Тема 8

Комплексный подход к обеспечению безопасности информационных систем

Содержание темы

- Организационно-технические и режимные меры обеспечения безопасности информационных систем.
- Методы и средства защиты информации от удаленных атак через сеть Интернет.
- Вредоносное программное обеспечение.
- Защита информации в распределенных сетях.
- Комплексные системы защиты информации.

Организ.-технич. и режимные меры

Для описания технологии защиты информации конкретной информационной системы обычно строится так называемая **Политика безопасности информационной системы**.

Политика безопасности - совокупность документированных правил, процедур, практических приёмов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Организ.-технич. и режимные меры

Для построения политики безопасности информационной системы рекомендуется отдельно рассматривать **следующие направления** ее **защиты**:

- **защита объектов информационной системы**;
- **защита процессов, процедур и программ обработки информации**;
- **защита каналов связи** (акустические, инфракрасные, проводные, радиоканалы и др.);
- **подавление побочных электромагнитных излучений**;
- **управление системой защиты**.

Организ.-технич. и режимные меры

При этом по каждому из перечисленных выше направлений политика информационной безопасности должна описывать следующие **этапы создания средств защиты информации**:

- **определение информационных и технических ресурсов, подлежащих защите**;
- **выявление полного множества потенциально возможных угроз и каналов утечки информации**;
- **проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки**;

Организ.-технич. и режимные меры

При этом по каждому из перечисленных выше направлений политика информационной безопасности должна описывать следующие **этапы создания средств защиты информации**:

- **определение требований к системе защиты**;
- **осуществление выбора средств защиты информации и их характеристик**;
- **внедрение и организация использования выбранных мер, способов и средств защиты**;
- **осуществление контроля целостности и управление системой защиты**.

Организ.-технич. и режимные меры

Политика информационной безопасности оформляется в виде документированных требований на информационную систему.

Документы обычно разделяют по уровням описания (детализации) процесса защиты:

- **верхнего уровня**;
- **среднего уровня**;
- **нижнего уровня**.

Организ.-технич. и режимные меры

Политика информационной безопасности оформляется в виде документированных требований на информационную систему.

Документы обычно разделяют по уровням описания (детализации) процесса защиты:

- **верхнего уровня**;
- **среднего уровня**;
- **нижнего уровня**.

Организ.-технич. и режимные меры

Документы **верхнего уровня** политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области.

Организ.-технич. и режимные меры

К **среднему уровню** относят документы, касающиеся отдельных аспектов информационной безопасности.

Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации.

Организ.-технич. и режимные меры

В политику информационной безопасности **нижнего уровня** входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

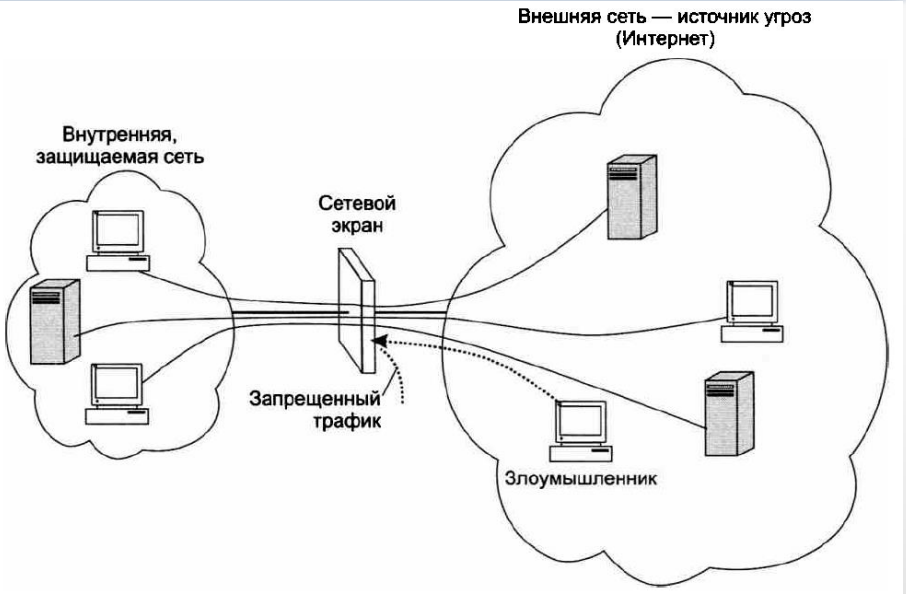
Защита информации от удаленных атак

Через сеть Интернет нарушитель может:

- вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;
- незаконно скопировать важную и ценную для предприятия информацию;
- получить пароли, адреса серверов и их содержимое;
- входить в информационную систему предприятия под логином зарегистрированного пользователя и т. п.

