Компьютерные системы и сети

Безопасность передачи данных. VPN

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы, 2011/2012

Задачи:

- Обеспечение доступности (availability) - авторизованные пользователи всегда должны иметь доступ к необходимой информации.
- Обеспечение конфиденциальности (confidentiality) - система должна обеспечивать доступ к данным только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
- Обеспечение целостности (integrity) - подразумевает, что неавторизованные пользователи не могут каким-либо образом модифицировать данные.

Шифрование – процесс преобразования сообщения из открытого текста (plaintext) в шифротекст (ciphertext)

- В алгоритмах шифрования предусматривается наличие ключа (key) - параметра, не зависящего от текста. Результат применения алгоритма шифрования зависит от используемого ключа.
- Стойкость шифра должна определяться только секретностью ключа (т.е.алгоритмы шифрования считаются известными).

Использование шифрования:

- *защита содержания данных:*
  - шифрование потока (SSL, TLS)
  - шифрование канала (VPN);
- *контроль целостности:*
  - хэш-функции;
  - электронные цифровые подписи.

Шифрование

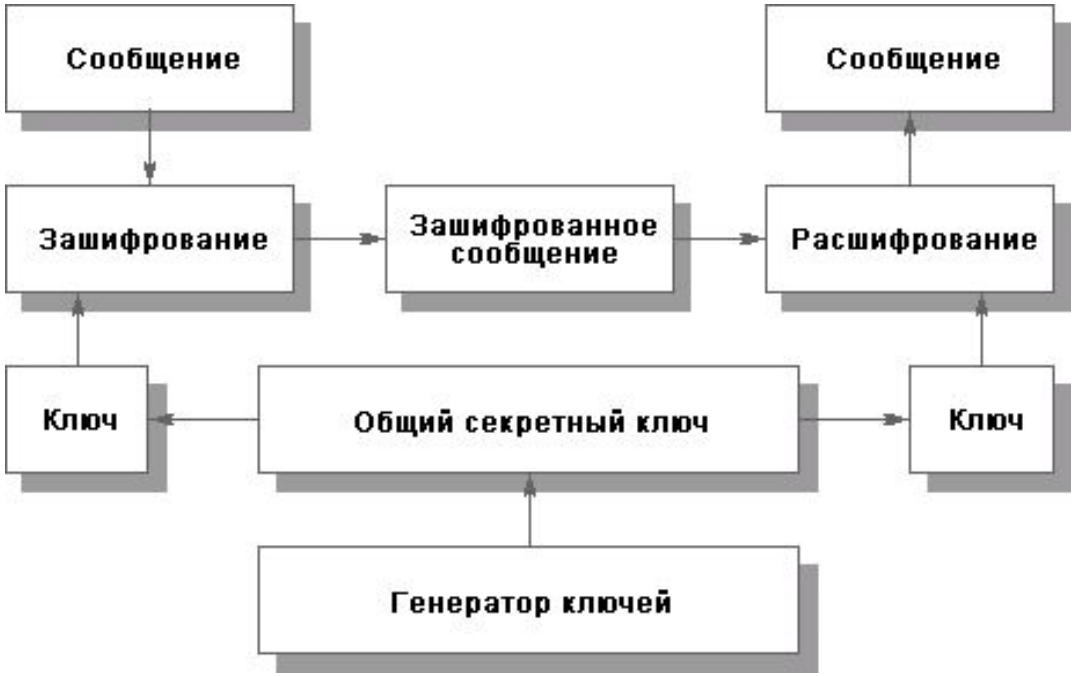
Хэш-функция **–** это необратимое преобразование данных (односторонняя функция) произвольной длины в выходную строку фиксированной длины (хеш-код, дайджест).

MD5 (Message Digest 5) - 128-битный алгоритм хеширования.
SHA-1 (Secure Hash Algorithm 1) - алгоритм генерирующий 160-битное хеш-значение.
SHA-2 (Secure Hash Algorithm Version 2) - алгоритмы, использующие хеш-функции SHA-224, SHA-256, SHA-384 и SHA-512.

Шифрование

Симметричный метод шифрования - один и тот же секретный ключ используется как для шифрования, так и для дешифрования данных.

Пример: DES



Алгоритмы симметричного шифрования:

Data Encryption Standard (DES) - использует 56-битный ключ для шифрования 64-битных блоков данных. Обеспечивает хорошую производительность при обеспечении конфиденциальности, приемлемой для ряда некритичных задач.

Triple DES (3DES) - создан для замены алгоритма DES, использует три различных 56-битных ключа для тройного шифрования данных 64-битного блока данных, что эквивалентно применению 168-битного ключа (2168 возможных ключей). Основной недостаток - медленная работа.

Advanced Encryption Standard (AES) - быстрый и эффективный алгоритм симметричного шифрования, позволяющий использовать ключи различной длины — 128, 192 и 256 бит для шифрования 128-битных блоков данных. Принят в США в качестве стандартного.

