МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт – Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

Специальность: 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

«Оператор электронно-вычислительных и вычислительных машин»

Преподаватель Рожков А.И.

Санкт-Петербург 2023

СПб ГУТ)))

ТЕМА 4.1. Защита информации при работе с офисными приложениями

Компьютерные сети и информационная безопасность.

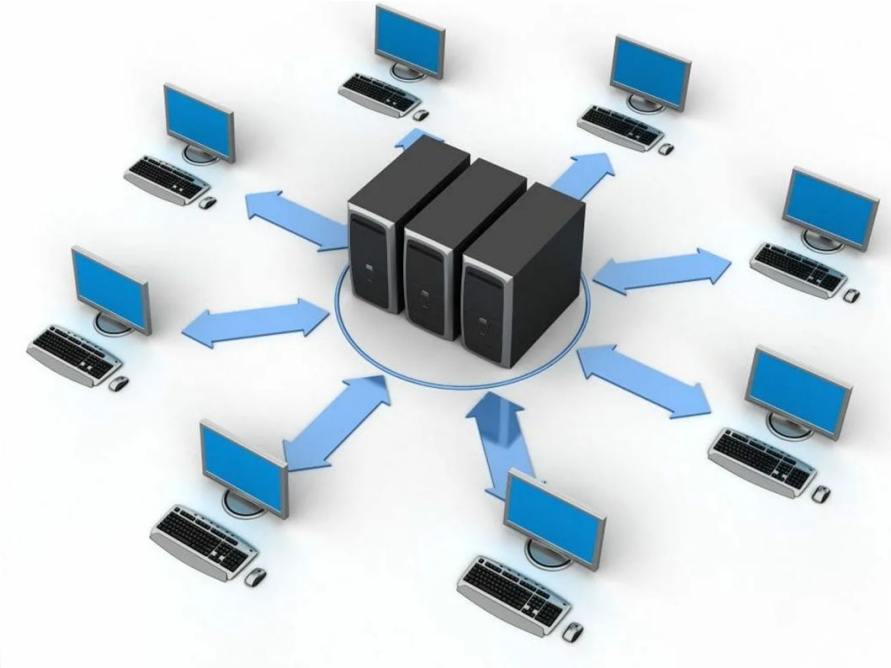
План занятия:

1. **Политика безопасности**
2. **Угрозы безопасности**
3. **Защита информации**

1. Политика безопасности

Компьютерная сеть образуется при физическом соединении (проводном или беспроводном) двух или более компьютеров для передачи данных между ними.

Главной целью объединения вычислительных устройств в сеть является удаленный доступ к разделяемым ресурсам.



Политика безопасности сети

Защита информации наиболее эффективна, когда в компьютерной сети поддерживается многоуровневая защита, которая складывается из следующих компонентов:

1. **политика безопасности локальной сети организации;**
2. **система защиты хостов локальной сети;**
3. **сетевой аудит;**
4. **защита на основе маршрутизаторов;**
5. **межсетевые экраны;**
6. **системы обнаружения вторжений;**
7. **план реагирования на выявленные атаки.**

Полная защита целостности сети зависит от реализации всех выше перечисленных компонентов защиты.

Использование многоуровневой защиты – это наиболее эффективный метод предотвращения НСД (несанкционированного доступа). Самым важным для функционирования защищенной сети является ее политика безопасности, которая определяет, что защищать и на каком уровне. Все остальные уровни защиты логически следуют после принятия для сети политики ее безопасности.

Проведение выбранной при создании сети организации ПБ предусматривает регулярный пересмотр этой политики и мер защиты, ее реализующих, что подразумевает:

- обновление политики и мер защиты безопасности, если это необходимо;
- проверку совместимости политики и мер защиты с существующей сетевой средой;
- разработку новых и удаление старых правил политики и мер защиты по мере необходимости.

ПБ можно разделить на две категории: административные политики и технические политики. В зависимости от этого ПБ базируется на правилах двух видов:

1. **Первая группа (административные политики) связана с заданием правил разграничения доступа ко всем ресурсам системы**,
2. **Вторая группа (технические политики) основана на правилах анализа сетевого трафика как внутри локальной сети, так и при его выходе из системы или входе в нее**.

