Тема 11

Протоколы сетевой безопасности

Содержание темы

- Фильтрация трафика.
- Межсетевые экраны.
- Прокси-серверы.
- Системы и средства мониторинга трафика.
- Системы обнаружения вторжений.
- Атаки на стек протоколов TCP/IP.
- Защита сетевых соединений.
- Протокол IPsec.

Содержание темы

- Безопасность сетевых служб.
- Компьютерные вирусы и механизмы борьбы с ними.
- Протокол HTTPS.
- Облачные сервисы и их безопасность.
- Защита информации беспроводных сетях.

Фильтрация трафика

Под **фильтрацией трафика** понимается обработка IP-пакетов маршрутизаторами и файерволами, приводящая к отбрасыванию некоторых пакетов или изменению их маршрута.

Фильтрация трафика позволяет либо предотвратить атаку на сеть, заранее блокируя доступ к ней для некоторых внешних сетей и хостов, либо, если источник атаки не был предварительно заблокирован, остановить ее.

Фильтрация трафика

Условия фильтрации бывают самыми разными, и не всегда удается найти простой признак, по которому одни пакеты нужно пропускать, а другие – отбрасывать.

Такое условие почти всегда является компромиссом между предотвращением атаки и поддержанием должной функциональности защищаемого узла.

Фильтрация трафика

Выборочная передача кадров/пакетов маршрутизатором осуществляется на основе стандартных и дополнительных правил, называемых также **фильтрами.**

Фильтрация трафика

Стандартные правила фильтрации определяются функциональностью устройств.

Концентратор повторяет блок данных, поступивший на любой его интерфейс на всех остальных его интерфейсах.

Коммутатор передает кадр только на соответствующий адресу интерфейс, если интерфейс не установлен – на все прочие интерфейсы.

Маршрутизатор пересылает или отбрасывает пакет в соответствии с правилами маршрутизации.

Фильтрация трафика

Дополнительные правила фильтрации, или **пользовательские фильтры**, задаются сетевыми администраторами исходя из политики безопасности или с целью изменения стандартных маршрутов.

Фильтрация трафика

Дополнительные правила фильтрации маршрутизаторов могут учитывать:

- IP-адреса источника и приемника;
- MAC-адреса источника и приемника;
- идентификаторы интерфейсов, с которых поступают пакеты;
- типы протоколов, сообщения которых несут IP-пакеты (то есть TCP, UDP, ICMP или OSPF);
- номера портов TCP/UDP (то есть типы протоколов прикладного уровня).

Фильтрация трафика

Фильтры, называемые **списками доступа** (**ACcess List**), являются очень распространенным средством ограничения пользовательского трафика в IP-маршрутизаторах.

Существует два типа списков доступа в Cisco:

- **стандартный список доступа** (**Standard**) позволяет задавать условия фильтрации, учитывающие только IP-адрес источника;
- **расширенный список доступа** (**Extended**) позволяет использовать дополнительные условия.

Фильтрация трафика

Стандартный список доступа имеет следующий формат:

access-list ***номер_списка_доступа*** { deny | permit } ***{адрес_источника*** [***метасимволы_ источника***] | any }

access-list – служебное слово;

номер_списка_доступа – число от 1 до 99;

deny – если условие выполняется, то запрет;

permit – если условие выполняется, то разрешение;

any – условие должно быть применено к любому значению адреса источника.

Фильтрация трафика

Пример стандартного списка доступа:
access-list 1 deny 192.78.46.0 0.0.0.255

Здесь: **1** – номер списка доступа; **deny** – пакет, который удовлетворяет условию данного списка доступа, должен быть отброшен; **192.78.46.0** – адрес источника; **0.0.0.255** – метасимволы источника.

Этот фильтр запрещает передачу пакетов, у которых в старших трех байтах адреса источника имеется значение 192.78.46.0.

Фильтрация трафика

Список доступа может включать более одного условия.

В этом случае он состоит из нескольких строк с ключевым словом access-list с одним и тем же номером.

access-list 1 permit 192.78.46.12 0.0.0.0
access-list 1 deny 192.78.46.0 0.0.0.255
access-list 1 permit any

Фильтрация трафика

Список на предыдущем слайде разрешает прохождение через маршрутизатор пакетов, отправляемых с хоста 192.78.46.12, и запрещает передачу пакетов, отправляемых любым другим хостом подсети 192.78.46.0/24.

Фильтрация трафика

Расширенный список доступа имеет следующий формат:

access-list ***номер_списка_доступа*** { deny | permit } ***ключевое_слово_протокола{адрес_источника метасимволы_источника*** [***операция порт_источника]*** | any }{ ***адрес_приемника метасимволы_приемника*** [***операция порт_приемника***] | any }

Фильтрация трафика

Параметры расширенного списка доступа:

номер_списка_доступа – номер списка доступа из диапазона 100-199;

ключевое слово протокола – ip, tcp, udp или icmp;

операция: eq, lt, gt (позволяет задать порт, диапазон портов UDP/TCP или тип пакета ICMP).

Фильтрация трафика

access-list 105 permit tcp any host 210.135.17.101 eq 21

Эта запись разрешает прием запросов от любого хоста, направленных FTP-серверу (TCP- порт 21) с адресом 210.135.17.101 (используется дополнительное служебное слово host вместо маски 0.0.0.0).

Фильтрация трафика

access-list 101 deny ICMP any 192.78.46.0 0.0.0.255 eq 8

Эта запись запрещает передачу эхо-запросов (ping-запросов) от любого хоста к хостам подсети 192.78.46.0/24.

Фильтрация трафика

access-list 105 permit tcp any eq 80 any gt 1023 established

Эта запись разрешает клиентам веб-службы (они всегда имеют порт TCP > 1023) получать ответы от любых веб-серверов (порт 80), с которыми у них уже установлено TCP- соединение (служебное слово established оговаривает это, маршрутизатор проверяет данный факт по наличию признака ACK в пакете).

Фильтрация трафика

Список доступа можно применять к любому интерфейсу маршрутизатора и в любом направлении:

- если список применяется с ключевым словом **in**, то он действует на входящие в интерфейс пакеты (выполняется **входная фильтрация** (**Ingress Filtering**));
- если – с ключевым словом **out**, то он будет воздействовать на пакеты, исходящие из интерфейса (выполняться **выходная фильтрация** (**Egress Filtering**)).

Фильтрация трафика

Для обеспечения подотчетности необходимо **протоколирование событий**, связанных с фильтрацией пакетов.

Маршрутизаторы Cisco могут помещать сообщения об обработке пакетов, удовлетворяющих условию некоторой записи списка доступа, в системный журнал маршрутизатора **syslog**.

Для этого необходимо добавить к записи ключевое слово log:

access-list 102 permit TCP any 21 any log

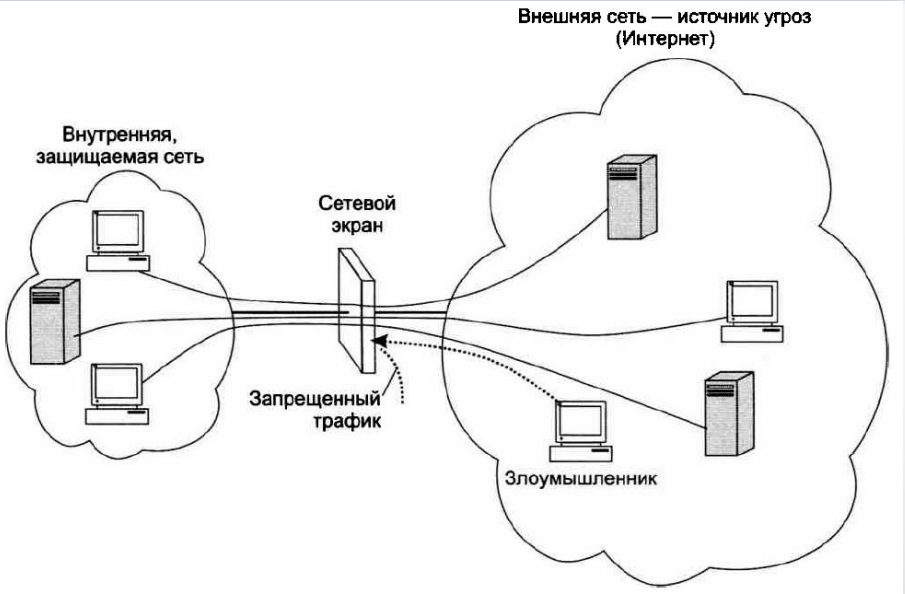
Фильтрация трафика

Фильтрация трафика в целях безопасности является важным средством **защиты от атак.**

Функцию фильтрации поддерживают **файерволы** разного типа, в том числе файерволы на базе маршрутизаторов.

Межсетевые экраны

Файервол (межсетевой экран, или **брандмауэр)** – это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа и фильтрации проходящего между ними трафика.



Межсетевые экраны

Для эффективного выполнения файерволом его главной функции – анализа и фильтрации трафика – необходимо, чтобы через него проходил **весь** трафик, которым обмениваются узлы защищаемой части сети с узлами Интернета.

В том случае, когда сеть связана с внешними сетями несколькими линиями связи, каждая линия связи должна быть защищена файерволом.

Межсетевые экраны

Основными функциями файервола являются:

- фильтрация трафика в целях защиты внутренних ресурсов сети;
- аудит – файервол должен фиксировать все события, связанные с обнаружением и блокировкой подозрительных пакетов.

Межсетевые экраны

Вспомогательные функции защиты файервола:

- антивирусная защита;
- шифрование трафика;
- функция прокси-сервера;
- фильтрация сообщений по содержимому (типы файлов, имена DNS и ключевые слова);
- предупреждение и обнаружение вторжений и сетевых атак;
- функции VPN;
- трансляция сетевых адресов (NAT).

Межсетевые экраны

Файерволы различают по способу реализации:

- **программный файервол** – программная система, работающая под управлением универсальной ОС;
- **аппаратный файервол** – набор дополнительных функций маршрутизатора;
- **программно-аппаратный файервол** – включает как программную систему, так и специализированный сервер, операционная система которого и аппаратура имеют конфигурацию и настройки, оптимизированные для работы файервола.

Межсетевые экраны

Файерволы различают по способу фильтрации:

- **файерволы без запоминания состояния** (**Stateless**) выполняют фильтрацию на основе статических правил, при этом не отслеживаются состояния соединений (сеансов);
- **файерволы с запоминанием состояния** (**Stateful**) принимают решения динамически с учетом текущего состояния сеанса и его предыстории.

Межсетевые экраны

К **файерволам канального уровня** могут быть условно отнесены управляемые коммутаторы, обладающие расширенным набором функций, в том числе возможностью фильтрации кадров канального уровня на основе задаваемых администратором списков доступа.

Межсетевые экраны

Файерволы сетевого уровня, называемые также **файерволами с фильтрацией пакетов**(**Packet Filtering Firewall**), решают задачу фильтрации пакетов по IP-адресам, а также по значению поля протокола верхнего уровня.

Более того, такие файерволы работают и на более высоком, транспортном уровне, то есть на уровне портов TCP и UDP, но только на основе статических правил, при которых не отслеживаются состояния соединений.

Межсетевые экраны

Файерволы сеансового уровня отслеживают состояния сеансов протоколов, другими словами, выполняют операцию запоминания состояния на уровнях ниже прикладного.

Для того чтобы контролировать процесс установления соединения, файервол должен фиксировать для себя текущее состояние соединения, то есть запоминать, какое последнее сообщение отправил клиент и какое сообщение он ожидает получить.

Межсетевые экраны

Файерволы прикладного уровня способны интерпретировать, анализировать и контролировать содержимое сообщений, которыми обмениваются приложения.

Они также работают на основе фильтрации с запоминанием состояния, но анализируют состояния протоколов не только нижних уровней вплоть до транспортного, но и прикладного уровня, таких как протоколы SSH, HTTP, FTP, SQL, SMTP, POP3, IMAP, FTP, SSH, SQL и др.

