Лекция 5. Сетевые характеристики: безопасность

Дисциплина: Сетевые технологии

Тема лекции: Сетевые характеристики: безопасность.

Цель лекции: изучить основные понятия компьютерной и сетевой безопасности, принципы защиты данных, а также сервисы и средства, которые обеспечивают безопасную работу компьютерных сетей.

Ключевые понятия: компьютерная безопасность, сетевая безопасность, конфиденциальность, целостность, доступность, аутентификация, авторизация, шифрование, межсетевой экран, антивирусная защита.

1. Компьютерная и сетевая безопасность

1.1. Понятие компьютерной безопасности

Компьютерная безопасность представляет собой совокупность мер, которые направлены на защиту компьютеров, программ, устройств и данных от несанкционированного доступа, повреждения, кражи и уничтожения.

Основная задача компьютерной безопасности заключается в защите информации и обеспечении правильной работы вычислительных устройств.

К основным объектам защиты относятся:

- аппаратное обеспечение;
- операционные системы и прикладные программы;
- файлы и базы данных;
- учетные записи пользователей;
- сетевые устройства;
- каналы передачи данных.

Например, пароль для входа в операционную систему защищает учетную запись пользователя. Антивирусная программа помогает обнаруживать вредоносные программы. Резервное копирование позволяет восстановить данные после их потери.

1.2. Понятие сетевой безопасности

Сетевая безопасность представляет собой совокупность технологий, правил и средств, которые обеспечивают защиту компьютерных сетей, сетевых устройств и передаваемой информации.

В компьютерных сетях данные передаются между компьютерами, серверами, маршрутизаторами и другими устройствами. Во время передачи информация может подвергаться перехвату, изменению или блокировке.

Поэтому сетевая безопасность направлена на решение следующих задач:

- предотвращение несанкционированного доступа к сети;
- защита данных во время передачи;
- обнаружение сетевых атак;
- ограничение доступа пользователей к ресурсам;
- обеспечение устойчивой работы сетевых служб;
- восстановление работы сети после сбоев и атак.

Пример. В университете создана локальная сеть, к которой подключены компьютеры преподавателей, студентов и сотрудников администрации. С помощью VLAN, списков контроля доступа и межсетевого экрана можно ограничить доступ студентов к административным серверам.

1.3. Различия между компьютерной и сетевой безопасностью

Компьютерная безопасность	**Сетевая безопасность**
Защита компьютера и его программ	Защита сети и сетевого обмена
Контроль доступа к файлам	Контроль доступа к сетевым ресурсам
Антивирусная защита устройства	Обнаружение сетевых атак
Защита операционной системы	Защита каналов передачи данных
Резервное копирование файлов	Защита сетевой инфраструктуры

Эти направления тесно связаны. Например, зараженный компьютер может стать источником атаки на другие устройства локальной сети.

2. Конфиденциальность, целостность и доступность данных

В основе информационной и сетевой безопасности лежит модель CIA, которая включает три основных принципа:

- Confidentiality, то есть конфиденциальность;
- Integrity, то есть целостность;
- Availability, то есть доступность.



2.1. Конфиденциальность (Confidentiality)

Конфиденциальность означает, что информация доступна только пользователям, которым разрешено ее просматривать.

Для обеспечения конфиденциальности применяются пароли, шифрование, разграничение прав доступа и многофакторная аутентификация.

Пример: студент не должен иметь доступ к ведомости с оценками других групп, если такие права ему не предоставлены.



2.2. Целостность (Integrity)

Целостность означает, что данные сохраняют правильность и не подвергаются несанкционированному изменению или уничтожению.

Для проверки целостности применяются хеш-функции, цифровые подписи, контрольные суммы и механизмы разграничения прав.

Пример: при передаче файла получатель может сравнить его хеш с исходным значением. Совпадение хешей подтверждает отсутствие изменений с высокой вероятностью, но само по себе не доказывает подлинность отправителя.



2.3. Доступность (Availability)

Доступность означает, что авторизованные пользователи могут получить доступ к данным и сетевым ресурсам в нужное время.

Для обеспечения доступности используются резервные серверы, резервные каналы связи, источники бесперебойного питания и резервное копирование.

Пример: если основной сервер университета выходит из строя, резервный сервер позволяет восстановить доступ к учебным материалам.

2.4. Взаимосвязь трех принципов безопасности

Все три принципа должны соблюдаться одновременно.