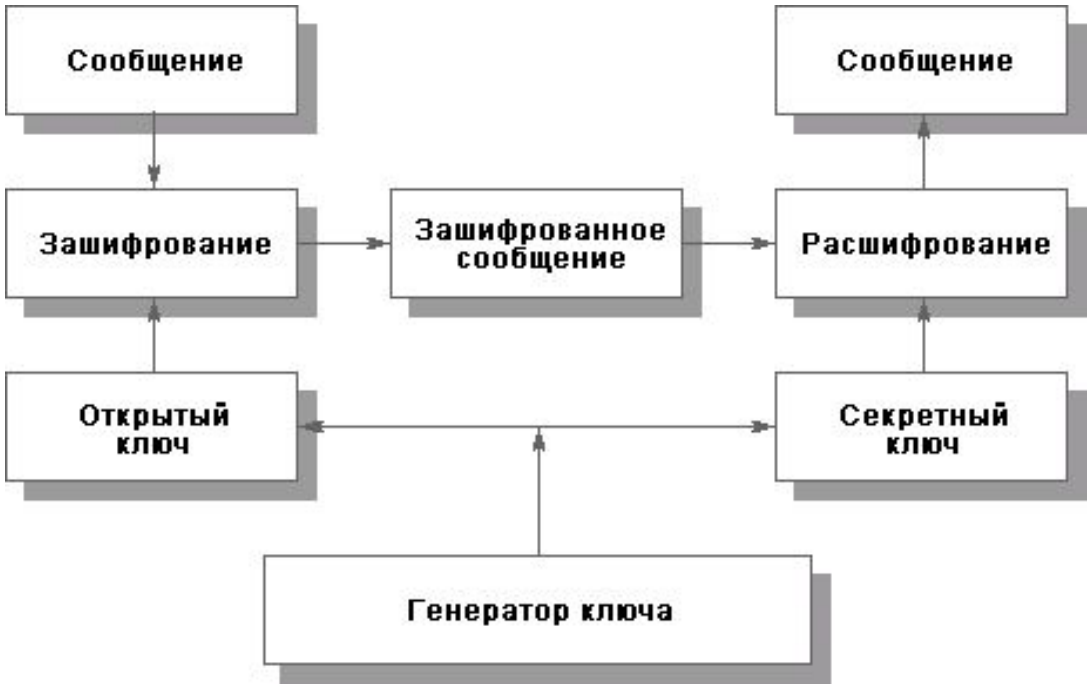
ГОСТ 28147-89 - российский стандартом для алгоритмов шифрования. Использует 256-битный ключ и оперирует 64-битными блоками данных.

Алгоритм RC4 потоковый алгоритм симметричного шифрования с длиной ключа от 40 до 256 бит.

Шифрование

Асимметричный метод шифрования (шифрование с открытым ключом) - используются два ключа. Один открытый (несекретный), другой - закрытый (секретный).

Пример: RSA



Алгоритмы симметричного шифрования:

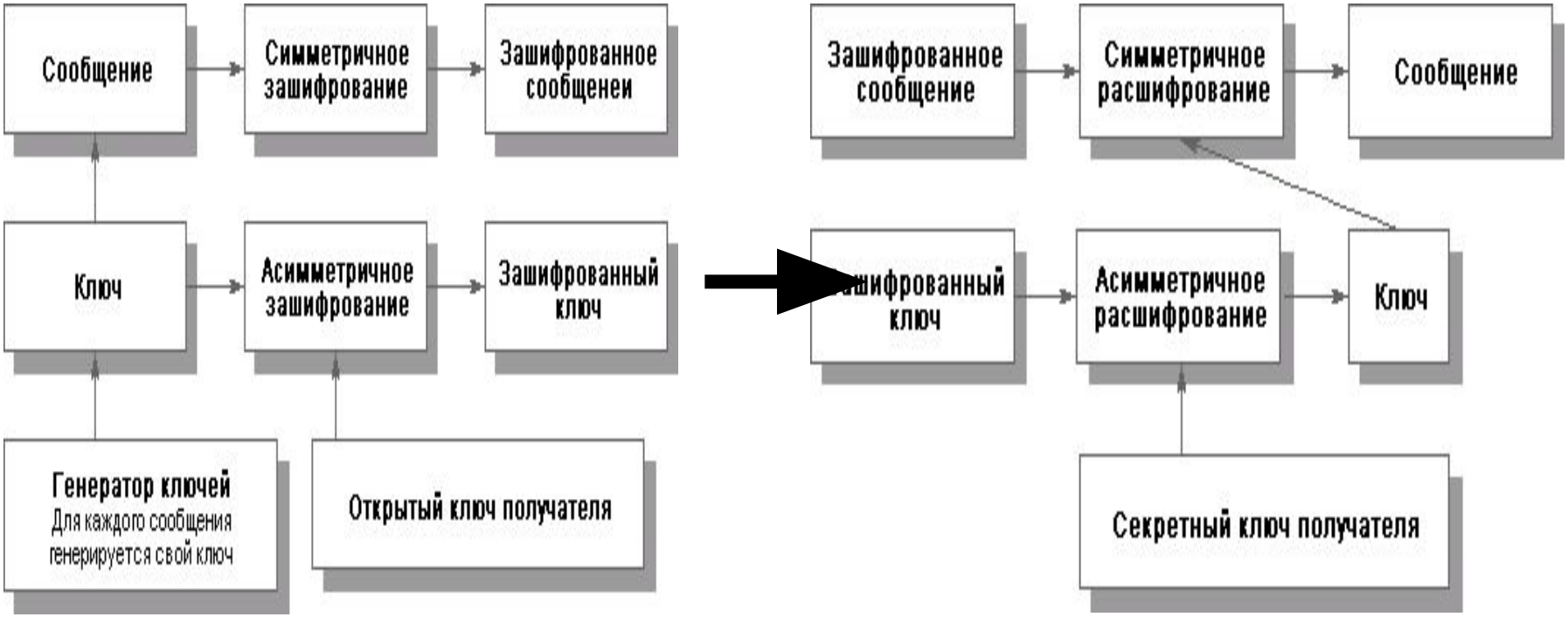
RSA - блочный криптографический алгоритм с открытым ключом. Используется и для шифрования, и для цифровой подписи.

DSA (Digital Signature Algorithm) - алгоритм с использованием открытого ключа для создания электронной подписи (не для шифрования).

ГОСТ Р 34.10-2001 – «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» - российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи.