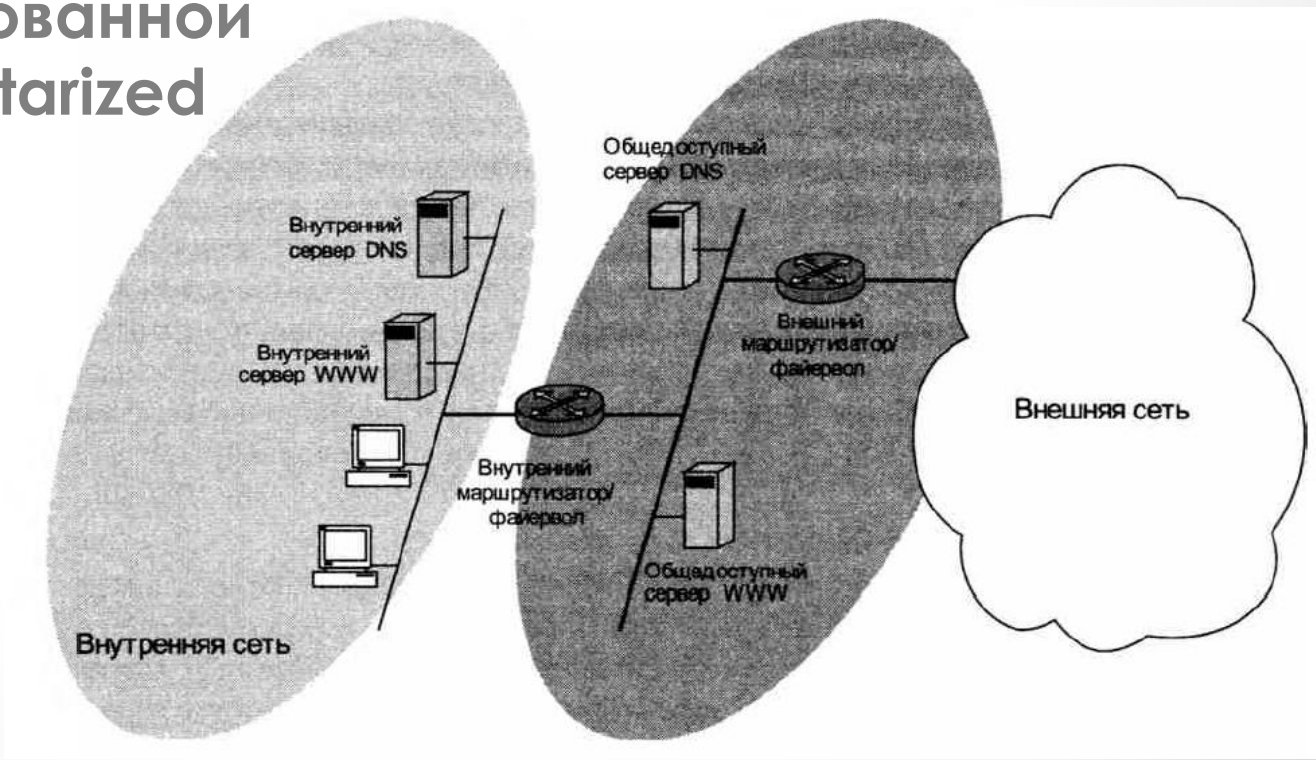
Межсетевые экраны

Для надежной и эффективной защиты корпоративной сети она должна быть **логически сегментирована** таким образом, чтобы ресурсы каждой подсети в отношении мер защиты были подобными.

Ресурсы корпоративной сети, к которым обращаются внешние пользователи составляют в отношении мер безопасности отдельную группу (почтовый сервер, веб-сервер, DNS-сервер).

Межсетевые экраны

Повсеместной практикой является выделение таких ресурсов в отдельную группу и размещение их в подсети, которая получила название **демилитаризованной зоны (DeMmilitarized Zone, DMZ).**



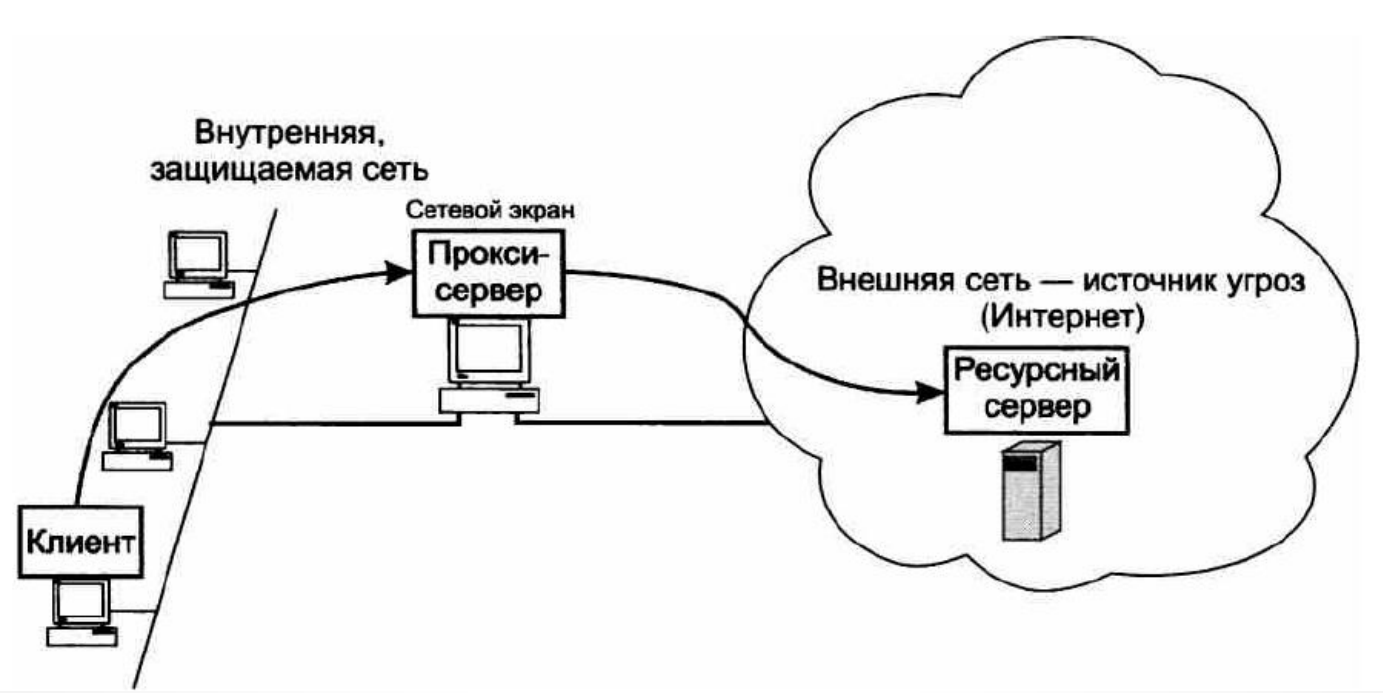
Прокси-серверы

Прокси-сервер (**Proxy Server**) — это особый тип приложения, которое выполняет функции посредника между клиентскими и серверными частями распределенных сетевых приложений, причем предполагается, что клиенты принадлежат внутренней (защищаемой) сети, а серверы — внешней (потенциально опасной) сети.

Подобно сетевому экрану, прокси-сервер может эффективно выполнять свои функции только при условии, что контролируемый им трафик не пойдет обходным путем.

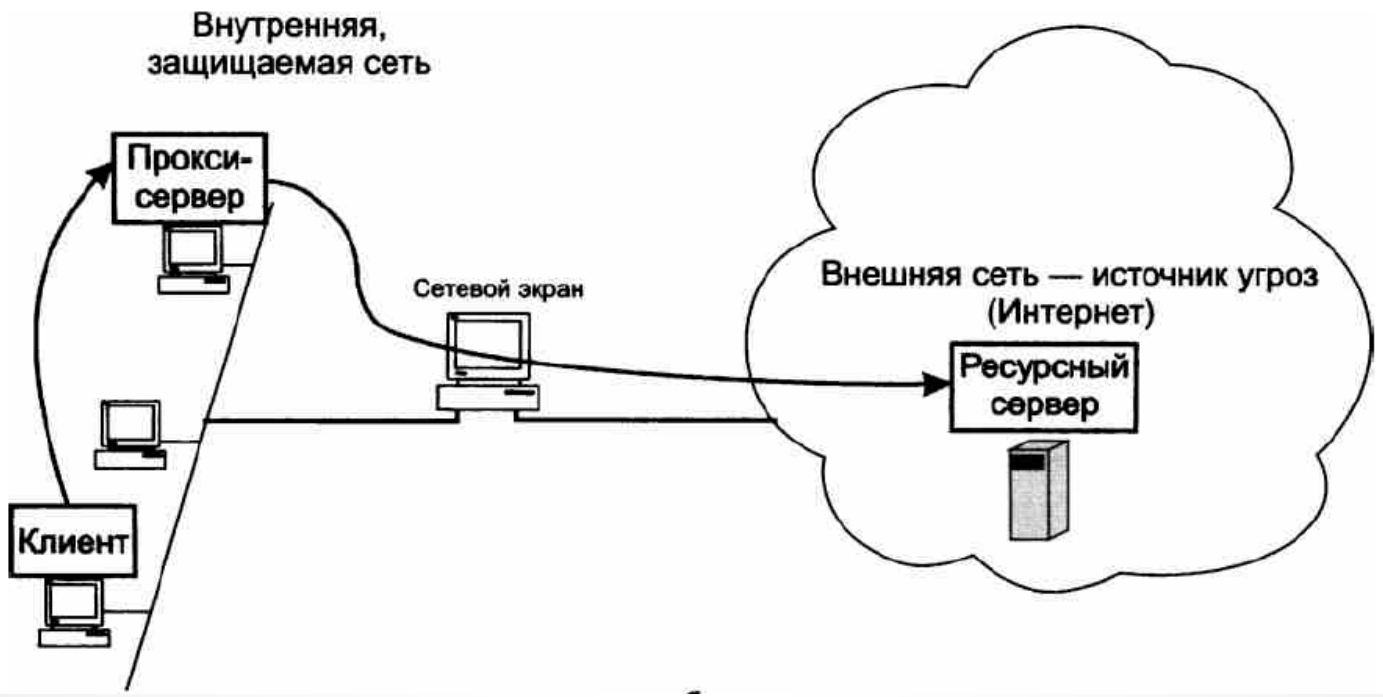
Прокси-серверы

Прокси-сервер установлен на платформе, где работают все остальные модули файервола.



Прокси-серверы

Прокси-сервер установлен на любом узле внутренней сети или сети демилитаризованной зоны.



Прокси-серверы

Когда клиенту необходимо получить ресурс (файл, веб-страницу, почтовое сообщение) от какого-либо сервера, он посылает свой запрос прокси-серверу.

Прокси-сервер анализирует этот запрос и на основании заданных ему администратором правил решает, каким образом он должен быть обработан (отброшен, передан без изменения ресурсному серверу, модифицирован тем или иным способом перед передачей, немедленно обработан силами самого прокси-сервера).

Прокси-серверы

Прокси-сервер прикладного уровня умеет **вклиниваться** в процедуру взаимодействия клиента и сервера по одному из прикладных протоколов (HTTP, HTTPS, SMTP/POP, FTP или telnet).

Чтобы выступать в роли посредника на прикладном уровне, прокси-сервер должен **понимать** смысл команд, **знать** форматы и последовательность сообщений, которыми обмениваются клиент и сервер соответствующей службы.

Прокси-серверы

Прокси-сервер сеансового уровня выполняет свою посредническую миссию на транспортном уровне, контролируя TCP-соединение.

Работая на более низком уровне, прокси-сервер имеет меньше возможностей для выявления и предупреждения атак.

Системы и средства мониторинга трафика

Мониторинг сетевого трафика – непрерывный процесс инструментального автоматизированного наблюдения за отдельными параметрами трафика с целью проверки соблюдения соглашения об уровне обслуживания, планирования сети, а также предотвращения негативных событий, таких как технические аварии, угрозы и атаки злоумышленников.

Путем использования мониторинга сетевого трафика можно обнаружить следы атак, которые смогли преодолеть барьер файервола.

Системы и средства мониторинга трафика

Средства мониторинга сетевого трафика:

- **анализаторы протоколов** (**сетевые сниферы**) – захватывают трафик локальных сетей и представляют его администратору для анализа;
- **маршрутизаторы**, поддерживающие **протокол NetFlow**, собирают обобщенные данные о трафике глобальных сетей и передают его NetFlow, для поиска атак и угроз;
- **системы обнаружения вторжений** (**Intrusion Detection Systems**, **IDS**) специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей.

Системы и средства мониторинга трафика

Средства мониторинга сетевого трафика:

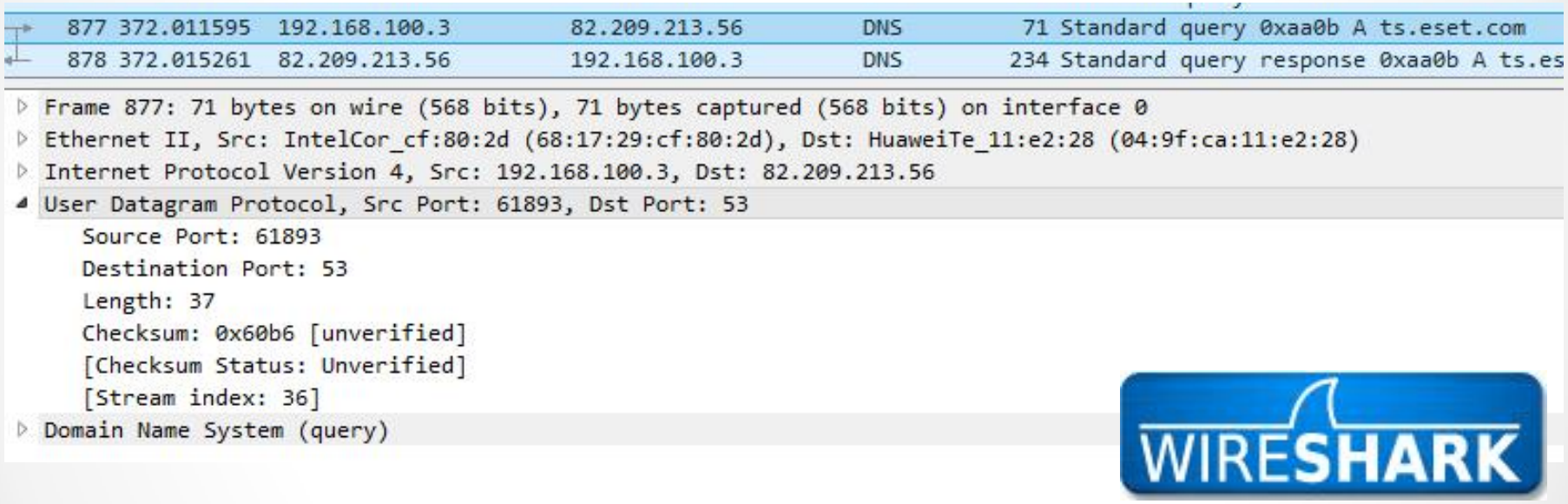
- **анализаторы протоколов** (**сетевые сниферы**) – захватывают трафик локальных сетей и представляют его администратору для анализа;
- **маршрутизаторы**, поддерживающие **протокол NetFlow**, собирают обобщенные данные о трафике глобальных сетей и передают его NetFlow, для поиска атак и угроз;
- **системы обнаружения вторжений** (**Intrusion Detection Systems**, **IDS**) специализируются на автоматическом распознавании вторжений и угроз в прослушиваемом трафике локальных сетей.