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.

Защита информации от удаленных атак

Компоненты межсетевых экранов:

- Фильтрующие маршрутизаторы.
- Шлюзы сеансового уровня.
- Шлюзы прикладного уровня.

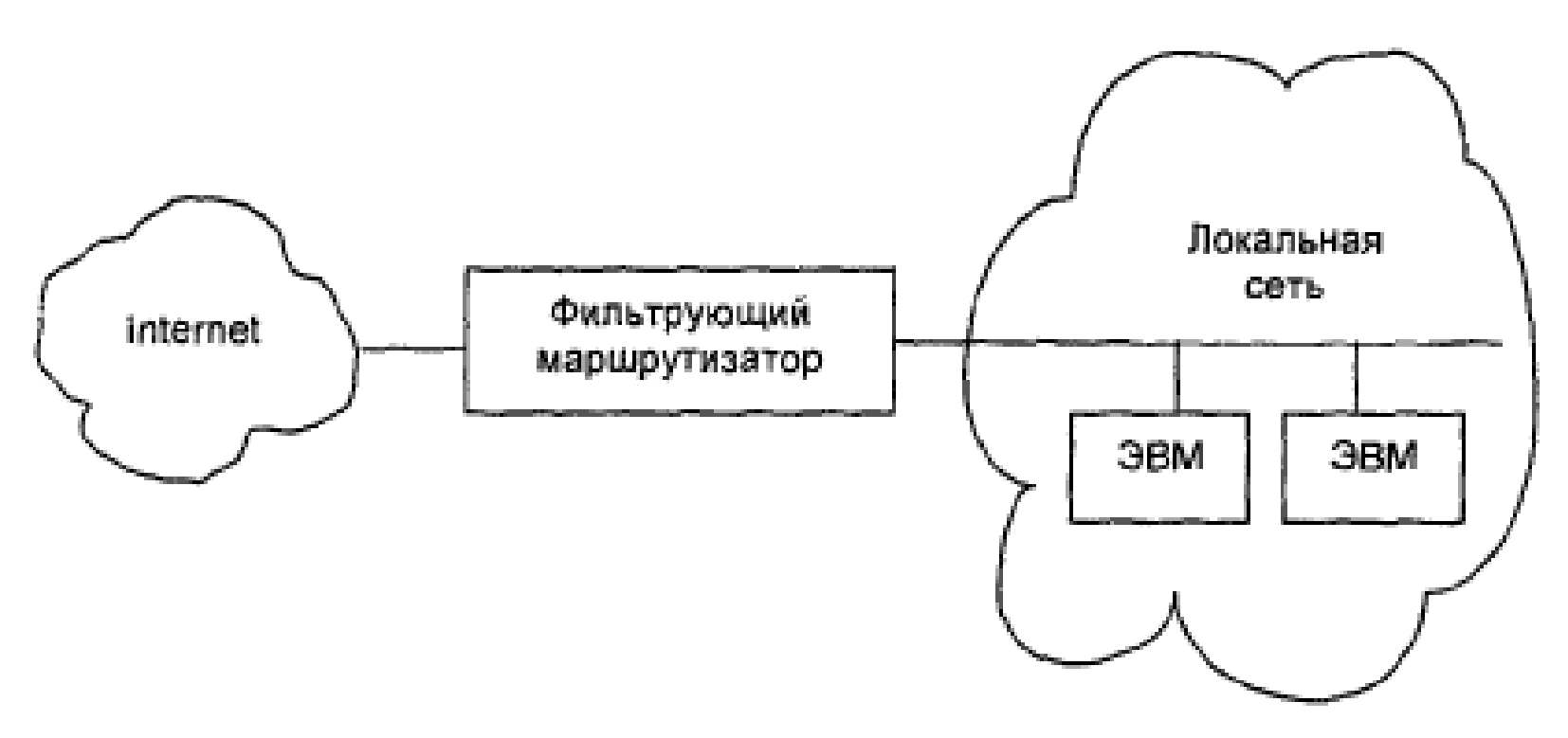
Защита информации от удаленных атак

Фильтрация пакетов.