Шифрование

сочетание симметричного и асимметричного методов

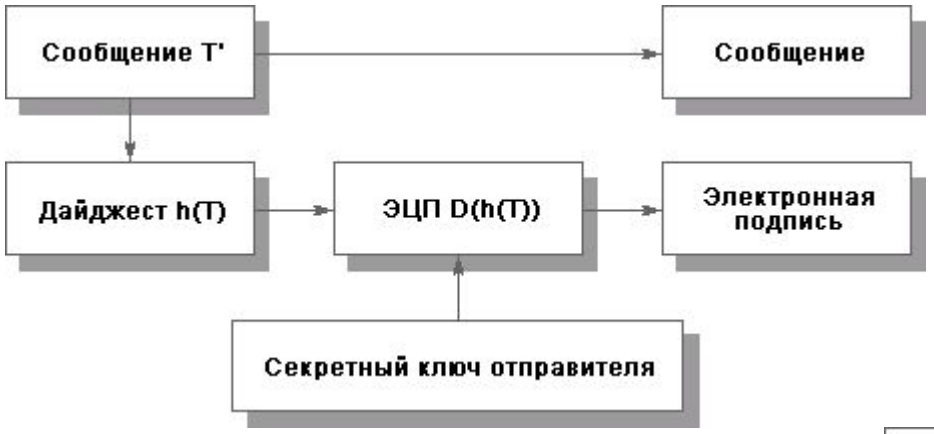


Стойкость алгоритмов шифрования:

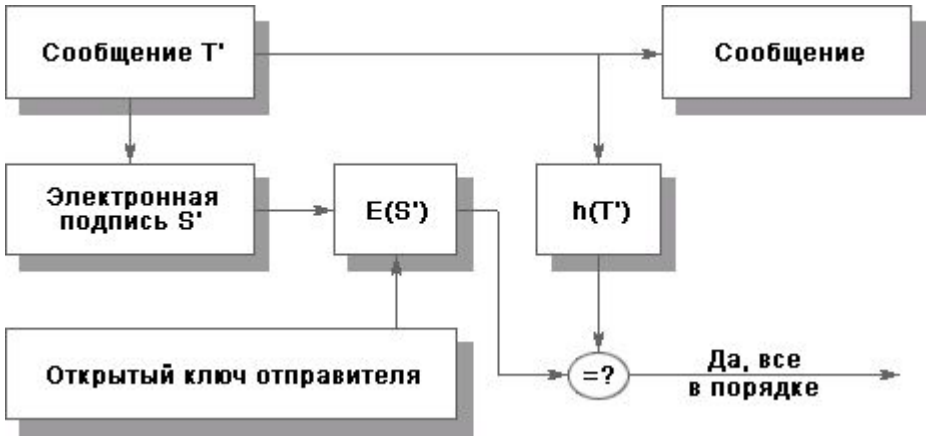
Длина симметричного ключа, бит	Длина несимметричного ключа, бит
56	384
64	512
80	768
112	1792
128	2304

Электронная цифровая подпись

создание



проверка



DSS (Digital Signature Standard) - стандарт цифровой подписи

Цифровой сертификат

структура:

- **порядковый номер сертификата;**
- **идентификатор алгоритма электронной подписи;**
- **имя удостоверяющего центра;**
- **срок годности;**
- **имя владельца сертификата;**
- **открытые ключи владельца сертификата;**
- **…..**
- **электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра.**

свойства:

- **любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;**

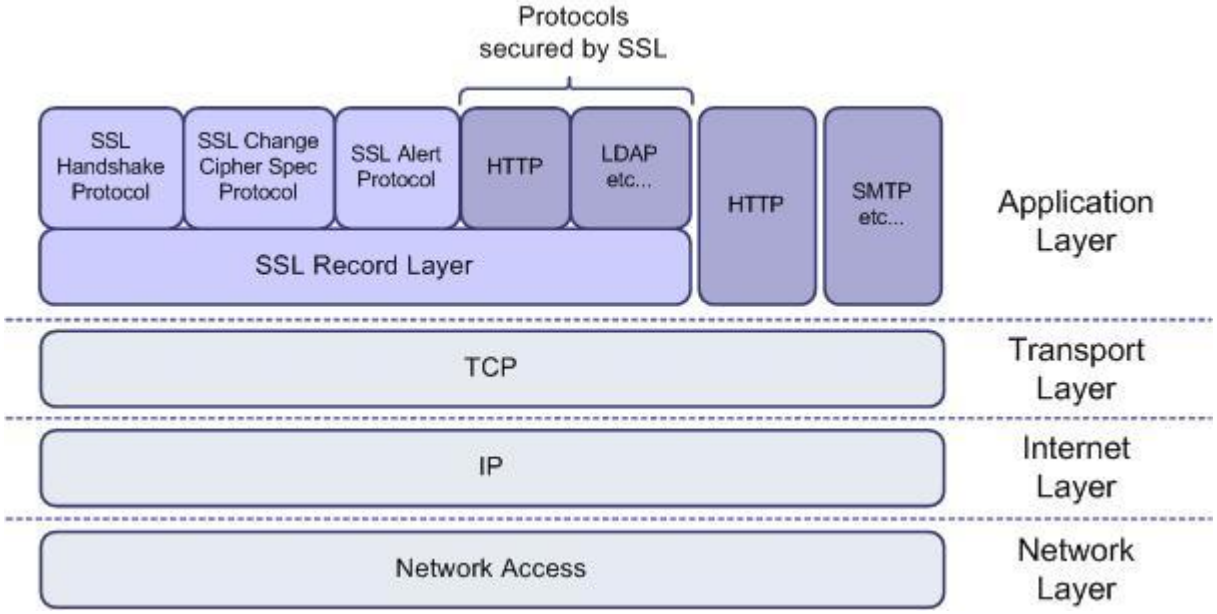
  никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

Шифрование потока

(уровень представления и прикладной)

SSL (Secure Sockets Layer)
TLS (Transport Layer Security)

устанавливают алгоритмы шифрования и ключи на обоих сторонах и создают шифрованный “туннель”, по которому могут передаваться другие протоколы (например HTTP)