Системы и средства мониторинга трафика

Анализаторы протоколов способны на основе некоторых заданных оператором логических условий захватывать отдельные пакеты и декодировать их, то есть показывать в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания полей каждого пакета.

Возможности анализатора во многом определяются устройством и объемом **буфера захвата пакетов**.

Системы и средства мониторинга трафика



Системы и средства мониторинга трафика

Система NetFlow сегодня является основным средством учета и анализа трафика, проходящего через маршрутизаторы и коммутаторы сети.

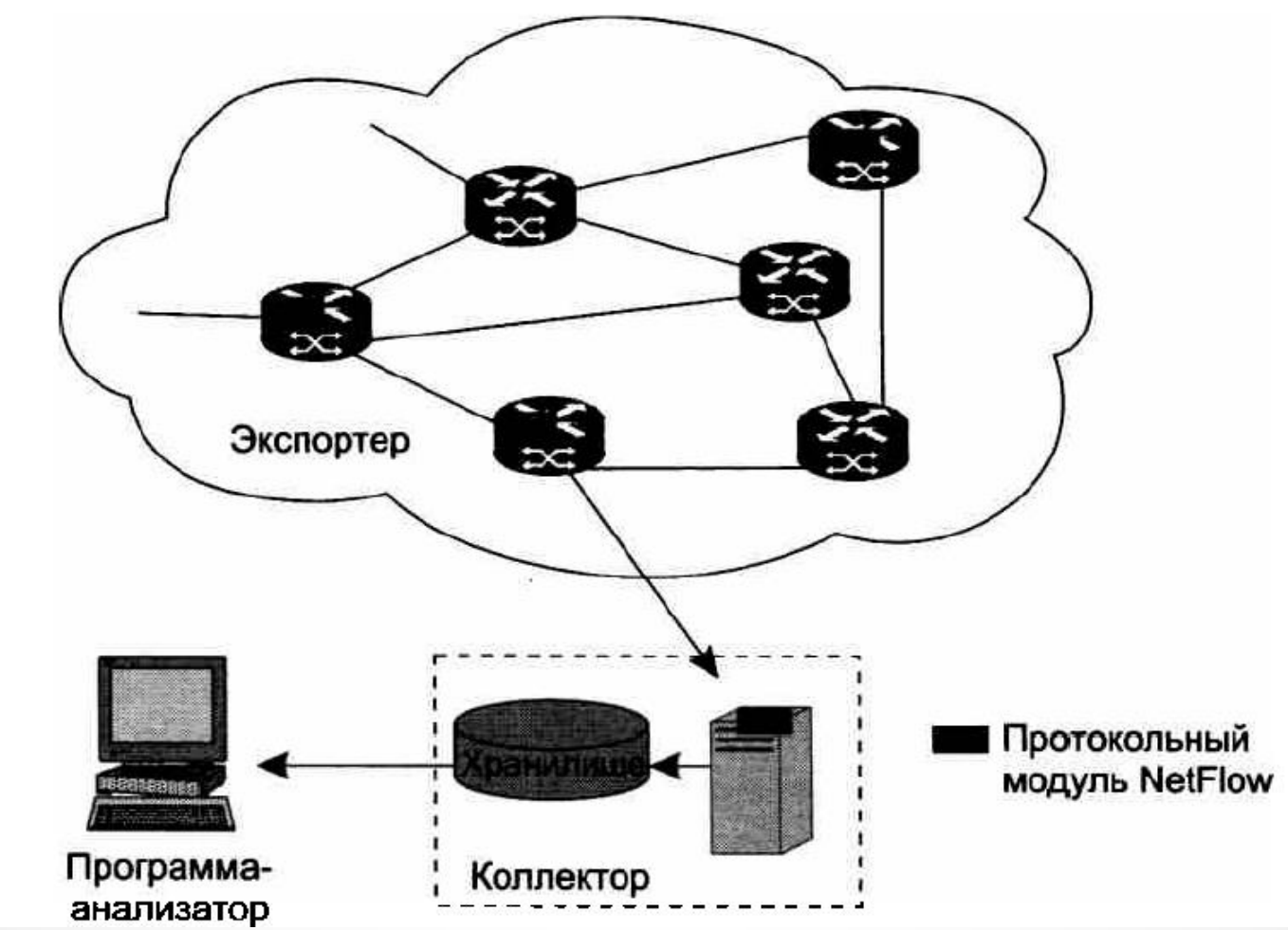
Поддерживающие протокол NetFlow сетевые узлы не только выполняют свою основную работу – передачу пакетов в соответствии с адресом назначения, но и собирают статистику о проходящих через них потоках данных и периодически отправляют их в **коллекторы** для хранения и обработки такой информации.

Системы и средства мониторинга трафика

NetFlow собирает статистику не о каждом пакете, а о **потоке пакетов** (**Net** – сеть, **Flow** – поток).

Под потоком понимается последовательность пакетов, принадлежащих одному и тому же соединению между определенными приложениями двух определенных компьютеров.

Системы и средства мониторинга трафика



Системы и средства мониторинга трафика

Атака обычно генерирует не совсем обычный образец трафика, и существуют рекомендации для распознавания таких аномалий:

- **выявление узлов с необычно большим числом запросов на установление соединений;**
- **выявление узлов с необычно интенсивным трафиком;**
- **анализ SYN и других флагов заголовка TCP;**
- **анализ ICMP-сообщений.**

Системы обнаружения вторжений

Система обнаружения вторжений (**Intrusion Detection System**, **IDS)** – это программное или аппаратное средство, которое выполняет непрерывное наблюдение за сетевым трафиком и деятельностью субъектов системы с целью предупреждения, выявления и протоколирования атак.

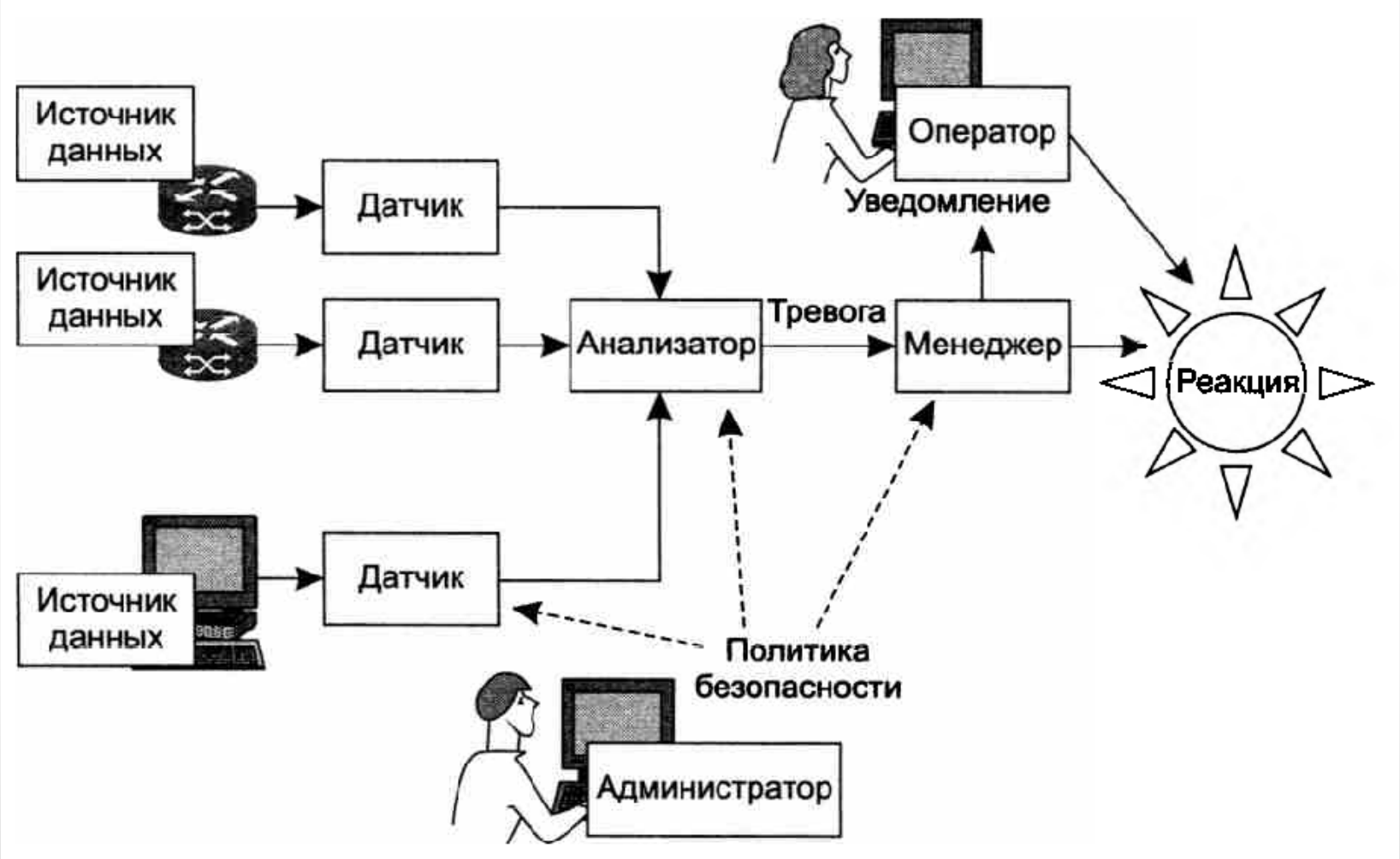
В отличие от файерволов и прокси-серверов, которые строят защиту сети исключительно на основе анализа сетевого трафика, системы обнаружения вторжений учитывают в своей работе различные подозрительные **события**, происходящие в системе.

Системы обнаружения вторжений

Типовая система IDS включает следующие функциональные элементы:

- источники данных;
- датчики;
- анализатор;
- администратор;
- оператор;
- менеджер.

Системы обнаружения вторжений



Системы обнаружения вторжений

Источниками данных для сетевой системы IDS являются маршрутизаторы, коммутаторы и хосты локальной сети.

Датчик копирует пакеты, циркулирующие в сети, и передает их анализатору для выявления подозрительной активности. Датчик может представлять собой отдельный компьютер, подключенный к зеркализованному порту коммутатора, или же это может быть программный компонент маршрутизатора, который имеет доступ к пакетам, буферизуемым на его интерфейсах.

Системы обнаружения вторжений

Анализатор является «мозгом» IDS, он получает данные от датчиков и проверяет их на наличие угроз и подозрительной активности в сети.

Анализатор работает на основе правил, составленных **администратором** системы безопасности предприятия в соответствии с политикой безопасности. При выполнении условия одного из правил анализатор вырабатывает сообщение тревоги и передает его **менеджеру** системы IDS – программному компоненту, который хранит конфигурацию IDS и поддерживает удобный интерфейс с оператором IDS.

Системы обнаружения вторжений

Менеджер IDS оповещает оператора IDS о тревоге

Оператор системы IDS на основе данных уведомления принимает решение о реакции сети на подозрительную активность (отключение сетевого интерфейса, через который поступает подозрительный трафик, изменение правил файервола для блокировки определенных пакетов или же игнорирование уведомления, если оператор считает, что вероятность вторжения крайне мала).

Системы обнаружения вторжений

Наряду с системами обнаружения вторжений существуют **системы предупреждения вторжений (Intrusion Prevention Systems, IDP)**, которые выполняют автоматические действия по прекращению атаки в случае ее обнаружения.

Системы обнаружения вторжений

В IDS для обнаружения вторжений применяются нескольких типов правил:

- **правила, основанные на сигнатуре (подписи) атаки (Signature Rules);**
- **правила, основанные на анализе протоколов (Protocol Rules);**
- **правила, основанные на статистических аномалиях трафика.**

Атаки на стек протоколов TCP/IP

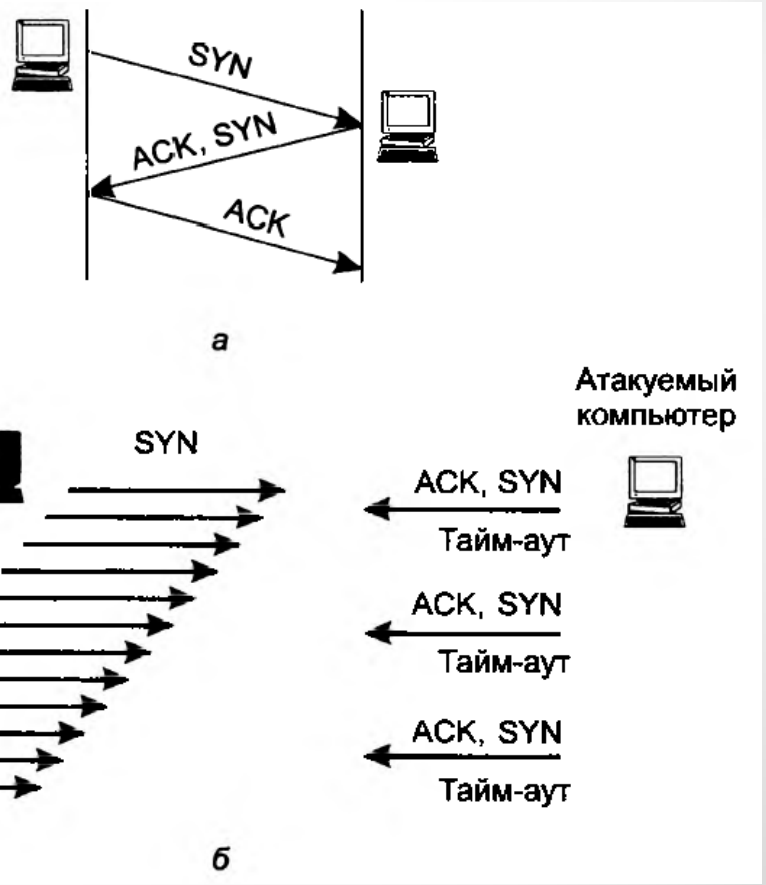
Протокол TCP используется злоумышленниками и как инструмент для организации атак (обычно это атаки отказа в обслуживании), и как цель нападения – нарушение TCP-сеанса атакуемого приложения, например, путем подделки сегмента.

