Дата: 16.09.2021

Тема: Средства обеспечения безопасности информации

Компьютерная и сетевая безопасность

- При всем своем многообразии средства защиты информации делятся на два больших класса:
  - средства **компьютерной безопасности** предназначены для защиты внутренних информационных ресурсов, находящихся в локальной сети или на отдельном компьютере пользователя;
  - средства **сетевой безопасности** предназначены для защиты информации в процессе ее передачи через сеть.

Брандмауэр

- Для обеспечения **компьютерной безопасности** нужно защитить от несанкционированного доступа все ресурсы, находящиеся внутри локальной сети:
  - аппаратные ресурсы (серверы, дисковые массивы, маршрутизаторы),
  - программные ресурсы (операционные системы, СУБД, почтовые службы и т. п.),
  - данные, хранящиеся в файлах и обрабатываемые в оперативной памяти.
- Наиболее часто используемым средством защиты этого типа является **брандмауэр,** устанавливаемый в местах всех соединений внутренней сети с Интернетом.

Брандмауэр

- Брандмауэр представляет собой межсетевой экран, который контролирует обмен сообщениями, ведущийся по протоколам всех уровней, и не пропускает подозрительный трафик в сеть.
- Брандмауэр может использоваться и внутри сети, защищая одну подсеть от другой.
- Помимо брандмауэра аналогичные проблемы призваны решать **встроенные средства безопасности операционных систем и приложений, таких как базы данных, а также встроенные аппаратные средства компьютера.**

Механизм виртуальных частных сетей

- Сегодня Интернет используется предприятиями не только как **источник информации**, хранящейся на многочисленных веб-сайтах, но и как дешевая **транспортная среда**, позволяющая объединить сеть центрального отделения с сетями филиалов, а также подключить к ресурсам предприятия телекомпьютеров — сотрудников, находящихся дома или в командировке работающих с корпоративной сетью удаленно.
- При этом во многих случаях предприятию важно, чтобы передаваемая через Интернет информация не была искажена, уничтожена или просмотрена посторонними людьми.
- Для решения этой задачи сегодня широко используется **механизм виртуальных частных сетей (VPN).**

Безопасная информационная система

- **Безопасная информационная система** — это система, которая,
  - защищает данные от несанкционированного доступа,
  - всегда готова предоставить их своим пользователям,
  - надежно хранит информацию и гарантирует неизменность данных.
- Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

Конфеденциальнсть, доступность, целостность данных

- **Конфиденциальность** — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
- **Доступность** — гарантия того, что авторизованные пользователи всегда получат доступ к данным.
- **Целостность** — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Конфиденциальность, доступность, целостность данных

- Целью злоумышленников может быть нарушение каждой их составляющих информационной безопасности — **доступности, целостности или конфиденциальности.**
- Требования безопасности могут меняться в зависимости от
  - назначения системы,
  - характера используемых данных,
  - типа возможных угроз.

Сервисы сетевой безопасности

- Средства обеспечения безопасности, называемые также **сервисами сетевой безопасности** (программные и аппаратные продукты, предназначенные для защиты данных), включают в себя следующие процедуры:
  - Шифрование информации,
  - Аутентификацию,
  - Идентификация,
  - Авторизацию,
  - Аудит,
  - Технология защищенного канала.

Шифрование

- **Шифрование** — это краеугольный камень всех систем информационной безопасности.
- Любая процедура шифрования, превращающая информацию из обычного «понятного» вида в «нечитабельный» зашифрованный вид, естественно должна быть дополнена процедурой дешифрирования, которая после применения к зашифрованному тексту снова делает его «понятным».
- Пара процедур — шифрование и дешифрирование — называется **криптосистемой.**

Аутентификация

- **Аутентификация** предотвращает доступ к сети нежелательных лиц и разрешает вход для легальных пользователей.
- Термин «аутентификация» в переводе с латинского означает «установление подлинности».
- В качестве объектов, требующих аутентификации, могут выступать не только пользователи, но и различные устройства, приложения, текстовая и другая информация.
- Аутентификация данных означает доказательство целостности этих данных, а также факт их поступления именно от того человека, который объявил об этом. Для этого используется механизм **электронной подписи.** Аутентификацию следует отличать от идентификации.

Идентификация

- **Идентификация** заключается в сообщении пользователем системе своего идентификатора.
- Идентификаторы пользователей применяются в системе с теми же целями, что и идентификаторы любых других объектов (файлов, процессов, структур данных), и они не всегда связаны непосредственно с обеспечением безопасности.

Авторизация

- **Авторизация** — процедура контроля доступа легальных пользователей к ресурсам системы с предоставлением каждому из них именно тех прав, которые определены ему администратором.
- Помимо предоставления пользователям прав доступа к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как
  - локальный доступ к серверу,
  - установка системного времени,
  - создание резервных копий данных,
  - выключение сервера.

Аудит

- **Аудит** — фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам.
- Подсистема аудита современных ОС позволяет дифференцированно задавать перечень интересующих администратора событий с помощью удобного графического интерфейса.
- Средства учета и наблюдения обеспечивают возможность обнаружить и зафиксировать важные события, связанные с безопасностью: попытки создать, получить доступ или удалить системные ресурсы.

Технология защищенного канала

- **Технология защищенного канала** обеспечивает безопасность передачи данных по открытой транспортной сети, например по Интернету, за счет:
  - взаимной аутентификации абонентов при установлении соединения;
  - защиты передаваемых по каналу сообщений от несанкционированного доступа;
  - обеспечения целостности поступающих по каналу сообщений.