В основе этих правил лежит принцип доверия. Определяя ПБ, нужно выяснить, насколько можно доверять людям и ресурсам.

Для первой группы правил главный вопрос заключается в том, кому и в какой степени в локальной сети можно доверять, имея в виду больше человеческий фактор, но, не забывая при этом и о запущенных в локальной сети процессах и приложениях.

Начальный этап задания этих правил состоит в определении тех, кто получает доступ. **Предварительные установки систем, обеспечивающих защиту информации в локальной сети, могут соответствовать принципу наименьшего доступа для всех.**

Далее для каждой группы пользователей и входящих в нее представителей определяются степени доверия. Компромиссное решение в данном случае и будет самым подходящим.

В данном контексте вопрос для второй группы правил звучит так: «**Каким пакетам в локальной сети доверять, а каким нет, ибо они могут циркулировать в локальной сети по инициативе злоумышленника**» Именно эти правила и являются главенствующими при установке и настройке основных систем анализа трафика в локальной сети и пакетных фильтров.

Для локальной сетей можно выделить три основные модели доверия:

- **либеральная** – доверять всем в течение всего времени работы;
- **запретительная** – не доверять никому и никогда;
- **разумная или компромиссная** – доверять иногда некоторым людям.

Обычно ПБ включает в себя следующие части:

2. **Предмет ПБ.** Перед описанием самой ПБ в данной области, нужно сначала определить саму область с помощью ограничений и условий в понятных всем терминах. Часто полезно ясно указать цель или причины разработки политики.
3. **Описание позиции организации.** Как только описан предмет ПБ, даны определения основных понятий и рассмотрены условия ее применения, в явной форме описывается позиция организации по данному вопросу.

3. **Применимость.** Это означает, что надо уточнить где, как, когда, кем и к чему будет применяться данная ПБ.
4. **Роли и обязанности.** Нужно указать ответственных лиц и их обязанности в отношении разработки и внедрения различных аспектов ПБ, а также в случае нарушения ПБ.
5. **Меры защиты.** Перечисляются конкретные меры, реализующие ПБ в организации, дается обоснование выбора именно такого перечня мер защиты и указывается, какие угрозы безопасности локальной сети наиболее эффективно предотвращаются какими мерами защиты.
6. **Соблюдение политики.** Для ПБ может оказаться уместным описание, с некоторой степенью детальности, нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно описаны наказания, применяемые к нарушителям ПБ.
7. **Ответственные,** или консультанты, по вопросам безопасности и справочная информация.

2. Угрозы безопасности

Атаки TCP/IP.