Например, если электронный журнал защищен паролем, но данные в нем могут быть изменены посторонним человеком, конфиденциальность обеспечена не полностью, а целостность нарушена.

Если данные защищены от изменения, но сервер недоступен из-за сетевой атаки, нарушается доступность.

Принцип	**Основная угроза**	**Средство защиты**
Конфиденциальность	Перехват или утечка данных	Шифрование, контроль доступа
Целостность	Несанкционированное изменение данных	Хеширование, цифровая подпись
Доступность	Отказ сервера, DDoS-атака	Резервирование, фильтрация трафика

3. Основные угрозы сетевой безопасности

Угроза сетевой безопасности представляет собой возможное событие или действие, которое может привести к нарушению конфиденциальности, целостности или доступности информации.

3.1. Вредоносное программное обеспечение

Вредоносные программы создаются для кражи данных, нарушения работы устройств или получения несанкционированного доступа.

К основным видам относятся:

- Вирусы: внедряют свой код в другие файлы или программы.
- Черви: распространяются между устройствами через сети.
- Троянские программы: маскируются под полезные приложения.
- Программы-вымогатели: блокируют доступ к данным или шифруют файлы с целью выкупа.
- Шпионские программы: собирают информацию о пользователе без его разрешения.

Для защиты применяются антивирусные программы, обновление операционных систем, фильтрация сетевого трафика и контроль запуска приложений.

3.2. Фишинг

Фишинг представляет собой способ обмана пользователя с целью получения паролей, банковских данных или другой конфиденциальной информации.

Злоумышленник может отправить электронное письмо со ссылкой на поддельную страницу входа. Если пользователь введет свои учетные данные, они могут попасть к злоумышленнику.

Для защиты необходимо проверять адрес отправителя, не открывать подозрительные ссылки и использовать многофакторную аутентификацию.

3.3. Перехват данных

Перехват данных возникает, когда посторонний человек получает доступ к информации во время ее передачи по сети.

Особенно опасны незащищенные каналы связи и поддельные точки доступа Wi-Fi.

Для защиты используются протоколы шифрования, например TLS, а также защищенные VPN-соединения.

3.4. DDoS-атаки

DDoS-атака представляет собой попытку сделать сетевой ресурс недоступным за счет большого количества запросов от множества устройств.

В результате сервер может перестать отвечать на запросы обычных пользователей.

Для защиты применяются фильтрация трафика, ограничение частоты запросов, распределение нагрузки и специализированные сервисы защиты от DDoS.

3.5. Несанкционированный доступ

Несанкционированный доступ возникает, когда пользователь получает доступ к данным или ресурсам без соответствующих прав.

Причинами могут быть слабые пароли, ошибки настройки сети, использование украденных учетных данных и отсутствие своевременных обновлений.

Для предотвращения таких случаев используются надежные пароли, разграничение прав доступа, многофакторная аутентификация и регулярная проверка настроек безопасности.

4. Сервисы сетевой безопасности

Сервисы сетевой безопасности представляют собой функции и механизмы, которые обеспечивают защиту информации и сетевого взаимодействия.

К основным сервисам относятся следующие.

4.1. Аутентификация

Аутентификация представляет собой проверку подлинности пользователя или устройства.

Она отвечает на вопрос: «Кто пытается получить доступ?»

Основные способы аутентификации:

- пароль;
- одноразовый код;
- аппаратный ключ безопасности;
- биометрические данные;
- многофакторная аутентификация.

Например, при входе в корпоративную сеть сотрудник вводит пароль и подтверждает вход с помощью одноразового кода.

4.2. Авторизация

Авторизация определяет, какие действия разрешены пользователю после успешной аутентификации.

Она отвечает на вопрос: «Что разрешено делать этому пользователю?»

Например, преподаватель может изменять оценки своей группы, а студент может только просматривать собственные оценки.

В компьютерных сетях авторизация реализуется с помощью списков контроля доступа (ACL), ролевых моделей и политик безопасности.

4.3. Шифрование данных

Шифрование преобразует исходную информацию в форму, которую нельзя прочитать без соответствующего ключа.

Шифрование защищает данные как при передаче по сети, так и при хранении на дисках.

Основные виды шифрования:

- Симметричное: для шифрования и расшифрования используется один секретный ключ.
- Асимметричное: используется пара ключей, открытый и закрытый.