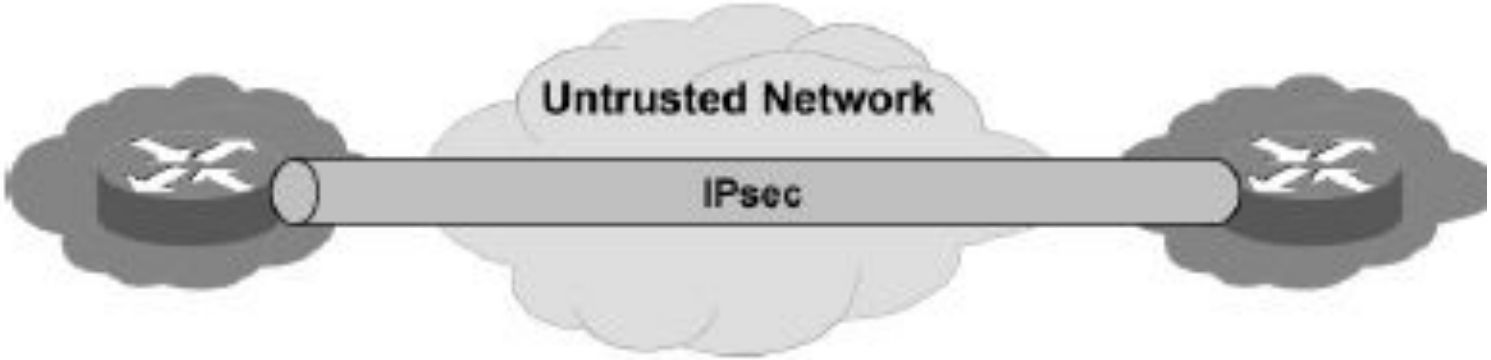


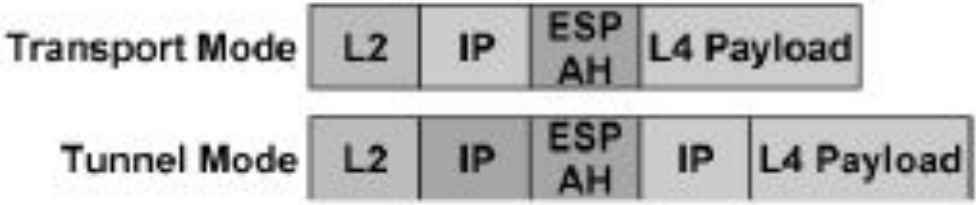
ГрГУ им. Я.Купалы

2011/2012

VPN

Virtual Private Net (VPN) – технология подключения клиента к VPN-серверу при помощи специального программного обеспечения поверх общедоступной сети.



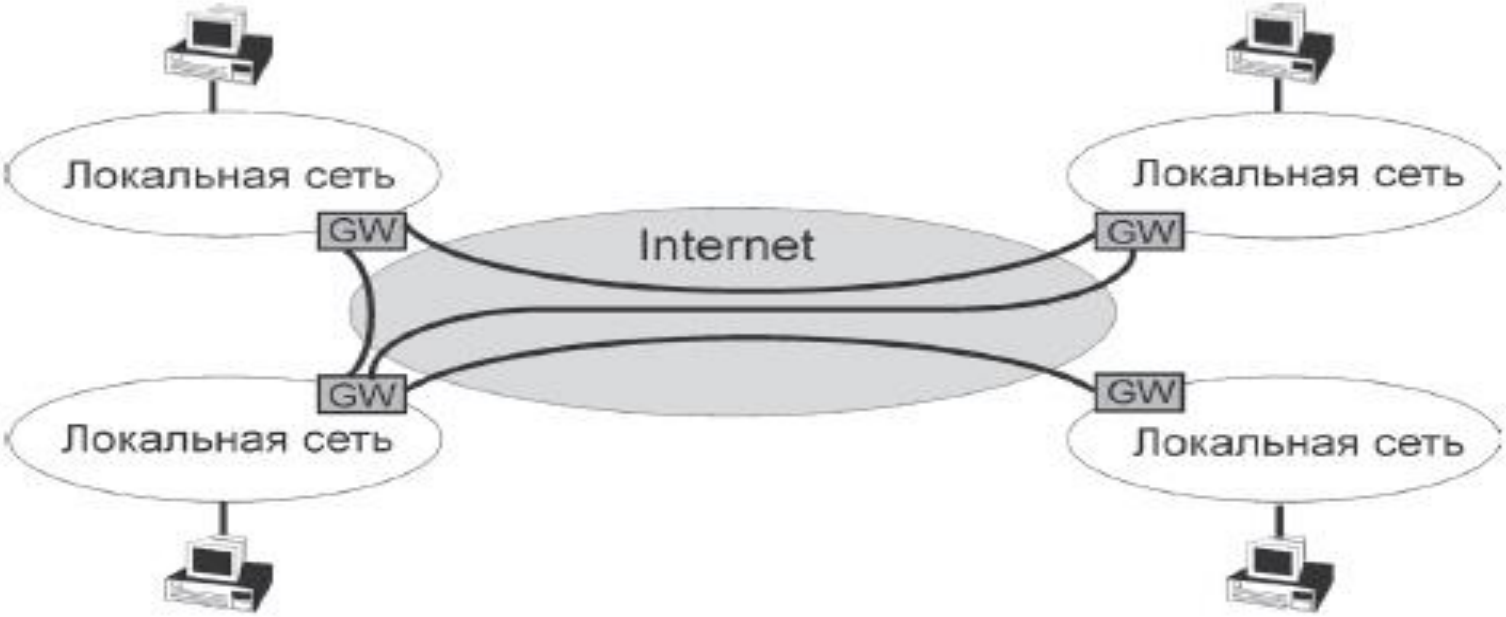


КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

Безопасность передачи данных

ГрГУ им. Я.Купалы

2011/2012



Virtual Private Net (VPN)

- В установленном соединении организуется зашифрованный канал, обеспечивающий высокую защиту передаваемой по этому каналу информации за счёт применения специальных алгоритмов кодирования.
- Технология позволяет нескольким пользователям организовать в одной сетевой инфраструктуре множество изолированных “частных” сетей, с выполнением требований владельца по пропускной способности, безопасности, адресации и т.д.).
- Применяется для решения проблемы создания множества изолированных ведомственных сетей на базе одной технической инфраструктуры

Virtual Private Net (VPN)

Туннель - логический путь данных, через который пересылаются пакеты.

Для источника и объекта назначения туннель является прозрачным и выглядит как обычное соединение между хостами.