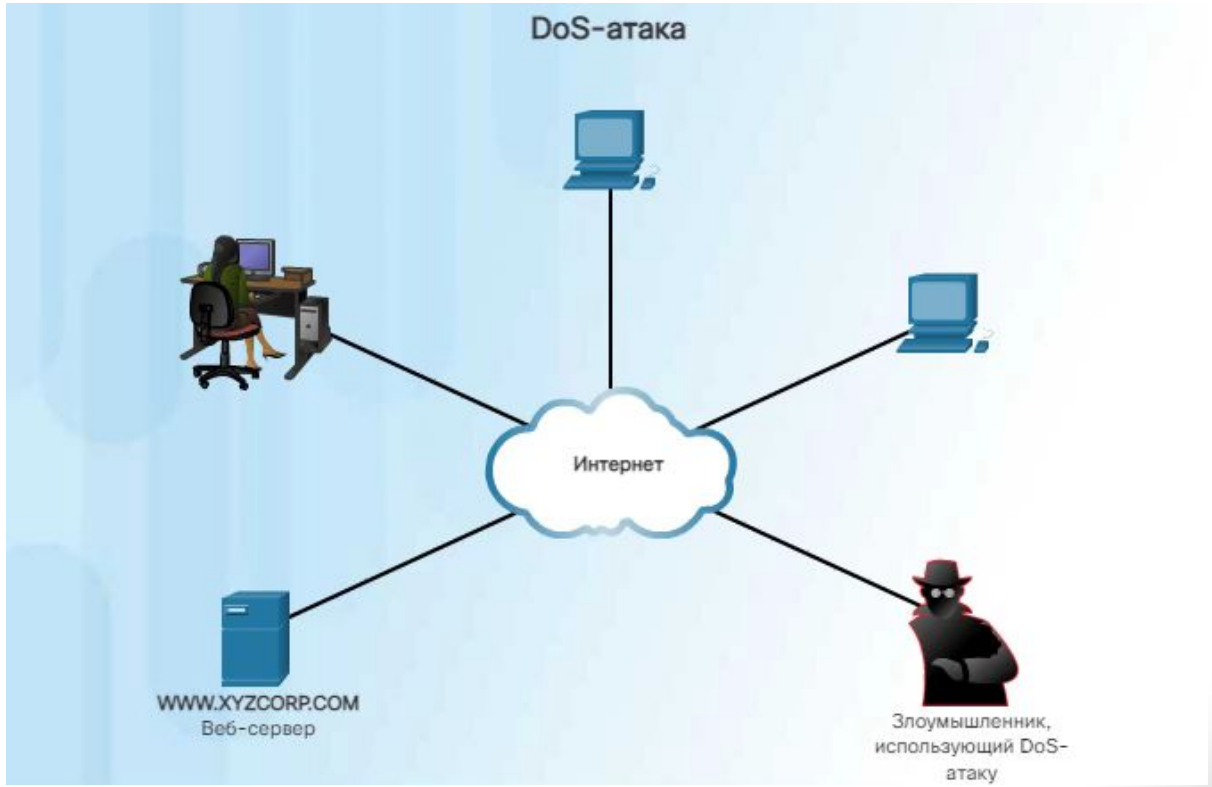
Для управления взаимодействия с Интернетом компьютер использует набор протоколов TCP/IP. К сожалению, некоторыми функциями TCP/IP можно манипулировать, что приводит к появлению уязвимостей в сети.

На рисунке перечислены основные типы атак, к которым уязвим протокол TCP/IP.

1. **DoS (Denial of Service, отказ в обслуживании) — тип атак, при которых создается чрезмерно большой объем запросов к сетевым серверам.** Злоумышленник нападает с целью вызвать перегрузку подсистемы, в которой работает атакуемый сервис. Воздействие осуществляется с одного сервера и нацелено на определенный домен или виртуальную машину.

Особенности DoS-атак:

- **Одиночный характер** – поток трафика запускается из одной-единственной подсети.
- **Высокая заметность** – попытки «положить» сайт заметны по содержимому лог-файла.
- **Простота подавления** – атаки легко блокируются при помощи брандмауэра.



2. **DDoS (Distributed Denial of Service, распределенный отказ в обслуживании) — атаки DDoS аналогичны атакам DoS, однако принципиальное отличие заключается в применении сразу нескольких хостов.** Сложность защиты от этого вида нападения зависит от количества машин, с которых осуществляется отправка трафика. Источником, как правило, оказываются «обычные сайты», предварительно зараженные вирусом или взломанные вручную. **Постепенно они образуют единую сеть, называемую ботнетом, и увеличивают мощность атаки.**

Особенности DDoS-атак:

- **Многопоточный характер** – такой подход упрощает задачу блокирования сайта, потому что быстро отсеять все атакующие IP-адреса практически нереально.
- **Высокая скрытность** – грамотное построение атаки позволяет замаскировать ее начало под естественный трафик и постепенно «забивать» веб-ресурс пустыми запросами.
- **Сложность подавления** – проблема заключается в определении момента, когда атака началась.

3. **Лавина SYN запросов (SYN flood) — запрос SYN представляет собой начальное сообщение, отправляемое для установления подключения TCP. Лавинная атака SYN открывает соединения со случайных портов TCP на источнике атаки и блокирует сетевое оборудование или компьютер большим числом ложных запросов SYN.** Это вызывает отказы в установлении сеансов для других клиентов. Атаки с использованием лавины SYN запросов относятся к атакам типа «отказ в обслуживании».