Например, HTTPS использует TLS для защиты соединения между браузером и веб-сервером.

4.4. Контроль целостности

Контроль целостности позволяет обнаружить изменение данных.

Для этого применяются хеш-функции, коды аутентификации сообщений (MAC) и цифровые подписи.

Хеш-функция формирует значение фиксированной длины на основе исходных данных. Даже небольшое изменение файла обычно приводит к другому хеш-значению.

Цифровая подпись также позволяет проверить подлинность подписанта и выявить изменение подписанных данных при условии надежной проверки ключа подписи.

4.5. Межсетевой экран (Firewall)

Межсетевой экран контролирует сетевой трафик на основе установленных правил.

Он может разрешать или блокировать соединения в зависимости от IP-адресов, портов, протоколов и других параметров.

Например, межсетевой экран может разрешать доступ к веб-серверу через HTTPS, но блокировать подключения к административному порту из внешней сети.

4.6. Система обнаружения и предотвращения вторжений

Система обнаружения вторжений (IDS) анализирует сетевые события и сообщает о подозрительной активности.

Система предотвращения вторжений (IPS) может не только обнаруживать, но и автоматически блокировать определенные атаки.

Основные задачи IDS и IPS:

- выявление подозрительных соединений;
- обнаружение известных шаблонов атак;
- анализ сетевого трафика;
- формирование предупреждений;
- блокировка опасных запросов, если такая функция предусмотрена.

4.7. VPN

VPN (Virtual Private Network) создает защищенный канал связи между устройством пользователя и удаленной сетью либо другим узлом.

VPN часто использует шифрование для защиты данных при передаче через недоверенные сети.

Например, сотрудник может подключиться к корпоративной сети университета из дома через VPN. Доступ к внутренним ресурсам при этом должен дополнительно контролироваться.

4.8. Резервное копирование и восстановление

Резервное копирование позволяет сохранить копии важных данных для последующего восстановления.

Оно особенно важно при отказах оборудования, ошибочном удалении файлов и атаках программ-вымогателей.

Для повышения надежности рекомендуется хранить несколько копий данных, использовать разные носители и проверять возможность восстановления.

5. Дополнительные средства защиты компьютерных сетей

Помимо перечисленных сервисов, для защиты сети используются следующие средства.

Средство	**Назначение**
Антивирус	Обнаружение и удаление вредоносных программ
VLAN	Логическое разделение локальной сети на сегменты
ACL	Ограничение доступа к сетевым ресурсам
WPA2/WPA3	Защита беспроводных сетей Wi-Fi
TLS	Защита данных при передаче
Система журналирования	Регистрация событий безопасности
Резервный канал связи	Сохранение сетевого соединения при отказе основного канала
Система управления обновлениями	Устранение известных уязвимостей программного обеспечения

Важно учитывать, что VLAN разделяет сетевые сегменты, но сама по себе не обеспечивает полную защиту. Для ограничения обмена между VLAN применяются маршрутизаторы, межсетевые экраны и списки контроля доступа.

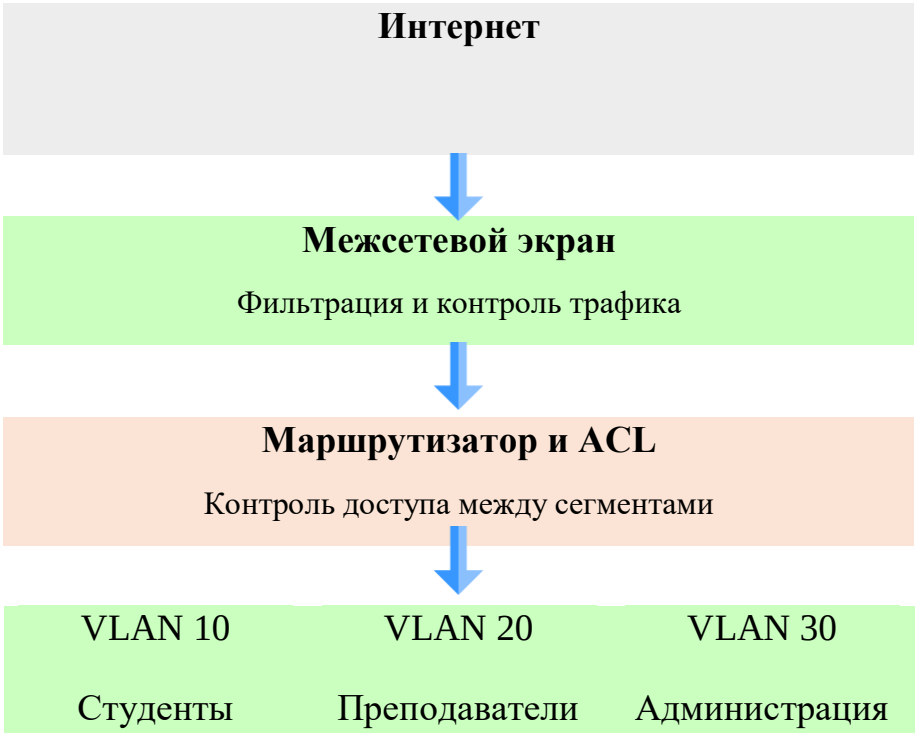
6. Практический пример обеспечения сетевой безопасности