Атаки на стек протоколов TCP/IP

Проведение DoS-атаки, в которой используются особенности протокола TCP:

а – нормальный порядок установления TCP-соединения;

б – DoS-атака путем создания множества незакрытых TCP-соединений.



Атаки на стек протоколов TCP/IP

Атака **подделкой TCP-сегмента** состоит в генерации TCP-сегментов, все атрибуты которых имеют значения, легитимные для некоторого существующего TCP-сеанса атакуемого компьютера (IP-адреса, номера TCP-портов, порядковые номера из текущего диапазона окна приема).

Принимающая сторона не может отличить такие поддельные сегменты от настоящих и помещает информацию злоумышленника в поток пользовательских данных – злоумышленник может поместить ложную информацию в базу данных, заразить атакуемый компьютер вирусом и т. п.

Атаки на стек протоколов TCP/IP

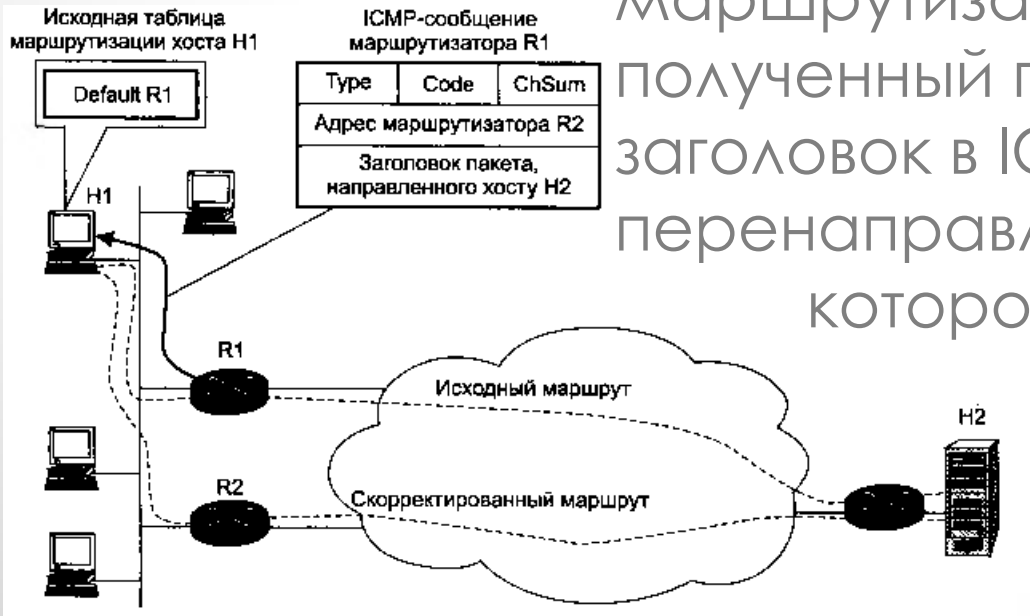
Атака **сбросом TCP-соединения** используется для разрыва TCP-соединений легальных пользователей. При поступлении TCP-сегмента с установленным флагом **RST** узел должен немедленно завершить сеанс, к которому относится этот сегмент, и удалить все данные, полученные в ходе сеанса.

Для проведения атаки злоумышленник должен подделать заголовок TCP-сегмента.

Атаки на стек протоколов TCP/IP

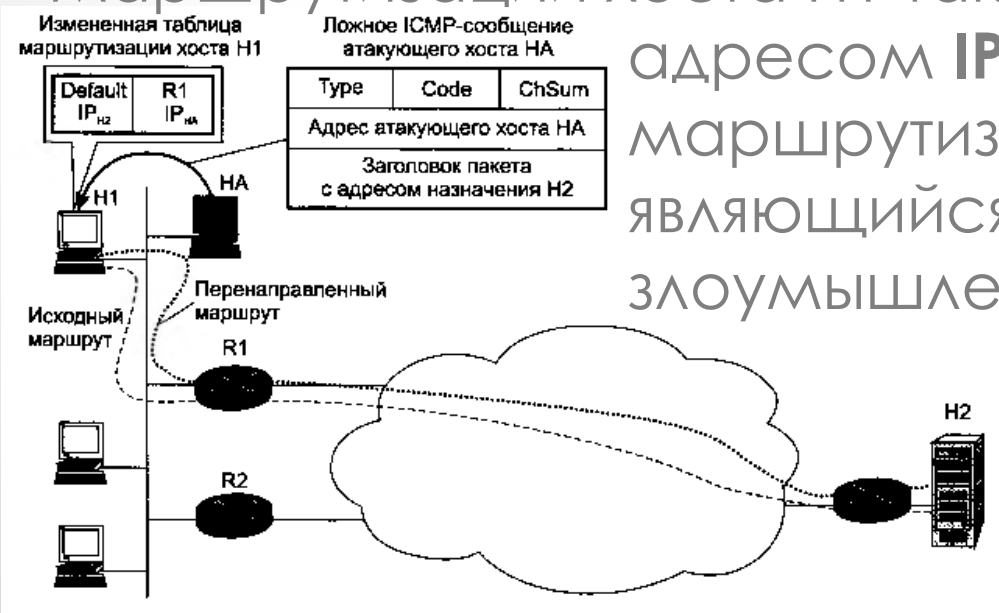
ICMP-атака «Перенаправление трафика»

Маршрутизатор по умолчанию R1, получив от хоста H1 пакет, адресованный хосту H2, определяет, что наилучший маршрут пролегает через маршрутизатор R1, отбрасывает полученный пакет и помещает его заголовок в ICMP-сообщение о перенаправлении маршрута, которое посылает хосту H1.



Атаки на стек протоколов TCP/IP

Злоумышленник формирует и посылает хосту H1 пакет, маскирующийся под ICMP-сообщение о перенаправлении маршрута. В этом сообщении содержится запрос о корректировке таблицы маршрутизации хоста H1 так, чтобы во всех пакетах с адресом IP_{H2} адресом следующего маршрутизатора стал адрес IP_{HA}, являющийся адресом хоста-злоумышленника HA.



Атаки на стек протоколов TCP/IP

ICMP-атака Smurf

ICMP-атака Smurf – это DDoS-атака, использующая функцию **эхо-запроса** протокола ICMP (название атаки произошло от имена файла **smurf.**c, содержащего код атаки и получившего распространение в 1998 году).

В атаке Smurf эхо-запрос посылается по **широковещательному** (**broadcast**) адресу некоторой сети.

Атаки на стек протоколов TCP/IP

В ICMP-атаке Smurf используется характерный прием – усиление атаки за счет **отражения** посланного пакета большим количеством компьютеров.

Атаки на стек протоколов TCP/IP

Ping-затопление – злоумышленник использует утилиту ping своей операционной системы для отправки эхо-запросов на атакуемый компьютер с максимально возможной частотой.

UDP-затопление относится к DoS-атакам и имеет целью исчерпание пропускной способности интерфейса атакуемого компьютера. Атакуемый компьютер обязан принимать все направляемые ему UDP-дейтаграммы и не может заставить передающий компьютер ограничить интенсивность потока направляемых ему пакетов, уменьшив размер окна приема.

Атаки на стек протоколов TCP/IP

Атака на IP-опции – представляет собой DoS-атаку на маршрутизаторы, в которой используется поле дополнительных опций протокола IP. В **IPv4** заголовок IP-пакета может включать поле опций, которые задают некоторую **нестандартную обработку** пакета маршрутизатором.

Атаки на стек протоколов TCP/IP

Атака на фрагментацию направлена на конечные узлы IP-сетей, в обязанность которых входит сборка фрагментированного IP-пакета в единое целое:

- **превышение максимальной длины пакета (переполнение буфера сборки)**;
- **перекрытие сегментов за счет специального подбора смещений и длин фрагментов**;
- **замещение фрагментов**;
- **незавершенные фрагменты**.

Защита сетевых соединений

Задачу защиты данных можно разделить на две подзадачи:

- защиту данных внутри компьютера;
- защиту данных в процессе их передачи от одного компьютера к другому.

Защита сетевых соединений

Технология защищенного канала обеспечивает защиту трафика между двумя точками в открытой транспортной сети.

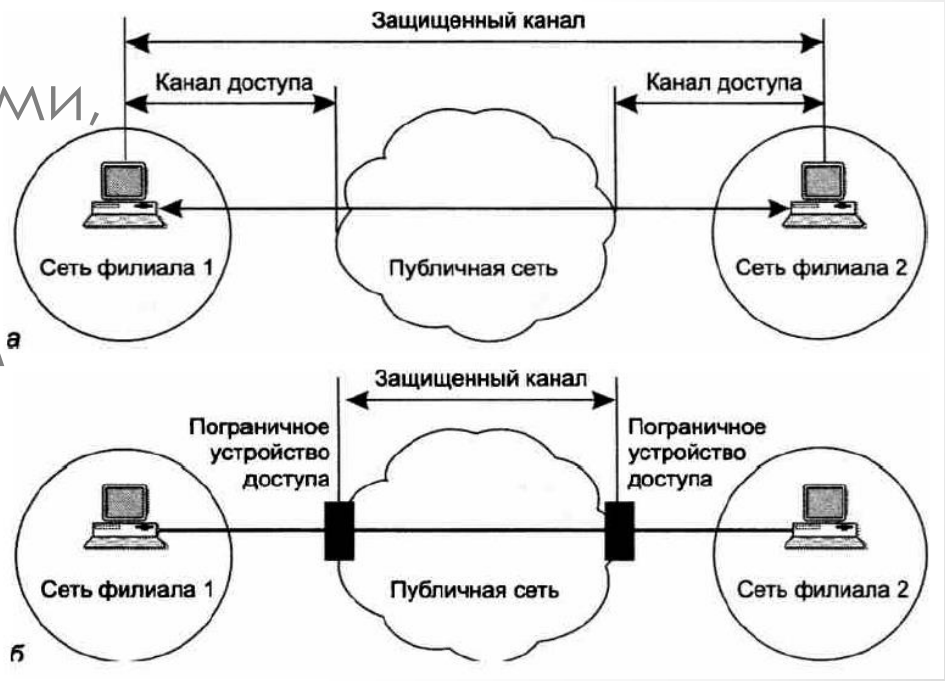
Защищенный канал подразумевает выполнение трех основных функций:

- **взаимная аутентификация** абонентов при установлении соединения (обмен паролями);
- **защита передаваемых** по каналу **сообщений** от несанкционированного доступа (шифрование);
- **подтверждение целостности** поступающих по каналу сообщений (ЭЦП).

Защита сетевых соединений

В зависимости от месторасположения программного обеспечения защищенного канала различают:

- схему с конечными узлами, взаимодействующими через публичную сеть;
- схему с оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями.



Защита сетевых соединений

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели OSI.

Уровни защищаемых протоколов	Протоколы защищенного канала	Свойства протоколов защищенного канала
Прикладной уровень	S/MIME	Непрозрачность для приложений, независимость от транспортной инфраструктуры
Уровень представления	SSL, TLS	
Сеансовый уровень		
Транспортный уровень		
Сетевой уровень	IPSec	Прозрачность для приложений, зависимость от транспортной инфраструктуры
Канальный уровень	PPTP	
Физический уровень		

Защита сетевых соединений

Защищенный канал, реализованный на самом высоком (прикладном) уровне, защищает только вполне определенную сетевую службу, например файловую, гипертекстовую или почтовую.

Протокол **S/MIME** защищает исключительно сообщения электронной почты.

При таком подходе для каждой службы необходимо разрабатывать собственную защищенную версию протокола.

Защита сетевых соединений

Протокол **SSL** (**Secure Socket Layer** – слой защищенных сокетов) работает на уровне представления и создает защищенный канал, используя следующие технологии безопасности:

- взаимная аутентификация приложений на обоих концах защищенного канала выполняется путем обмена **сертификатами** (стандарт X.509);
- для контроля целостности передаваемых данных используются **дайджесты**;
- секретность обеспечивается шифрацией средствами **симметричных ключей сеанса**.

Защита сетевых соединений

Средства защищенного канала становятся прозрачными для приложений в тех случаях, когда безопасность обеспечивается на сетевом и канальном уровнях.