4. **Спуфинг (spoofing, подмена адресов) — при атаке с помощью подмены адресов компьютер маскируется под доверенный компьютер для получения доступа к ресурсам. Компьютер использует поддельный IP или MAC-адрес с целью выдать себя за компьютер, являющийся доверенным в сети.**

5. **Атака воспроизведения (replay) — для выполнения атаки с воспроизведением передача данных перехватывается и записывается злоумышленником и впоследствии повторно передается им от имени законного пользователя.** Например: A и B общаются через защищенный канал связи, а C подслушивает их переговоры. Позднее (не обязательно после завершения сеанса связи) C может повторить все сообщения одной из сторон. Например, A связывается с B и просит перевести на счет C деньги за какую-то услугу в банк и при этом он подписывает сообщение (то есть B уверен, что имеет дело именно с A).

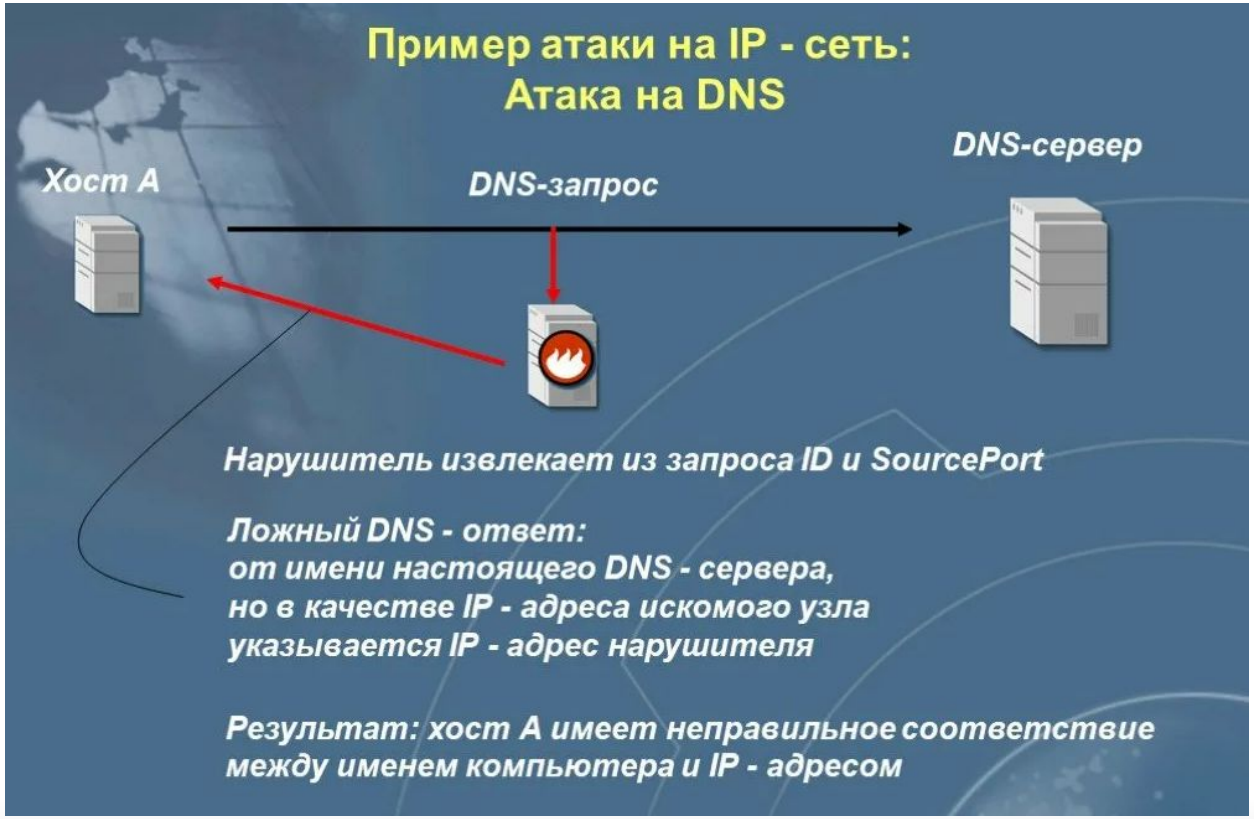
6. **Атаки типа «человек посередине» (man-in-the-middle, также атака незаконного посредника) — злоумышленник осуществляет атаку «человек посередине», перехватывая сообщения между компьютерами для хищения информации, передаваемой по сети. Атака «человек посередине» также может использоваться для манипулирования сообщениями и передачи ложной информации между узлами, поскольку узлам неизвестно об изменении сообщений.**

