы:**

1. Виды компьютерных преступлений.
2. Перечислите методы защиты информации.
3. Организационно-правовая защита информации.
4. Инженерно-техническая защита информации.
5. Основная задача аппаратных средств защиты.
6. Перечислите средства защиты информации в сети Интернет.
7. Какой способ защиты является основным при передаче данных?
8. Понятие VPN.
9. На каких уровнях и какие протоколы использует VPN?
10. Что такое межсетевой экран?