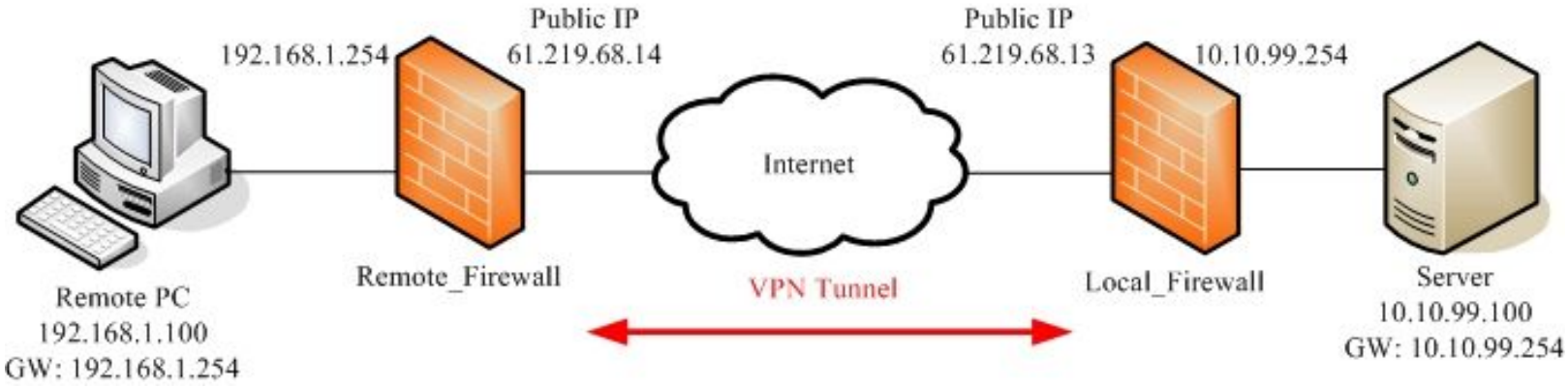
Оконечные точки (в туннеле) не имеют информации о маршрутах, прокси-серверах и иных шлюзах, через которые проходят пакеты, образующие туннель.

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

Безопасность передачи данных

ГрГУ им. Я.Купалы

2011/2012



Virtual Private Net (VPN)

- *Customer Provided VPN - Организация VPN силами потребителя*
- *Provider Provisioned VPN - Организация VPN силами поставщика телекоммуникационных услуг.*

Virtual Private Net (VPN)

Способы организации тоннелей

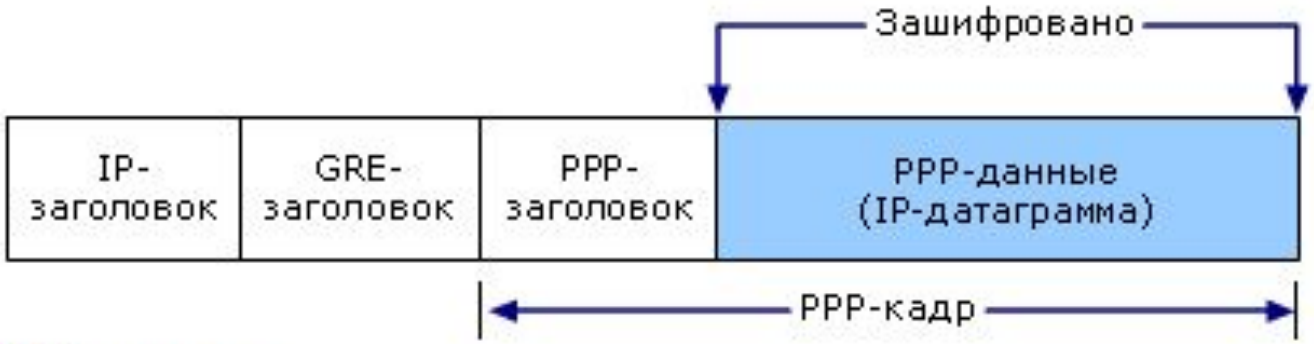
- *PPTP (Point-to-Point Tunneling Protocol)*
- *L2TP (Layer 2 Tunneling Protocol)*
- *IPsec (IP Security Protocol)*

Virtual Private Net (VPN)

Способы организации тоннелей

- PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол, представляющий собой расширение протокола PPP (Point-to-Point Protocol) для создания защищенных виртуальных каналов. Предусматривает создание криптозащищенного туннеля на канальном уровне модели OSI. Для передачи данных используются IP-пакеты, содержащие инкапсулированные PPP-пакеты. Инкапсулированные PPP-пакеты содержат в свою очередь зашифрованные инкапсулированные исходные пакеты (IP, IPX, NetBEUI).

Структура PPTP-пакета, содержащего IP-датаграмму

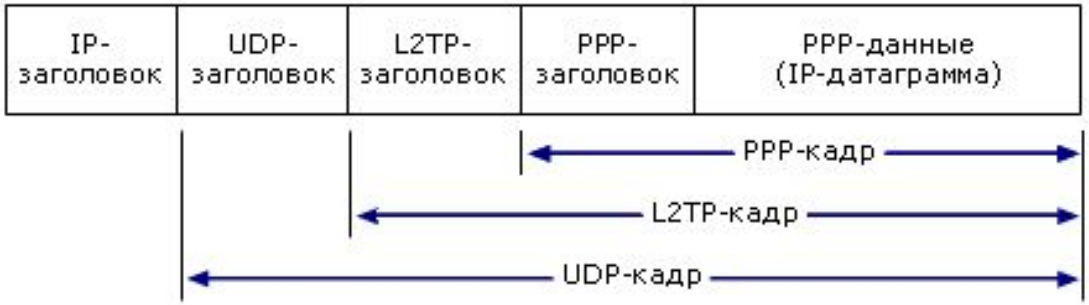


Virtual Private Net (VPN)