В основном, данная атака предназначена для взлома протоколов, не предусматривающих взаимной аутентификации. В ходе этой атаки Злоумышленник может переадресовывать трудные вопросы, задаваемые одним из участников протокола, другому участнику, получать от него ответ, а затем пересылать спрашивающему, и наоборот.

Последовательность:

1. Когда жертва запрашивает вед-страницу, запрос направляется на ПК злоумышленника
2. ПК злоумышленника получает запрос и загружает подлинную страницу с веб-сайта.
3. Злоумышленник изменяет настоящую веб-страницу и выполняет преобразование данных.
4. Злоумышленник пересылает измененную страницу жертве.

7. **Атака путем подделки DNS (отравление DNS, DNS Poisoning) — записи DNS в системе изменяются так, чтобы узел обращался на поддельные DNS-серверы**. Пользователь пытается открыть настоящий сайт, но трафик переадресуется на поддельный веб-сайт. Поддельный веб-сайт используется для выманивания конфиденциальной информации, такой как имена пользователей и пароли. Затем злоумышленник может собрать все эти данные с сервера.



Атаки нулевого дня

Атаки нулевого дня (zero-day), которую иногда называют угрозой неизвестного типа, — это атака на компьютер с использованием уязвимостей в программном обеспечении, о которых не знает разработчик такого ПО или которые он намеренно скрывает.

Для обозначения момента обнаружения угрозы используются следующие термины:

- **Нулевой день**. Это день, когда разработчик обнаружил ранее неизвестную уязвимость. Этот день считается точкой отсчета при определении сроков, потребовавшихся разработчику на устранение уязвимости.
- **Нулевой час** – момент, когда был обнаружен вредоносный код, позволяющий использовать уязвимости ПО.

Сеть остается уязвимой в период времени между нулевым днем и днем выпуска исправления разработчиком.

Социальная инженерия.

Социальная инженерия используется в тех случаях, когда злоумышленник пытается получить доступ к оборудованию или сети, обманным путем получая от пользователей необходимую для доступа информацию.

Например, как показано на рисунке, злоумышленник, завоевывает доверие сотрудника и убеждает его сообщить имя пользователя и пароль.

В таблице описаны некоторые из способов, к которым прибегают злоумышленники, пользующиеся социальной инженерией, чтобы получить необходимую информацию.

Прием	Описание
Вымышленный предлог	Хакер притворяется, что ему необходимы личные или финансовые данные пользователя для подтверждения подлинности получателя.
Фишинг	Хакер отправляет поддельное сообщение электронной почты, замаскированное под письмо от законной организации. Оно предназначено для того, чтобы обмануть получателя и убедить его установить вредоносное ПО на устройство либо предоставить личную или финансовую информацию.
Выборочный фишинг	Хакер подготавливает фишинговую атаку, направленную на определенного человека или организацию.
Спам	Хакер использует спам, чтобы обмануть пользователя и убедить его перейти по зараженной ссылке или загрузить зараженный файл.
Проход «паровозиком»	Злоумышленник быстро следует за доверенным лицом, чтобы проникнуть в защищенное помещение. Таким образом он может попасть на защищенную территорию.
Услуга за услугу	Ситуации, когда злоумышленник просит предоставить от другой стороны личную информацию в обмен на что-нибудь, например, бесплатный подарок.
Приманка	Хакер оставляет в общедоступном месте, таком как уборная для сотрудников компании, физическое устройство, зараженное вредоносным ПО (например, флеш-диск USB). Обнаруживший такое устройство человек подключает его к компьютеру и тем самым непреднамеренно устанавливает вредоносное ПО.

3. Защита информации

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Система защиты информации – комплекс организационных и технических мероприятий по защите информации, проводимых на объекте управления с применением средств и способов в соответствии с концепцией, целью и замыслом защиты.