Здесь наблюдается **зависимость** сервиса защищенного канала от протокола нижнего уровня.

Например, протокол PPTP, не являясь протоколом канального уровня, защищает кадры протокола PPP канального уровня, упаковывая их в IP-пакеты.

Защита сетевых соединений

Работающий на сетевом уровне протокол **IPSec** является компромиссным вариантом.

С одной стороны, он прозрачен для приложений, с другой – может работать практически во всех сетях, так как основан на широко распространенном протоколе IP и использует любую технологию канального уровня (PPP, Ethernet, ATM и т. д.).

Протокол IPsec

Протокол IPSec в стандартах Интернета называют **системой** – это согласованный набор открытых стандартов, ядро которого составляют протоколы:

- **AH (Authentication Header – заголовок аутентификации)**;
- **ESP (Encapsulating Security Payload – инкапсуляция зашифрованных данных)**;
- **IKE (Internet Key Exchange – обмен ключами Интернета)**.

Протокол IPsec

<table>
<tr><th>Выполняемые функции</th><th colspan="2">Протокол</th></tr>
<tr><td>Обеспечение целостности</td><td rowspan="2">AH</td><td rowspan="3">ESP</td></tr>
<tr><td>Обеспечение аутентичности</td></tr>
<tr><td>Обеспечение конфиденциальности (шифрование)</td><td></td></tr>
<tr><td>Распределение секретных ключей</td><td colspan="2">IKE</td></tr>
</table>

Протокол IPsec

Протокол **AH** позволяет приемной стороне убедиться, что:

- пакет был отправлен стороной, с которой установлена безопасная ассоциация;
- содержимое пакета не было искажено в процессе его передачи по сети;
- пакет не является дубликатом уже полученного пакета.

Протокол IPsec

Протокол **ESP** решает две группы задач:

- задачи обеспечения аутентификации и целостности данных на основе дайджеста, аналогичные задачам протокола AH;
- защита передаваемых данных путем их шифрования от несанкционированного просмотра.

Протокол IPsec

Протокол **IKE** решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

Безопасность сетевых служб

Программная система, состоящая из десятков тысяч строк кода, всегда имеет **уязвимости**, которые может использовать злоумышленник.

Эти уязвимости могут быть результатом ошибок программистов: в соответствии с исследованием CyLab Университета Карнеги Мэллона **в среднем каждые 1000 строк кода содержат 20-30 ошибок**, из которых 5 % влияют на безопасность системы, а 1 % открывает возможности для взлома системы.

Вредоносное программное обеспечение

Многочисленная группа атак на информационные системы в настоящее время связана с внедрением в компьютеры **вредоносных программ**, к числу которых относятся **троянские** и **шпионские программы**, **черви**, **вирусы**, **спам**, **логические бомбы** и некоторые другие типы программ, нацеленные на преодоление системы безопасности.

Вредоносный код чаще всего классифицируют по **способу проникновения** кода в чужой компьютер, а также по **целевому назначению**.

Вредоносное программное обеспечение

Троянские программы, или **трояны** (**trojan**), – это разновидность вредоносных программ, которые наносят ущерб системе, маскируясь под какие-либо полезные приложения.

Троянские программы могут применять в качестве прикрытия знакомые пользователю приложения.

При другом подходе в полном соответствии с древней легендой троянская программа принимает вид нового приложения, которое пытается заинтересовать пользователя-жертву какими-то своими якобы полезными функциями.

Вредоносное программное обеспечение

Сетевые черви (**worm**) – это программы, способные к самостоятельному распространению своих копий среди узлов в пределах локальной сети, а также по глобальным связям, перемещаясь от одного компьютера к другому без всякого участия в этом процессе пользователей сети.

Поскольку большинство сетевых червей передаются в виде файлов, основным механизмом их распространения являются сетевые службы, основанные на файловом обмене. Червь может рассылать свои копии по сети в виде вложений в электронной почте или путем размещения ссылок на зараженный файл на веб-сайте.

Вредоносное программное обеспечение

Главная цель и результат деятельности червя состоит в том, чтобы **передать свою копию на максимально возможное число компьютеров**. При этом для поиска компьютеров – новых потенциальных жертв – черви задействуют встроенные в них средства.

Типичная программа-червь не удаляет и **не искажает** пользовательские и системные файлы, **не перехватывает электронную почту** пользователей, **не портит содержимое баз данных**, а наносит вред атакованным компьютерам **потреблением их ресурсов** (рассылка спама или проведения массированной атаки в составе ботнета).

Вредоносное программное обеспечение

Червь состоит из двух основных функциональных компонентов:

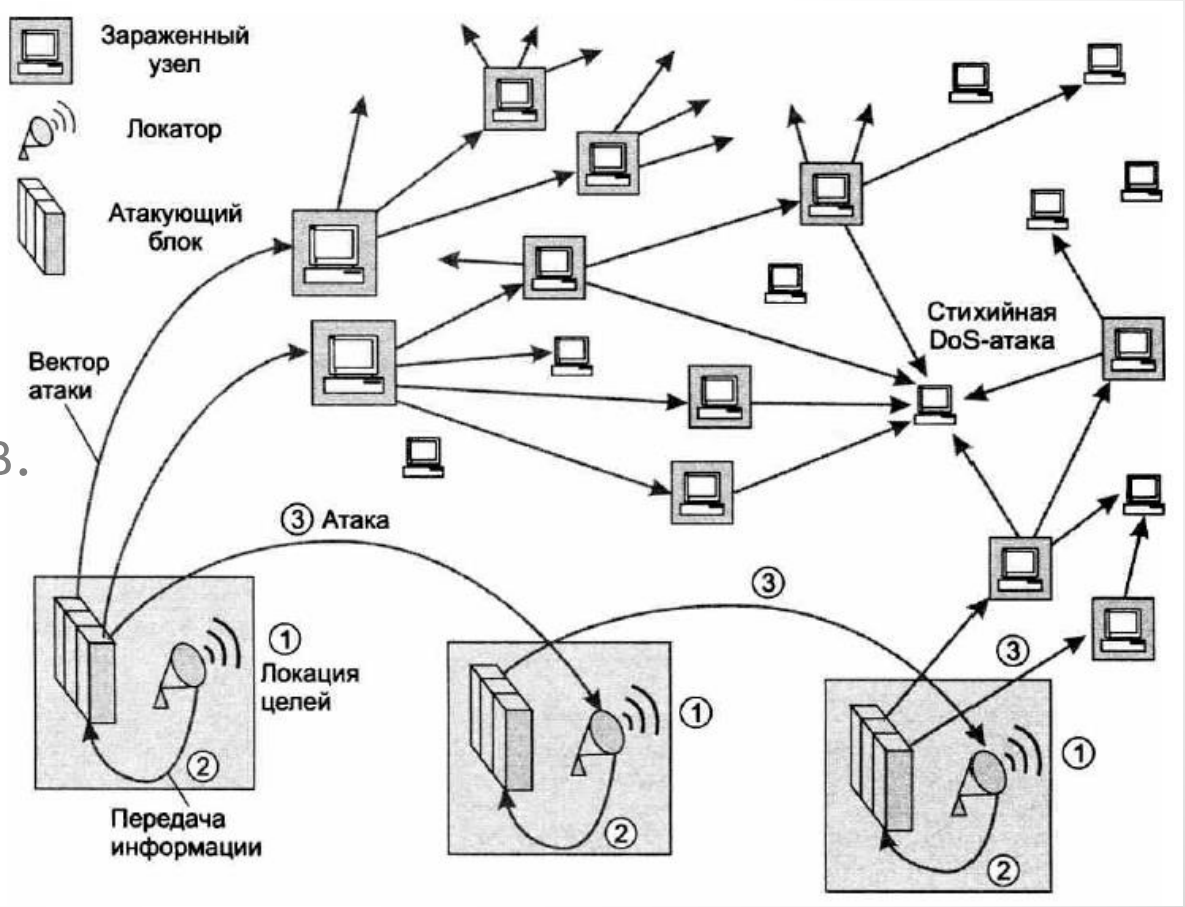
- **атакующий блок** состоит из нескольких модулей (векторов атаки), каждый из которых рассчитан на поражение конкретного типа уязвимости. Этот блок открывает «входную дверь» атакуемого хоста и передает через нее свою копию;
- **блок поиска целей** (**локатор**) собирает информацию об узлах сети, а затем на основании этой информации определяет, какие из исследованных узлов обладают теми уязвимостями, для которых хакер имеет средства атаки.

Вредоносное программное обеспечение

1 – запуск локатора;

2 – поиск узлов-целей и их атака;

3 – копирование своей сущности на новые носители и запуск локаторов.



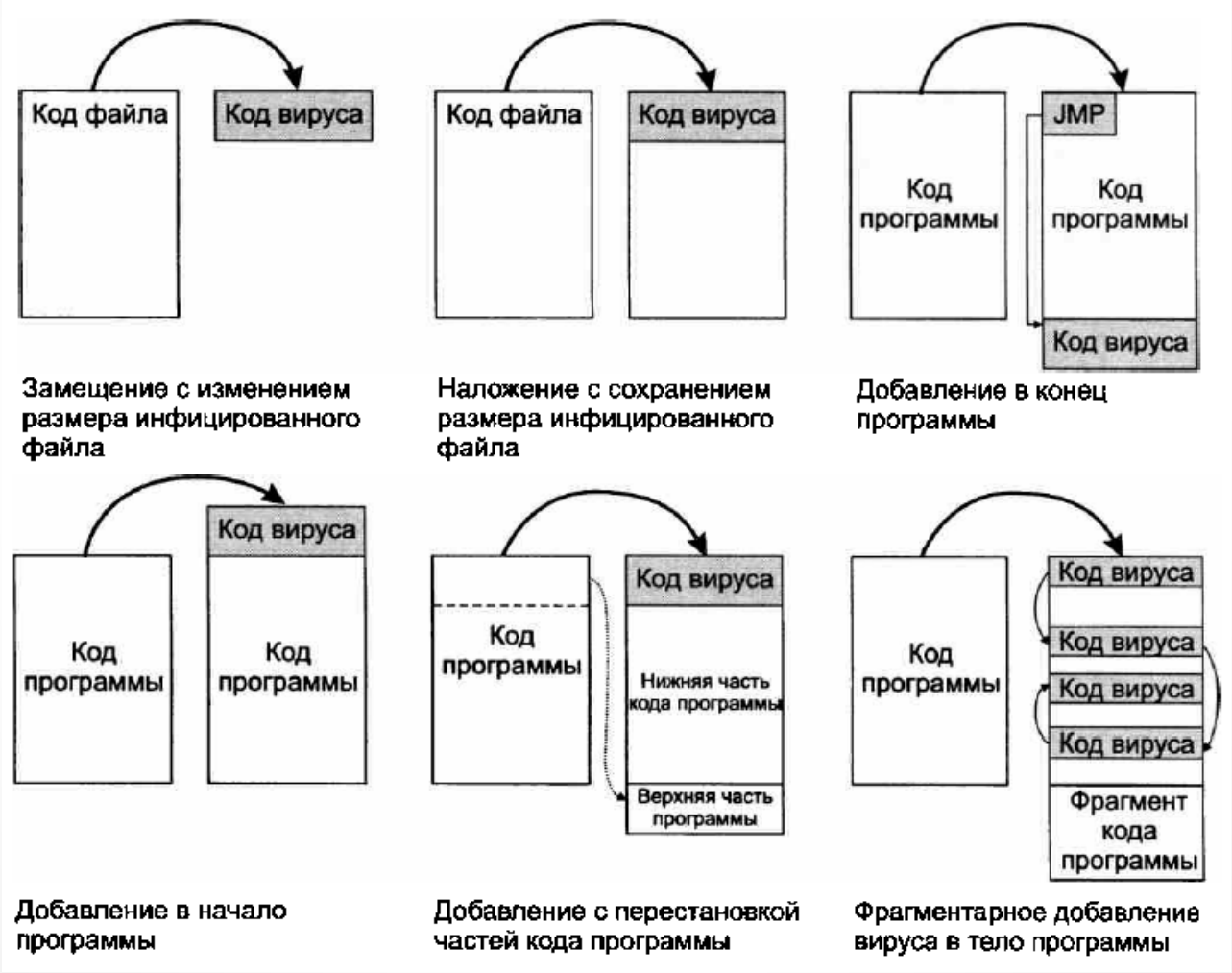
Вредоносное программное обеспечение

Вирус (**virus**) – это вредоносный программный фрагмент, который может внедряться в другие файлы.

В отличие от червей вирусы (так же, как и троянские программы) не содержат в себе встроенного механизма активного распространения по сети, они способны размножаться **своими силами** только в пределах одного компьютера.

Вирус может внедрять свои фрагменты в разные типы файлов, в том числе в файлы исполняемых программ.

Вредоносное программное обеспечение



Вредоносное программное обеспечение

Программная закладка – это встроенный в программное обеспечение объект, который при определенных условиях (входных данных) инициирует выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию.

Функции, описание которых отсутствует в документации, называют **недекларированными возможностями,** поэтому обычно понятие «программная закладка» несет **отрицательный смысл.**

Вредоносное программное обеспечение

Программные закладки могут выполнять различную вредоносную работу:

- шпионить за действиями пользователя и передавать эту информацию на определенный сервер – это так называемые **шпионские программы** (**spyware**);
- получать доступ к конфиденциальной информации;
- искажать и разрушать данные.