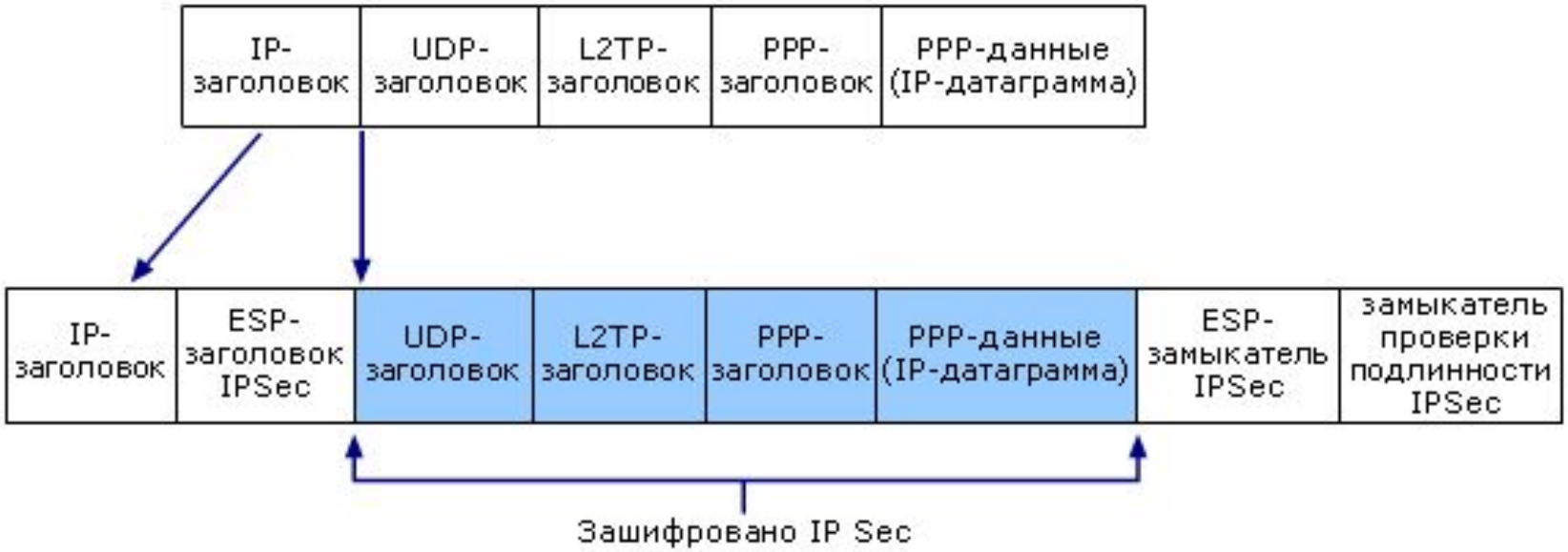
Способы организации тоннелей

L2TP (Layer 2 Tunneling Protocol) - индустриальный стандарт Интернет, туннельный протокол, который обеспечивает инкапсуляцию и пересылку кадров протокола PPP. Протокол L2TP шифрует IP-трафик и пересылает через среду. Реализация протокола Microsoft L2TP использует IPSec шифрование для защиты потоков данных на всем пути от VPN клиента до VPN сервера. L2TP и IPSec обеспечивают более высокую степень защиты данных, чем PPTP, так как использует алгоритм шифрования Triple Data Encryption Standard (3DES). Соединения по протоколу L2TP/IPSec требуют аутентификации, основанной на сертификатах.

Структура L2TP-пакета, содержащего IP-датаграмму



Шифрование L2TP-трафика с помощью протокола ESP IPsec



Virtual Private Net (VPN)

Способы организации тоннелей

- IPsec (IP Security Protocol) - это служба обеспечивающая аутентификацию, доступ и контроль за надежностью.

Работает на уровне сети. IPSec позволяет создавать кодированные туннели VPN или кодировать трафик между двумя узлами. В состав службы входят протоколы:

AH (Autentication Header) – заголовок аутентификации,

ESP (Encapsulating Security Payload – инкапсуляция зашифрованных данных),

IKE (Internet Key Exchange – обмен ключами).

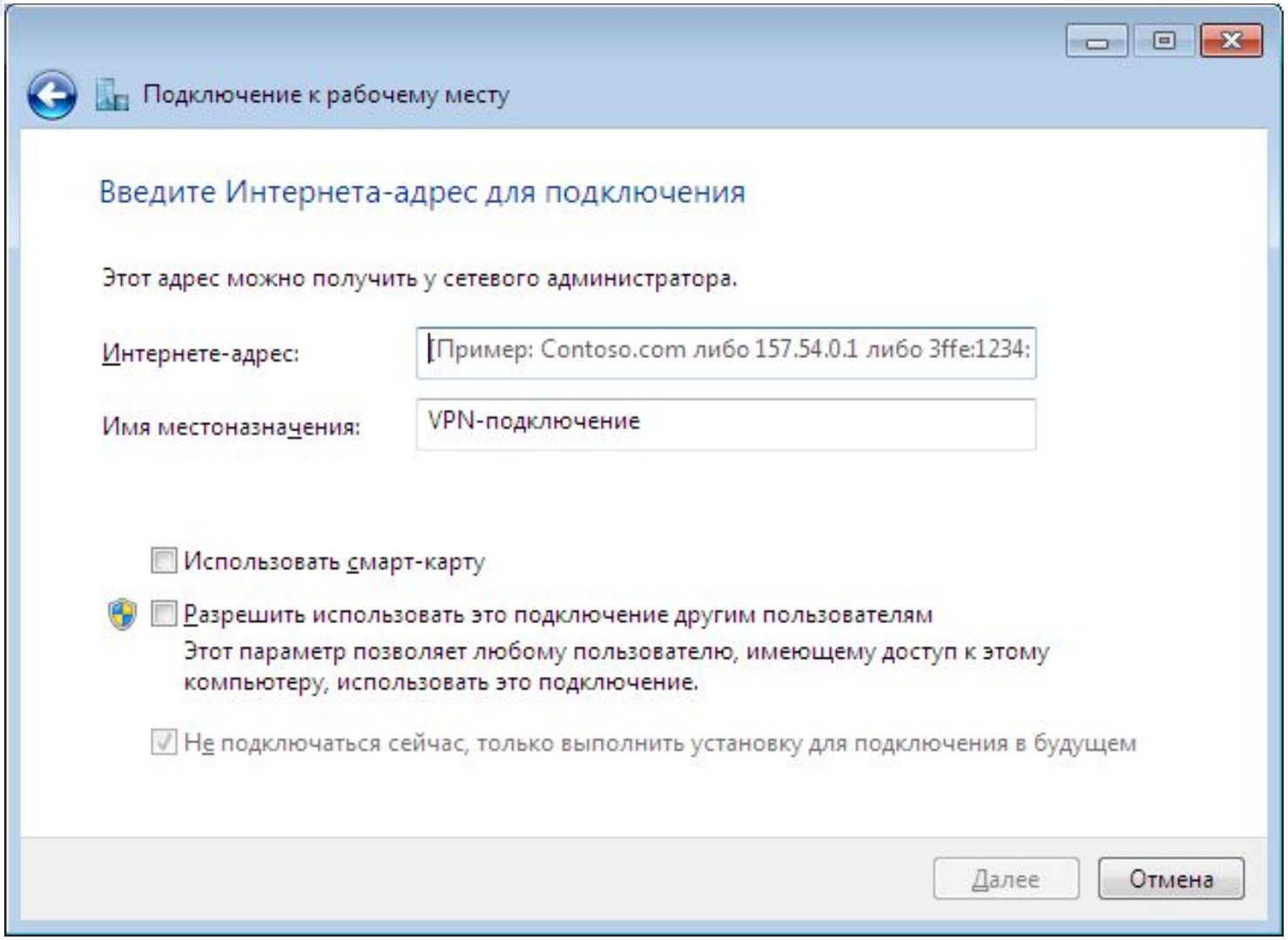
Для шифрования данных в системе IPsec может быть применен любой симметричный алгоритм шифрования.