Средства защиты информации

1. **Технические средства – реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на:**
   - **аппаратные** – устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой систем обработки данных по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);
   - **физические** – реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения и т.п.);

2. **Программные средства** – программы, специально предназначенные для выполнения функций, связанных с защитой информации:
3. **Организационные средства** – организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации систем обработки данных для обеспечения защиты информации.
4. **Законодательные средства** – законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил;
5. **Морально-этические средства.**

Методы защиты информации

1. **Управление доступом, включающее следующие функции защиты:**
   - **идентификацию пользователя** (присвоение персонального имени, кода, пароля и опознание пользователя по предъявленному идентификатору);
   - **проверку полномочий,** соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту;
   - **разрешение и создание условий работы в пределах установленного регламента;**
   - **регистрацию обращений** к защищаемым ресурсам;
   - **реагирование** (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

- **криптографическое шифрование** – готовое к передаче сообщение(текст, речь, графика) зашифровывается, т.е. преобразуется в шифрограмму. Когда санкционированный пользователь получает это сообщение, он дешифрует его посредством обратного преобразования криптограммы.

3. **Механизм цифровой (электронной) подписи, основывающийся на алгоритмах асимметричного шифрования и включающий две процедуры: формирование подписи отправителя и ее распознавание (верификацию) получателем.**

4. **Механизмы контроля доступа осуществляют проверку полномочий объектов АИТ (программ и пользователей) на доступ к ресурсам сети.**

4. **Механизмы обеспечения целостности данных** (например, отправитель дополняет передаваемый блок данных криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке).

5. **Механизмы управления маршрутизацией** обеспечивает выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам и др.

Периметр сети - **это граница, отделяющая внутреннюю** (доверенную) **сеть от внешних** (не доверенных, un-trusted) **сетей. Периметр -** это первая линия защиты от внешних угроз.

Защита периметра - это контроль взаимодействия внутренней сети с внешними сетями.

Для зашиты периметра используются следующие средства:

- **Межсетевые экраны (МЭ), называемые также сетевые экраны, или firewall или брандмауэры,**
- **Антивирусные системы сетевого уровня,**
- **Устройства для построения виртуальных частных сетей (Virtual Private Network, VPN),**
- **Системы противодействия атакам.**

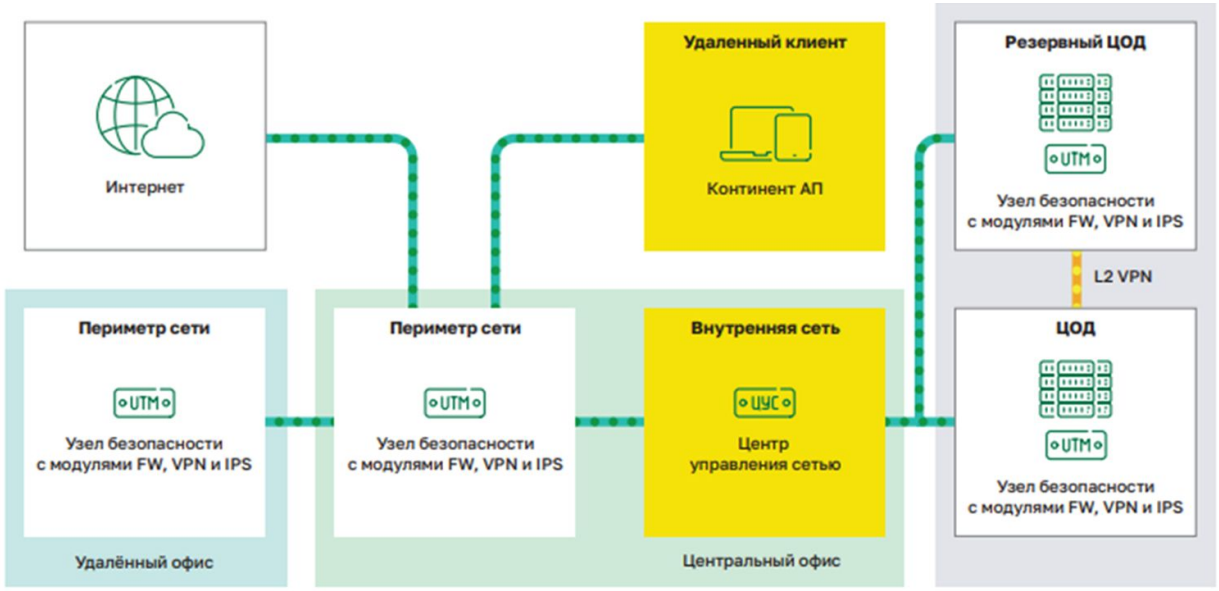
Межсетевой экран (МЭ) — это специализированное программное или аппаратное (или программно-аппаратное) **средство, позволяющее разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую.**