Вредоносное программное обеспечение

Ботнет – это совокупность сетевых устройств, на которые проникла программа (**бот**), выполняющая некоторые автоматические (часто интеллектуальные) действия по командам удаленного центра управления.

Бот является **программным роботом**, который может реагировать на возникающую ситуацию и полученные извне команды некоторыми действиями:

- протоколированием сообщений (полезный бот ведет архив чатов);
- отправкой сообщений;
- участием в DDoS-атаке на какой-то сайт или сервер.

Вредоносное программное обеспечение

Боты проникают в удаленные компьютеры нелегально, как вирусы, черви или троянские кони.

Пользователь может не знать, что его компьютер заражен ботом, потому что компьютеру этого пользователя бот не причиняет вреда, его цели находятся где-то в Интернете.

Вредоносное программное обеспечение

Для управления ботами центр управления использует различные протоколы, одним из наиболее распространенных является протокол **IRC** (**Internet Relay Chat**), позволяющий передавать мгновенные сообщения (чат).

Так как «хозяин» ботнета точно не знает, какие именно машины оказались зараженными кодом бота, для распознавания компьютеров-зомби используются методы сетевого сканирования, например сканирование портов, если код бота слушает определенный порт TCP.

Протокол HTTPS

Веб-браузер для взаимодействия с веб-сервером по умолчанию использует протокол HTTP без дополнительных мер по обеспечению основных свойств безопасных коммуникаций, то есть аутентификации сторон, а также конфиденциальности, доступности и целостности данных.

Естественно, это создает значительные риски безопасности при работе с сайтами Интернета.

Протокол HTTPS

Очевидно, что прослушивание открытого трафика между браузером и веб-сервером может нарушить **конфиденциальность** данных и их **целостность**, если злоумышленник по какой-то причине внесет какие-то изменения в данные. Злоумышленник может также нарушить **доступность** данных, просто отбрасывая ответы веб-сайта.

Протокол HTTPS

Основным способом обеспечения перечисленных свойств безопасности данных, циркулирующих между веб-браузером и веб-сайтом, является использование безопасного **протокола передачи гипертекста** (**Hypertext Transfer Protocol Secure**, **HTTPS**) вместо HTTP.

В HTTPS-соединении сам протокол HTTP, работающий поверх протокола SSL, остается неизменным. Все атрибуты безопасности коммуникаций – аутентификация, конфиденциальность и целостность – обеспечиваются протоколом защищенного канала SSL.

Протокол HTTPS

Аутентификация в протоколе SSL основана на цифровых сертификатах.

Поэтому при обращении веб-браузера к веб-серверу по протоколу HTTPS каждая из сторон должна иметь подписанный центром сертификации сертификат, достоверность которого можно проверить по цепочке доверия, ведущей к одному из доверенных корневых центров сертификации.

Протокол HTTPS

Производители с каждой копией своего браузера поставляют так называемый **встроенный цифровой сертификат**, который может применяться для аутентификации данного браузера.

Этот сертификат не аутентифицирует пользователя, работающего с браузером, он служит только для создания защищенного канала при передаче данных между браузером и веб-сервером.

Протокол HTTPS

Аутентификация сервера при установлении HTTPS-соединения всегда выполняется на основе **цифрового сертификата сервера**, получаемого владельцем сервера.

Этот сертификат подтверждает, что данный веб-сервер имеет определенные (одно или несколько) доменные имена.

Облачные сервисы и их безопасность

Новая концепция организации вычислений, получившая название **облачных вычислений** (**cloud computing**), изменяет привычный мир пользователя, так как в соответствии с ней компьютер, который выполняет программу пользователя, находится где-то в «облаке» вычислительных ресурсов – процессоров, оперативной памяти, дисковых накопителей.

Облачные сервисы и их безопасность

Облачные вычисления – это модель, предоставляющая удобный доступ по требованию к разделяемому пулу конфигурируемых вычислительных ресурсов, которые могут быть быстро выделены пользователю и отданы обратно в пул с минимальными затратами на управление этим процессом или с минимальным взаимодействием с провайдером услуг.

Облачные сервисы и их безопасность

С этим определением связаны следующие свойства облачных вычислений:

- Качественно новый уровень разделения ресурсов.
- Высокая степень масштабируемости.
- Эластичность.
- Гибкость оплаты использованных ресурсов.
- Самостоятельное выделение ресурсов.

Облачные сервисы и их безопасность

По способу реализации облачные среды делятся на публичные, частные и гибридные.

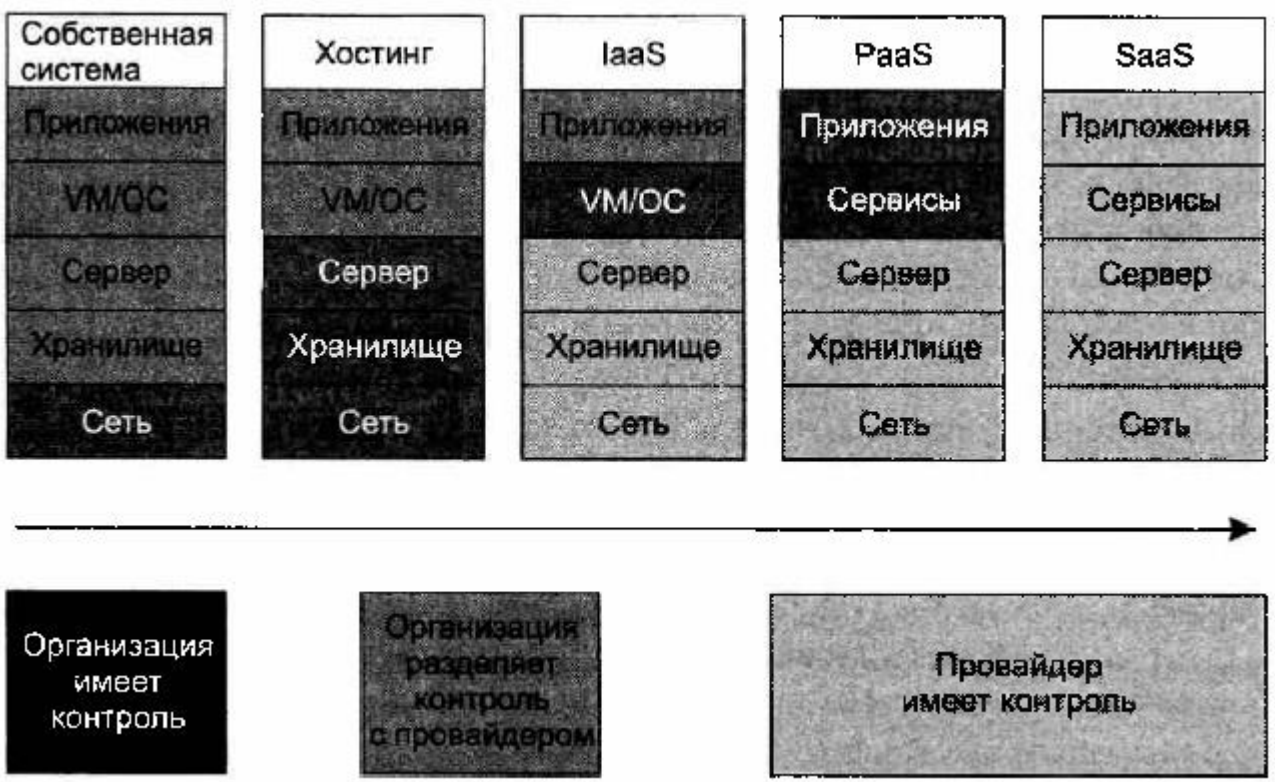
- **Публичные облака** создаются провайдерами услуг и их сервисы предоставляются предприятиям или частным лицам как публичным клиентам.
- **Частные облака** создаются некоторыми предприятиями для использования только сотрудниками этих предприятий, то есть как часть корпоративной сети предприятий.
- ***Гибридные облака*** – это комбинация публичных и частных облаков, которыми пользуется некоторое предприятие.

Облачные сервисы и их безопасность

На сегодня существуют три основные модели сервисов, предоставляемых провайдерами облачных вычислений:

- **приложения как сервис** (**Software-As-a-Service**, **SaaS**);
- **платформа как сервис** (**Platform-AS-a-Service**, **PaaS**);
- **инфраструктура как сервис** (**The Infrastructure-As-a-Service**, **IaaS**).

Облачные сервисы и их безопасность



Распределение контроля и ответственности между провайдером и клиентом в разных моделях облачных сервисов.

Облачные сервисы и их безопасность

Модель облачных вычислений существенно отличается от традиционной модели вычислений, используемой сегодня в корпоративных ИС, и это отличие прежде всего сказывается на обеспечении безопасности ИС.

Природа данного отличия довольно проста – вместо того, чтобы строить собственную информационную систему и управлять ею силами сотрудников предприятия, предприятие начинает пользоваться услугами информационной системы, созданной посторонней организацией-провайдером.

Облачные сервисы и их безопасность

Предприятие-клиент облачных сервисов имеет весьма **ограниченный контроль** над механизмами безопасности своих данных, обрабатываемых виртуальными машинами провайдера и хранящимися в виртуальных хранилищах.

Особенно это справедливо для услуг модели **SaaS**, когда защита всех элементов ИС, включая прикладные программы пользователя, осуществляется провайдером.

Предприятие-клиент в этом случае участвует лишь в обеспечении безопасности компьютеров своих сотрудников, которые применяются как терминалы облачной среды.

Облачные сервисы и их безопасность

Клиент **IaaS**-сервиса должен самостоятельно заботиться о безопасности своих приложений – следить за тем, чтобы обновления приложений периодически получались и устанавливались, устанавливать и обслуживать антивирусные программы и программы блокировки спама, выполнять все остальные действия в соответствии с политикой безопасности предприятия, которые относятся к приложениям.

В модели **PaaS** контроль над средствами безопасности верхних уровней разделяется между провайдером и клиентом.

Облачные сервисы и их безопасность

При использовании услуг облачного провайдера **разделяется его инфраструктура** с другими неизвестными арендаторами.

При этом разделение ресурсов провайдера осуществляется не на физическом уровне, а с помощью механизмов виртуализации.

Злоумышленник может заключить договор с провайдером и попытаться использовать бреши в механизмах виртуализации для получения несанкционированного доступа к чужим данным. Кроме того, нельзя исключать ошибок персонала провайдера, в результате которых виртуальные барьеры могут быть нарушены.

Защита информации беспроводных сетях

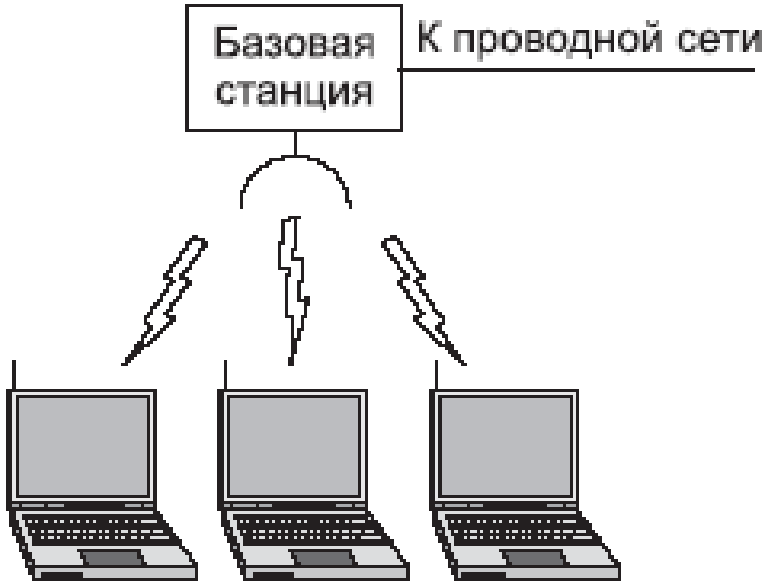
На профессиональном жаргоне стандарт получил название **Wi-Fi** (Wireless Fidelity).

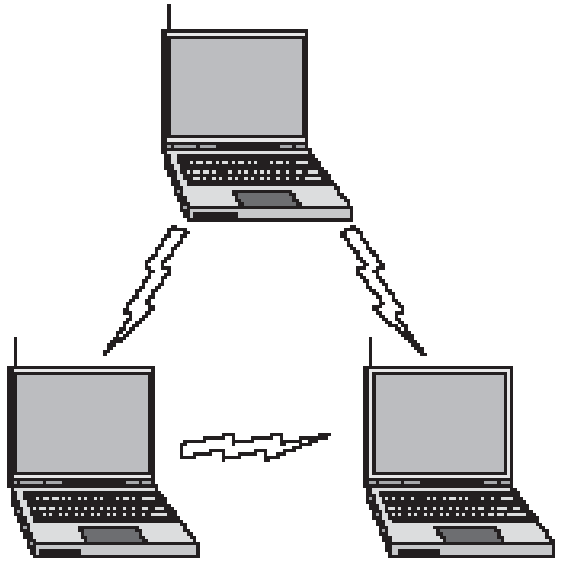
IEEE 802.11 работает на частотах ISM-организаций (для некоммерческого использования в промышленности, научных и медицинских организациях):

902–928 МГц, 2.4–2.5 ГГц, 5.725–5.825 ГГц.

Всем устройствам разрешается использовать эти частоты при условии, что они ограничивают свою мощность передачи до 1 мВт, чтобы не создавать помех в работе других устройств.