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ

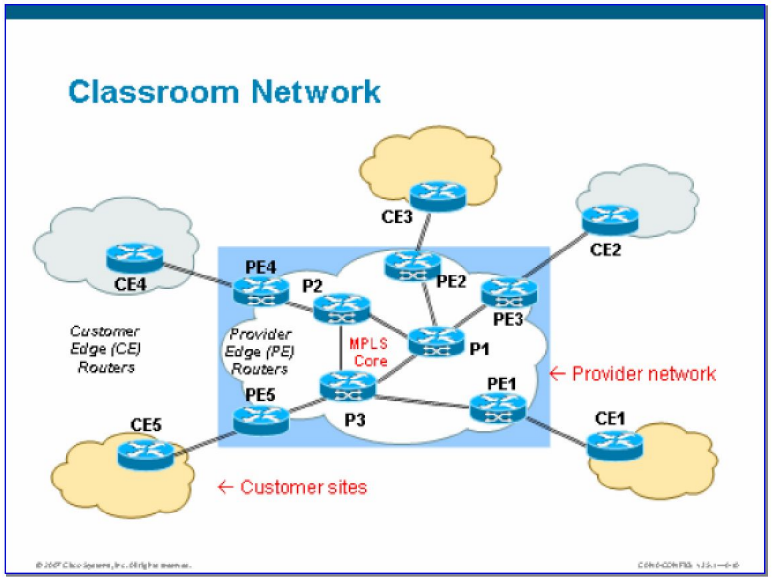
Безопасность передачи данных

ГрГУ им. Я.Купалы

2011/2012



MPLS (Multiprotocol Label Switching) - Сети MPLS VPN могут строиться как на канальном (L2VPN), так и на сетевом (L3VPN) уровнях модели взаимодействия OSI. Преимуществами являются хорошая масштабируемость, возможность автоматического конфигурирования, интеграция VPN с другими возможностями MPLS, такими, как управление трафиком и обеспечение качества на основе QoS. Регламентируется рекомендациями RFC2547bis.

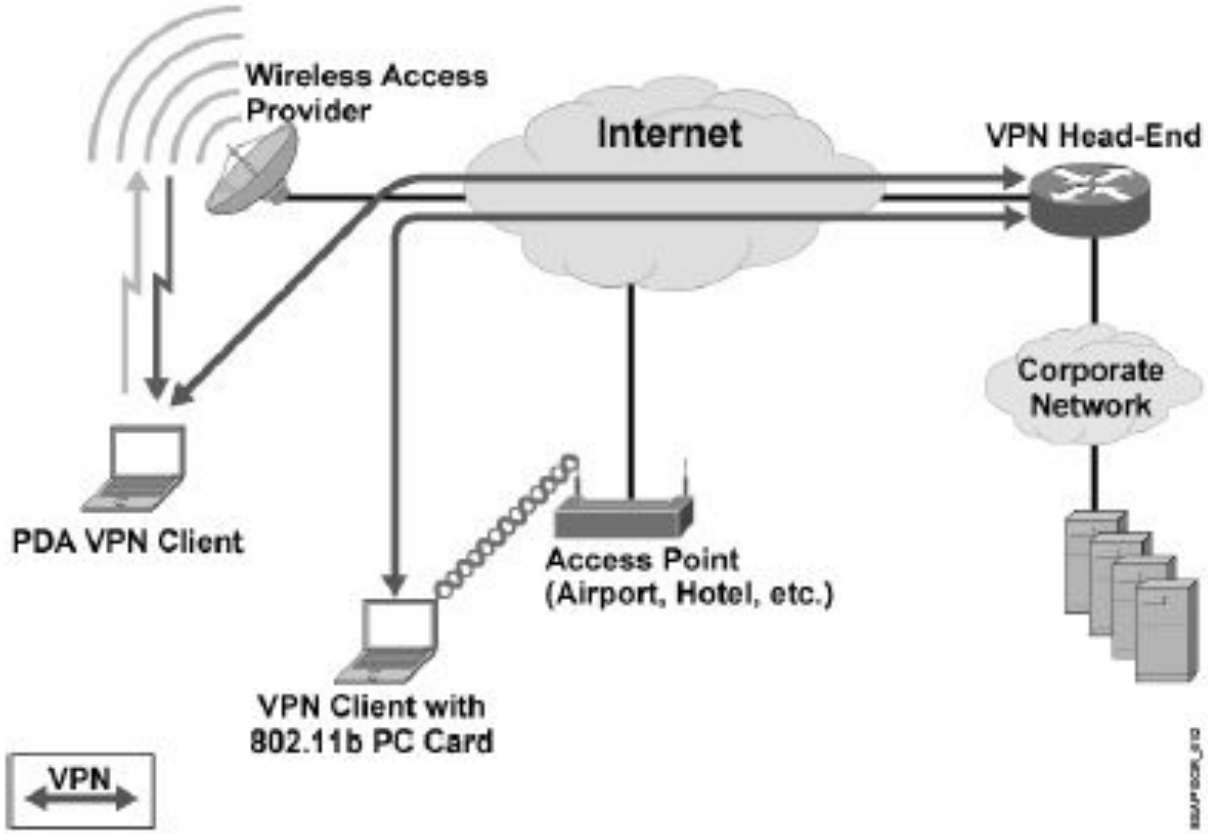


Virtual Private Net (VPN)