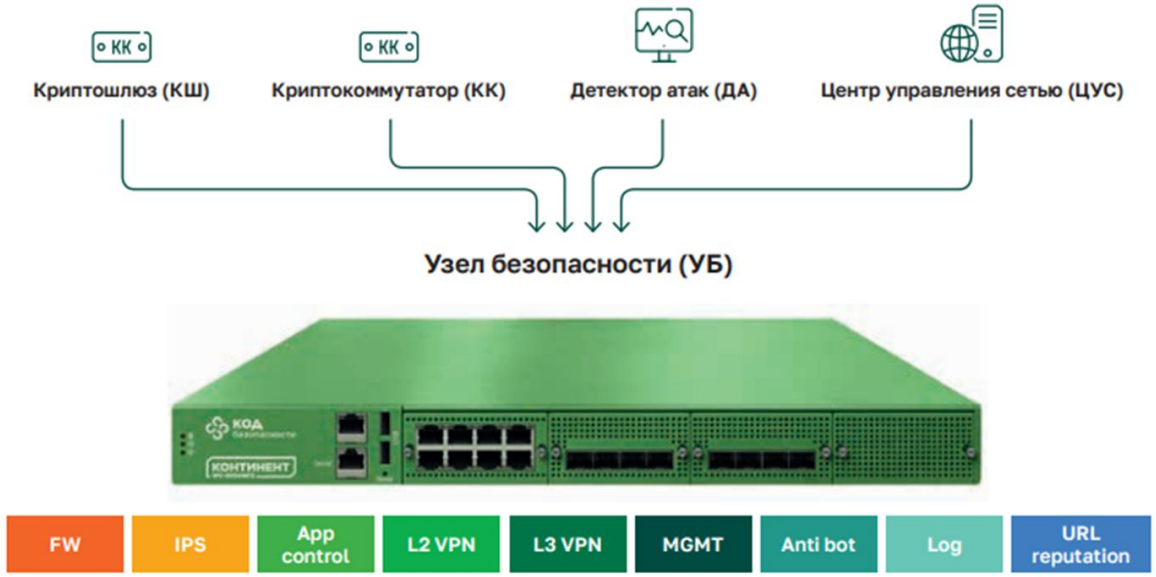
В рамках защиты периметра решаются следующие задачи:

- **Фильтрация трафика,**
- **Построение VPN,**
- **Антивирусная защита,**
- **Противодействие атакам,**
- **Анализ содержимого трафика,**
- **Защита от СПАМа,**
- **Контроль беспроводных устройств.**

В настоящее время применяются универсальные устройства корпоративного уровня для всесторонней защиты сети (UTM).

UTM - продукт по формату «все включено», объединяющий в себе межсетевой экран, систему обнаружения и предотвращения вторжений, антивирус и т.д.





На рис. представлена концепция UTM и устройство UTM Континент 4.

Защита от атак с применением методов социальной инженерии заключается в применении рекомендаций, которым должны следовать все сотрудники.

Способы защиты от социальной инженерии

Антропогенная защита

- Привлечение внимания людей к вопросам безопасности.
- Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.
- Осознание пользователями всей серьезности проблемы и принятие политики безопасности системы.

Техническая защита

К технической защите можно отнести средства, мешающие заполучить информацию и средства, мешающие воспользоваться информацией.