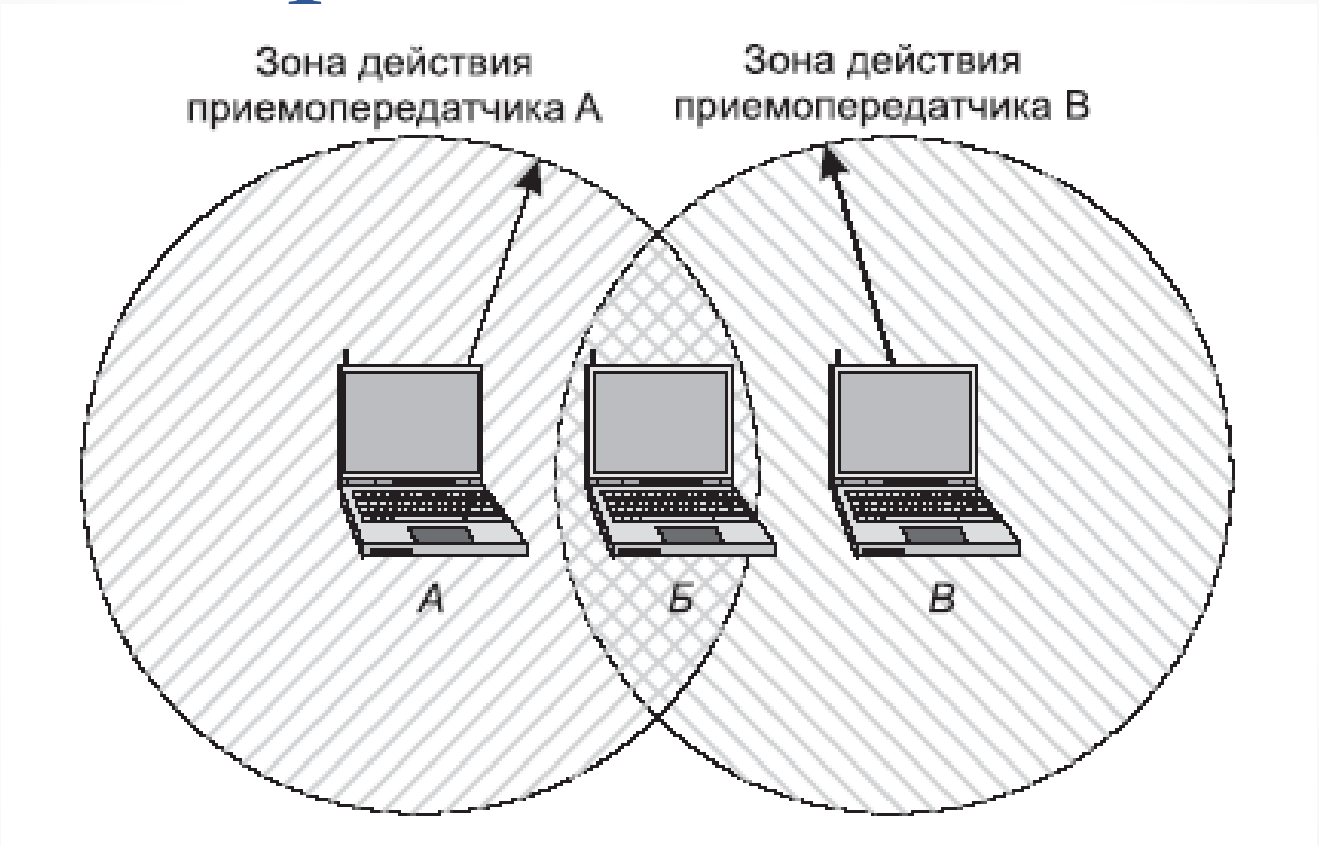
Защита информации беспроводных сетях





Беспроводная сеть с точкой доступа и специальная сеть

Защита информации беспроводных сетях



Радиус действия одного радиопередатчика может не покрывать всю систему

Защита информации беспроводных сетях

Стандарт 802.11 определяет сервисы, чтобы клиенты, точки доступа и соединяющие их сети могли быть согласованными беспроводными ЛВС:

- ассоциация;
- реассоциация;
- дизассоциация;
- аутентификация;
- служба распределения;
- служба интеграции;
- доставка данных;
- служба конфиденциальности;
- служба планирования трафика QOS;
- регулирование мощности передатчика;
- динамический выбор частоты.

Защита информации беспроводных сетях

Ассоциация. Этот сервис используется мобильными станциями для подключения к точкам доступа.

Обычно он применяется сразу же после вхождения в зону действия точки доступа.

По прибытии станция узнает идентификационную информацию и возможности точки доступа.

Защита информации беспроводных сетях

Возможности точки доступа включают поддерживаемую скорость передачи данных, меры безопасности, возможности энергосбережения, поддержку качества обслуживания и т. д.

Мобильная станция посылает запрос на ассоциацию с точкой доступа, которая может принять либо отвергнуть этот запрос.

Защита информации беспроводных сетях

Реассоциация позволяет станции сменить точку доступа.

Эта возможность полезна при перемещении станции от одной точки доступа к другой в той же расширенной 802.11 LBC, по аналогии с передачей в сотовой сети.

По инициативе мобильной станции или точки доступа может быть произведена **дизассоциация**, то есть разрыв отношений.

Она требуется при выключении станции или ее уходе из зоны действия точки доступа.

Защита информации беспроводных сетях

Когда кадры достигают точки доступа, **служба распределения** определяет их маршрутизацию.

Если адрес назначения является локальным для данной точки доступа, то кадры следуют напрямую по радиоканалу.

В противном случае, их необходимо пересылать по проводной сети.

Защита информации беспроводных сетях

Служба интеграции поддерживает трансляцию, необходимую, если кадр нужно выслать за пределы сети стандарта 802.11 или если он получен из сети не этого стандарта (соединение между беспроводной ЛВС и Интернетом).

Для обработки трафика с различными приоритетами имеется служба **планирования трафика QoS**.

Защита информации беспроводных сетях

Регулирование мощности передатчика дает станциям информацию, которая нужна им, чтобы соответствовать установленным нормативным пределам мощности передачи, которые варьируются в зависимости от региона.

Служба **динамического выбора частоты** дает станциям информацию, необходимую, чтобы избежать передачи в частотном диапазоне 5 ГГц, который используется радарами.

Безопасность в сетях 802.11

Прежде чем станции смогут посылать кадры через точку доступа, они должны пройти **аутентификацию**.

В зависимости от выбора схемы безопасности аутентификация поддерживается по-разному.

Если сети 802.11 «открыты», их разрешают использовать любому. Если нет – для аутентификации нужны параметры учетной записи.

Безопасность в сетях 802.11

Рекомендуемая схема, названная **WPA2** (**WiFi Protected Access 2 – WiFi Защищенный Доступ 2**), обеспечивает безопасность в соответствии со стандартом 802.11i (WPA – временная схема).

Существует два обычных сценария, в которых используется WPA2.

Безопасность в сетях 802.11

Первый – это корпоративное использование, когда у компании есть отдельный сервер для аутентификации, хранящий имена пользователей и пароли, которые используются, чтобы определить, имеет ли право клиент получить доступ к сети.

Основные стандарты – это **802.1X**, где точка доступа позволяет клиенту вести диалог с сервером аутентификации и наблюдать результат, и **EAP** (**Extendable Authentication Protocol – расширенный протокол аутентификации**), который описывает, как взаимодействуют клиент и аутентификационный сервер.

Безопасность в сетях 802.11

Второй сценарий – домашнее использование в условиях, где нет аутентификационного сервера. Вместо него есть единый общий пароль, который используется клиентами для доступа в беспроводную сеть.

Эта система менее сложная, чем в случае с аутентификационным сервером, но она и менее надежная.

Безопасность в сетях 802.11

Основная разница состоит в том, что при наличии аутентификационного сервера каждый клиент получает ключ для шифрования трафика, неизвестный другим клиентам.

При едином общем пароле для каждого клиента создается свой ключ, но у всех клиентов одинаковый пароль, и они могут узнать ключи друг друга, если захотят.

Безопасность в сетях 802.11

Ключи, использующиеся для шифрования трафика, рассчитываются как часть аутентификационного опознавания.

Опознавание происходит сразу после ассоциации и аутентификации клиента на аутентификационном сервере, если он есть.

В начале опознавания у клиента есть либо пароль для аутентификационного сервера (вариант 1), либо общий пароль сети (вариант 2).

Безопасность в сетях 802.11

Пароль используется для получения основного ключа. Но основной ключ не используется прямым образом для шифрования пакетов.

Существует стандартная криптографическая практика создавать новый ключ для каждого периода использования, менять ключ для разных сеансов и держать основной ключ в секретности.

При опознавании рассчитывается именно ключ сеанса.

Безопасность в сетях 802.11

Ключ сеанса рассчитывается при четырехпакетном опознавании.

Во-первых, **AP** (**Access Point – точка доступа**) посылает случайный номер для идентификации.

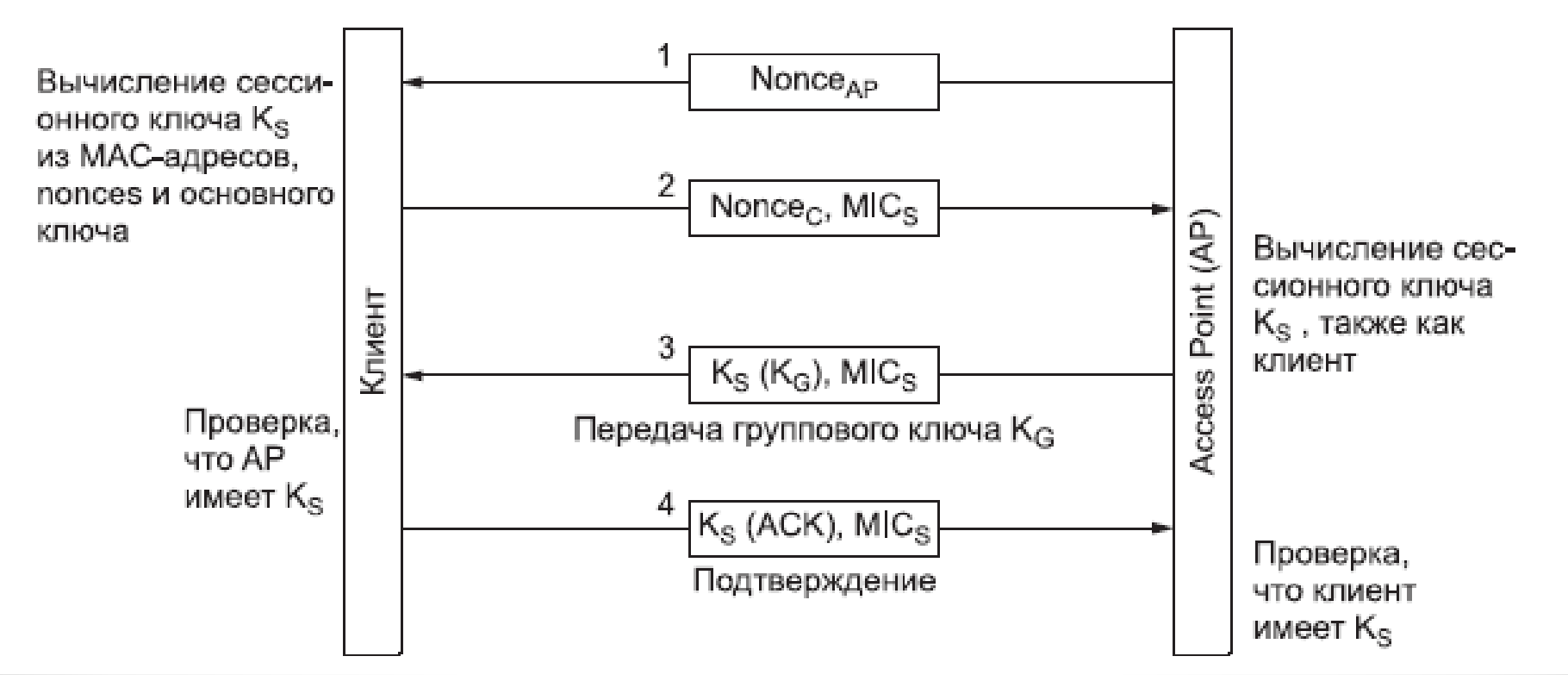
Случайные номера, использующиеся только один раз в протоколах безопасности, таких как этот, называются **nonces** (**нонсы – временные значения**), это сокращение выражения «number used once» - «номер, использующийся только один раз».

Безопасность в сетях 802.11

Клиент также выбирает свой собственный временный номер.

Он использует временный номер, адрес MAC и адрес AP, а также основной ключ, чтобы вычислить ключ сеанса, Ks.

Безопасность в сетях 802.11



Безопасность в сетях 802.11

Клиент посылает свой временный номер AP, AP производит тот же самый расчет, чтобы получить ключ сеанса.

Временные номера могут быть посланы открытым способом, так как на основании них невозможно рассчитать ключи без дополнительной, секретной информации.

Сообщение от клиента защищено проверкой целостности, которая называется **MIC** (**Message Integrity Check – проверка целостности сообщения**), данная проверка основывается на ключе сеанса.

Безопасность в сетях 802.11

В последнем из двух сообщений AP выдает клиенту общий ключ K_G, и клиент подтверждает подлинность сообщения.

Безопасность в сетях 802.11

Схема, которая использовалась до WPA, называется **WEP** (**Wired Equivalent Privacy – приватность на уровне проводной связи**).

Для этой схемы аутентификация с предустановленным ключом выполнялась перед ассоциацией.