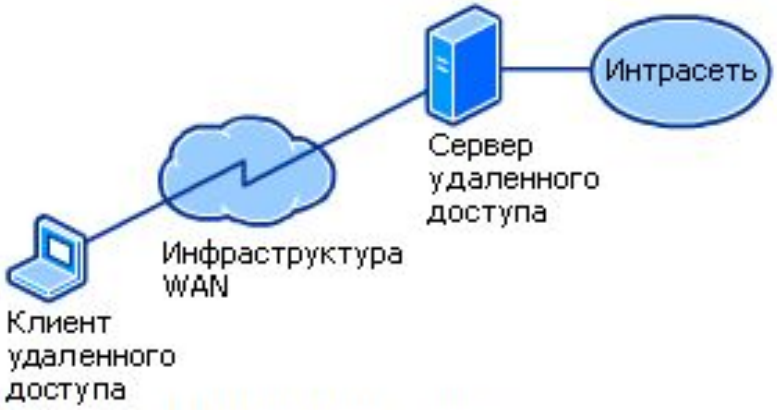
Альтернатива обособленным корпоративным сетям. Преимущества:

- отсутствие значительных капитальных вложений при создании сети;
- развитая топология сети (широкий географический охват);
- высокая надежность;
- легкость масштабирования (подключения новых сетей или пользователей);
- оперативность в изменении конфигурации;
- возможность интеграции дополнительных сервисных возможностей.

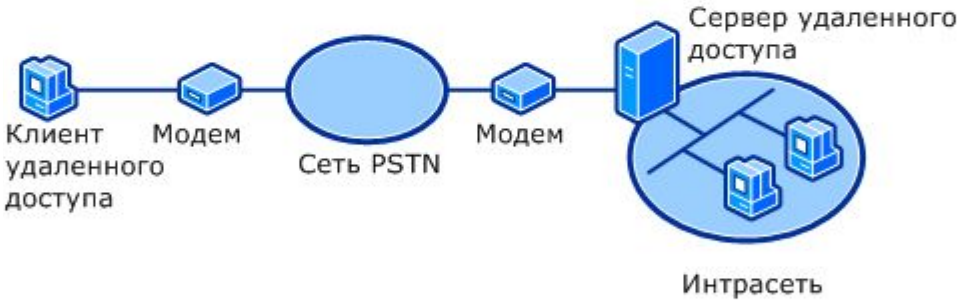
Удаленный доступ к сети



Удаленный доступ к сети



Стандартное PSTN-подключение



- **ИНТЕРНЕТ (INTERNET)** – открытая сеть
- **ИНТРАНЕТ (INTRANET)** – закрытая корпоративная сеть
- **ЭКСТРАНЕТ (EXTRANET)** – корпоративная сеть с удаленными пользователями и сетями партнеров

ГрГУ им. Я.Купалы

2011/2012

Сетевая безопасность

Сетевые угрозы

- **Spoofing** – подмена адреса (MAC, IP, DNS).

Сетевые угрозы

- **DoS, DDoS —** сетевые атаки, выполняемые посылкой многочисленных запросов к серверам и сервисам, что приводит к отказу в обслуживании, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов (DoS = Denial of Service).

  DoS-программы реализуют атаку с одного компьютера. DDoS-программы (Distributed DoS) реализуют распределенные атаки с разных компьютеров, обычно без ведома владельца зараженного компьютера.

Сетевые угрозы

- **Flood** (ping, SYN) — «затопление» сети. Реализуется посылкой большого количества бесполезных сообщений, загружающих телекоммуникационные и информационные каналы (IP-сети, электронную почту и т. д.)

Сетевые угрозы

- **Nuker** — фатальные сетевые атаки. Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

Сетевые угрозы

- Использование протокола **ARP**
- Сканирование зоны **DNS**
- Сканирование сети методом **ping**
- Сканирование **TCP** портов
- Сканирование **UDP** портов

Противодействие сетевым угрозам

- **Фильтрация** трафика.
- ***Локализация трафика*** (VLAN, VPN).
- Организация маршрутов через надёжные узлы.
- Использование средств шифрования трафика (***криптографии***) - самый действенный способ борьбы со снифферами. IPSec, SSL, SSH.

Противодействие сетевым угрозам

1. ***Межсетевые экраны*** – средства, организующие фильтрацию пакетов на основе их заголовков и/или других критериев.

2. ***Снифферы*** – программы, осуществляющие перехват всего проходящего трафика в сегменте для дальнейшего его анализа вручную или автоматическими средствами.

3. ***Средства обнаружения атак/вторжений*** – так же, как и снифферы, перехватывают весь или часть траффика и осуществляют поиск в нём подозрительных событий. Используются различные методы поиска, чаще всего сигнатурный метод. Иногда средства обнаружения вторжений дополнительно имеют свойства из других категорий.

4. ***Ловушки*** – осуществляющие имитацию работы той или иной службы/хоста/сети. Контролирующие и протоколирующие все обращения к ним. Перспективны с точки зрения сбора доказательств злого умысла нападающего, не подвергая при этом реальные системы какой-либо опасности.

5. ***Антивирусные программы***, осуществляющие поиск вирусов и подозрений на вирусы в файлах или информационных потоках.

Компьютерные системы и сети

Безопасность передачи данных. VPN

Олизарович Евгений Владимирович

ГрГУ им. Я.Купалы, 2011/2012