Рассмотрим локальную сеть университета, в которой используются три группы устройств:

- компьютеры студентов;
- компьютеры преподавателей;
- серверы администрации.

Для защиты такой сети могут быть приняты следующие меры:

1. Созданы отдельные VLAN для каждой группы устройств.
2. Настроены ACL для ограничения доступа между сегментами.
3. Установлен межсетевой экран для контроля внешних соединений.
4. Включена аутентификация пользователей.
5. Для удаленного доступа организовано VPN-подключение.
6. Важные данные защищены резервным копированием.
7. Сетевые события записываются в журналы и проверяются администратором.



Упрощенная схема защиты локальной сети университета.

Такая организация сети помогает ограничить доступ к конфиденциальным ресурсам и уменьшить последствия возможной атаки. При этом безопасность зависит также от правильной настройки устройств, своевременных обновлений и соблюдения правил работы с информацией.

7. Основные правила обеспечения сетевой безопасности

Для снижения риска сетевых атак необходимо соблюдать следующие правила:

- использовать сложные и уникальные пароли;
- включать многофакторную аутентификацию;
- своевременно обновлять операционные системы и сетевые устройства;
- предоставлять пользователям только необходимые права;
- применять шифрование для защиты передаваемых данных;
- создавать резервные копии важных файлов;
- контролировать сетевой трафик и журналы событий;
- не открывать подозрительные ссылки и вложения;
- отключать неиспользуемые сетевые службы;
- регулярно проверять настройки безопасности.

Безопасность сети требует не только технических средств, но и правильных действий пользователей и администраторов.

Заключение

Компьютерная и сетевая безопасность необходимы для защиты устройств, информации и сетевых ресурсов. Основу защиты составляют три принципа: конфиденциальность, целостность и доступность данных.

Для реализации этих принципов используются аутентификация, авторизация, шифрование, межсетевые экраны, системы обнаружения вторжений, VPN и резервное копирование.

Эффективная защита достигается за счет совместного применения технических средств, правильной настройки сети и соблюдения правил информационной безопасности.

Контрольные вопросы

1. Что такое компьютерная безопасность?
2. Чем сетевая безопасность отличается от компьютерной безопасности?
3. Какие три принципа составляют модель CIA?
4. Что означает конфиденциальность данных?
5. Какими способами обеспечивается целостность информации?
6. Что такое доступность сетевых ресурсов?
7. Какие основные угрозы существуют в компьютерных сетях?
8. Чем аутентификация отличается от авторизации?
9. Для чего используется шифрование данных?
10. Какую функцию выполняет межсетевой экран?
11. Чем отличаются IDS и IPS?
12. Для чего применяется VPN?
13. Как VLAN и ACL помогают защитить локальную сеть?
14. Почему резервное копирование важно для сетевой безопасности?

Практическое задание

Тема: Анализ средств сетевой безопасности.

Представьте, что в компьютерном классе университета есть 20 компьютеров, сервер с учебными материалами и подключение к Интернету.

Выполните следующие задания:

1. Определите три возможные угрозы безопасности этой сети.
2. Укажите, какие угрозы нарушают конфиденциальность, целостность или доступность данных.
3. Предложите не менее четырех средств защиты сети.
4. Объясните, для чего в такой сети нужны межсетевой экран, VLAN и резервное копирование.
5. Составьте краткую схему защищенной сети университета.