Однако ее польза не велика из-за недостатков конструкции, которые делают WEP легко взламываемым.

Безопасность в сетях 802.11

В 802.11i могут быть использованы два протокола для обеспечения конфиденциальности, цельности и аутентификации.

1 TKIP (**Temporary Key Integrity Protocol – временный протокол целостности ключа**) был временным решением.

Он был разработан для того, чтобы увеличить безопасность старых и медленных карт 802.11, так что безопасность у него, по крайней мере, выше, чем у WEP.

Безопасность в сетях 802.11

2 CCMP (**Counter mode with Cipher block chaining message authentification code protocol**) – режим счетчика с протоколом аутентификации в режиме сцепления обратной связи.

CCMP работает довольно прямым путем. Он использует шифрование AES с помощью ключа и блоков размером 128 бит.

Чтобы обеспечить конфиденциальность, сообщения зашифровываются с помощью AES в режиме счетчика.

Безопасность в сетях 802.11

Режим счетчика подмешивает счетчик в процесс шифрования сообщения.

Чтобы обеспечить целостность, сообщение, включая поля заголовков, кодируется шифром в режиме обратной связи, и последний блок из 128 бит сохраняется как MIC.

Затем и сообщение, и MIC высылаются. И клиент, и AP могут осуществлять данную кодировку или проверить ее при получении беспроводного пакета.

Безопасность в сетях 802.11

Алгоритм шифрования для WPA2 основан на **AES** (**Advanced Encryption Standard – улучшенный стандарт шифрования**), американском правительственном стандарте, одобренном в 2002 году.

Ключи, которые используются для шифрования, определяются во время процедуры аутентификации.

Безопасность систем Bluetooth

В 1994 году компания Л. М. Эриксона заинтересовалась вопросом беспроводной связи между мобильными телефонами и другими портативными устройствами. Совместно с четырьмя другими небезызвестными компаниями (IBM, Intel, Nokia и Toshiba) в 1998 году была сформирована специальная группа (**SIG – Special Interest Group**), которая занялась развитием стандарта беспроводного соединения вычислительных устройств и устройств связи, а также созданием аксессуаров, использующих недорогие маломощные радиоустройства небольшого радиуса действия.

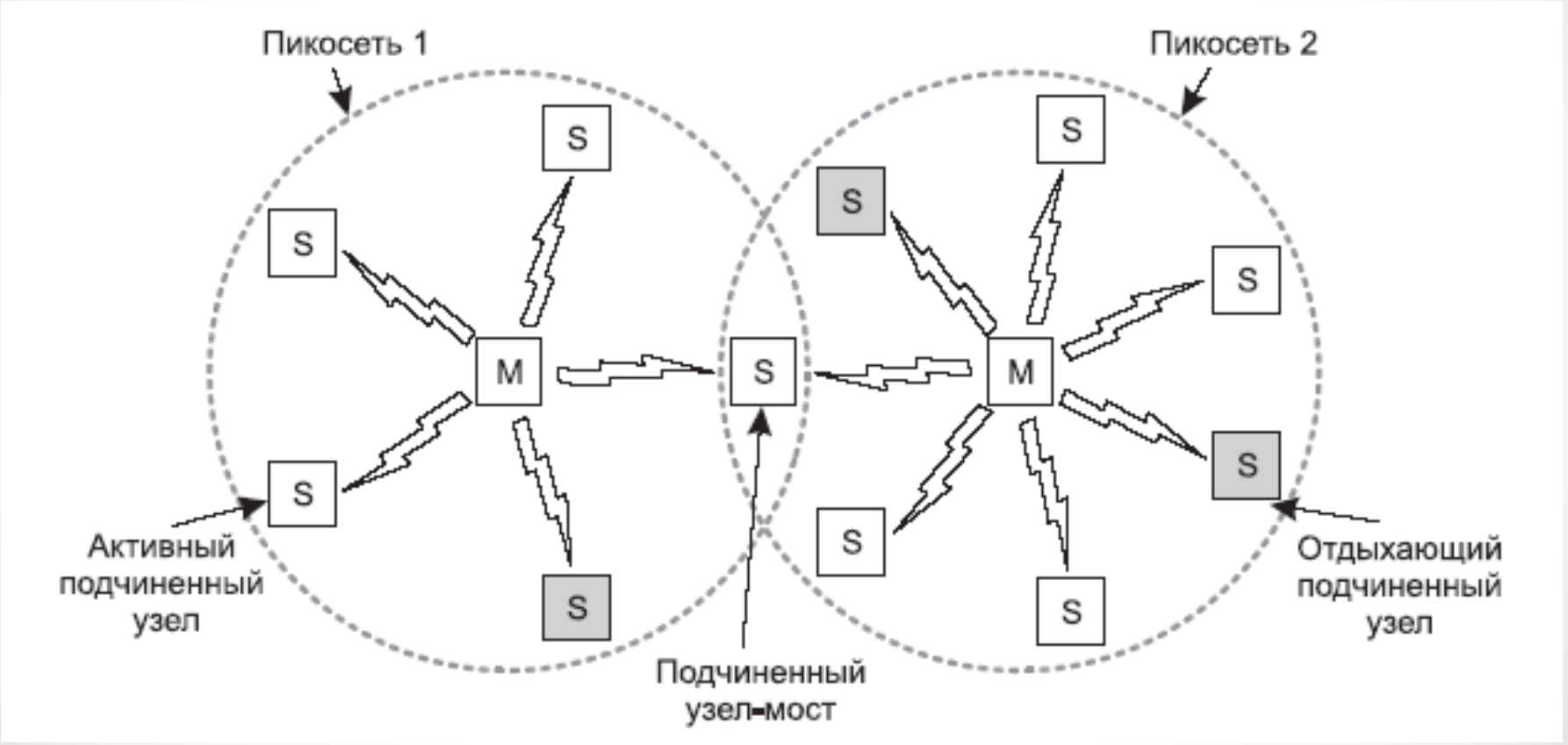
Безопасность систем Bluetooth

Проект был назван **Bluetooth** («Синий зуб») в честь великого короля викингов по имени Гаральд Синий Зуб II (940—981), который завоевал Данию и Норвегию.

Основу Bluetooth составляет **пикосеть**, состоящая из одного главного узла и нескольких (до семи) подчиненных узлов, расположенных в радиусе до 10 метров.

Пикосети могут связываться друг с другом посредством моста (специального узла). Несколько объединенных вместе пикосетей составляют **рассеянную сеть**.

Безопасность систем Bluetooth



Безопасность систем Bluetooth

Проект был назван **Bluetooth** («Синий зуб») в честь великого короля викингов по имени Гаральд Синий Зуб II (940—981), который завоевал Данию и Норвегию.

Основу Bluetooth составляет **пикосеть**, состоящая из одного главного узла и нескольких (до семи) подчиненных узлов, расположенных в радиусе до 10 метров.

Пикосети могут связываться друг с другом посредством моста (специального узла). Несколько объединенных вместе пикосетей составляют **рассеянную сеть**.

Безопасность систем Bluetooth

Радиус действия систем Bluetooth значительно меньше, чем сетей 802.11, поэтому взломщику не удастся произвести атаку, оставив ноутбук в припаркованной рядом со зданием машине, однако вопрос безопасности важен и тут.

Система защиты Bluetooth (версии 2.1 и более поздние) может работать в четырех режимах, начиная от полного бездействия и заканчивая тотальным шифрованием данных и контролем целостности.

Безопасность систем Bluetooth

Bluetooth обеспечивает безопасность на нескольких уровнях.

На физическом уровне для этого применяются скачкообразные изменения частот, но поскольку любое устройство, появляющееся в микросети, должно узнать последовательность скачков частоты, эта последовательность, очевидно, не является секретной.

Безопасность систем Bluetooth

До появления Bluetooth 2.1 предполагалось, что оба устройства совместно использовали предварительно установленный закрытый ключ.

В некоторых случаях он прошивается в обоих устройствах (например, в гарнитуре и мобильном телефоне, продающихся вместе).

В других случаях в одном из устройств (например, в гарнитуре) ключ прошит, а в сопряженное устройство (например, мобильный телефон) пользователь должен ввести ключ вручную в виде десятичного числа. Общие ключи такого типа называются **отмычками**.

Безопасность систем Bluetooth

Отмычки очень часто жестко кодируются как «1234» или другие предсказуемые значения, и в любом случае это будет четырехзначное число, имеющее только 104 варианта.

При Bluetooth 2.1 устройства выбирают код из шестизначного диапазона, что делает отмычку менее предсказуемой, но все же недостаточно надежной.

Безопасность систем Bluetooth

Перед установкой канала подчиненное и управляющее устройства должны выяснить, владеют ли они отмычками.

В случае положительного ответа им необходимо договориться о том, каким будет канал: шифрованным, с контролем целостности или и таким, и таким.

Безопасность систем Bluetooth

Затем выбирается ключ сеанса длиной 128 бит, некоторые биты которого могут быть сделаны общедоступными.

Такое послабление сделано в целях соответствия системы ограничениям, введенным правительствами разных стран и запрещающим экспорт или использование ключей, длина которых больше той, что способно взломать правительство.

Безопасность систем Bluetooth

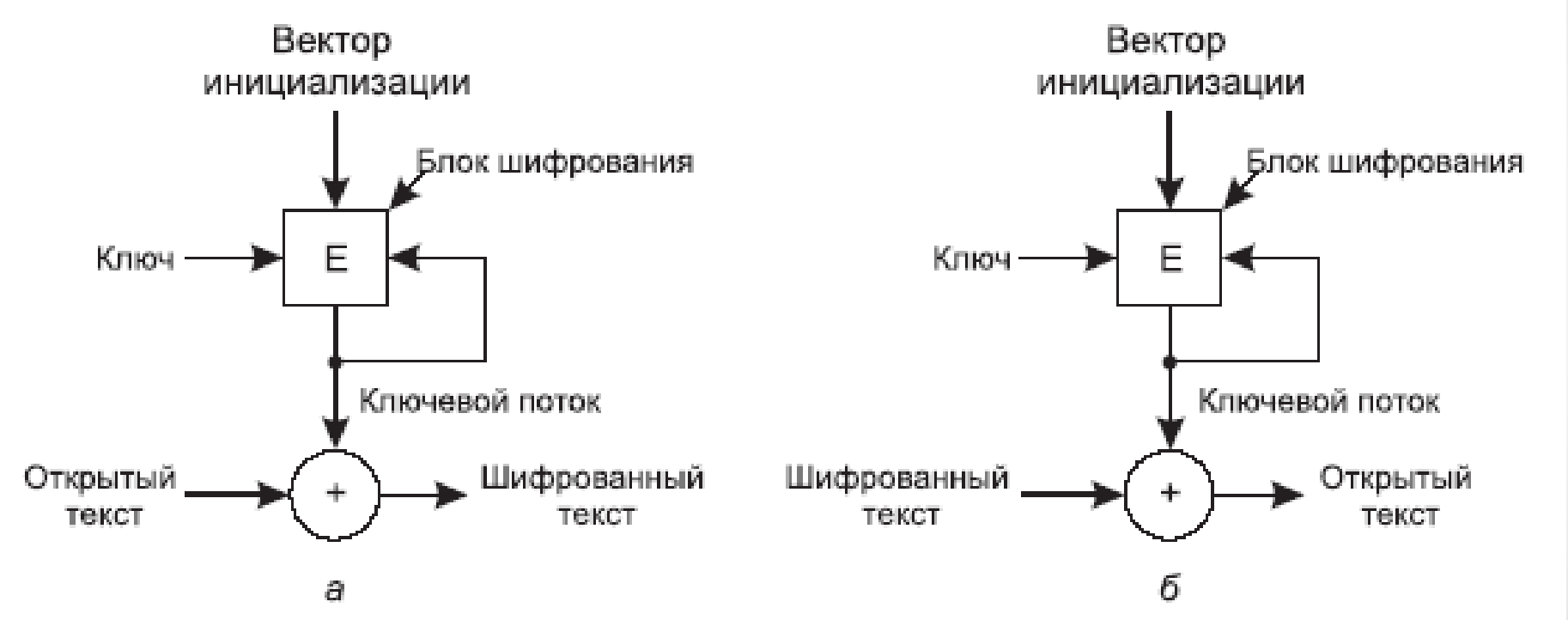
Шифрование выполняется с применением потокового шифра E0, контроль целостности – с применением **SAFER+**.

И тот и другой представляют собой традиционные блочные шифры с симметричными ключами.

SAFER+ пытались использовать в AES, однако очень быстро отказались от этой мысли, так как он работал гораздо медленнее других.

К сожалению, алгоритм E0 чрезвычайно слаб. В настоящий момент он еще не взломан, но он схож с шифром A5/1, чей провал угрожает безопасности всего GSM-трафика.

Безопасность систем Bluetooth



Групповой шифр:
а – шифрование; *б* – дешифрация

Безопасность систем Bluetooth

Еще одна проблема безопасности, связанная с Bluetooth, состоит в том, что система идентифицирует только устройства, а не пользователей.

Это приводит к тому, что вор, укравший устройство Bluetooth, получит доступ к финансовым и другим счетам жертвы.

Безопасность систем Bluetooth

Тем не менее система безопасности в Bluetooth реализована и на верхних уровнях, поэтому даже в случае взлома защиты на канальном уровне некоторые шансы еще остаются, особенно если приложение для выполнения транзакции требует ввода PIN-кода вручную с помощью какой-нибудь разновидности клавиатуры.