Брандмауэр с фильтрацией пакетов представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Брандмауэр пропускает или отбраковывает пакеты в соответствии с информацией, содержащейся в IP-заголовках пакетов.

Защита информации от удаленных атак

Фильтрация пакетов.



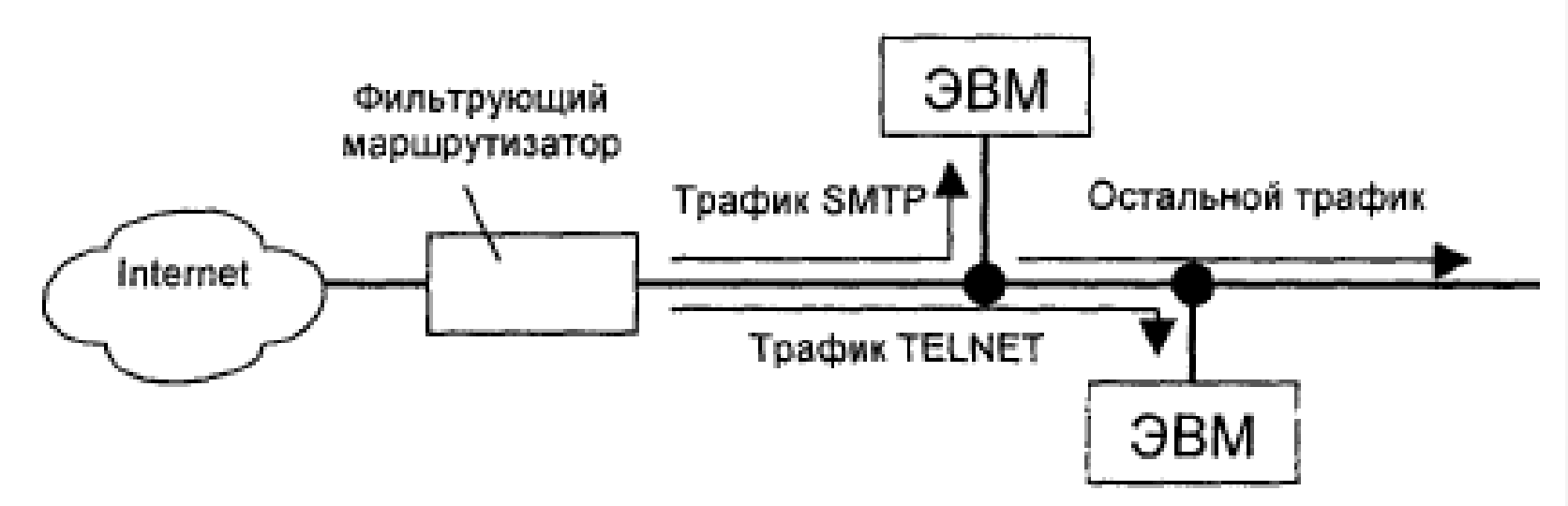
Защита информации от удаленных атак

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы из следующих полей пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- информации о приложении или протоколе;
- TCP/UDP-порт отправителя;
- TCP/UDP-порт получателя.

Защита информации от удаленных атак

Схема фильтрации трафика SMTP и TELNET



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.

Защита информации от удаленных атак

Шлюз сеансового уровня следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым.

При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем брандмауэр с фильтрацией пакетов.

Защита информации от удаленных атак

Последовательность процедур квитирования связи по протоколу TCP

Защита информации от удаленных атак

Шлюз прикладного уровня, как и шлюз сеансового уровня, перехватывает входящие и исходящие пакеты, использует программы-посредники, копирующие и перенаправляющие информацию через шлюз, а также функционирует в качестве сервера-посредника, исключая прямые соединения между доверенным сервером или клиентом и внешним хостом.

Защита информации от удаленных атак

Прикладные шлюзы имеют серьезные преимущества перед обычным режимом, при котором прикладной трафик пропускается напрямую к внутренним хостам.

Они включают в себя:

- **скрытие информации,** при котором имена внутренних систем необязательно будут известны внешним системам с помощью DNS, так как прикладной шлюз может быть единственным хостом, чье имя должно быть известно внешним системам;

Защита информации от удаленных атак

- **надежную аутентификацию и протоколирование**, при котором прикладной трафик может быть предварительно аутентифицирован до того, как он достигнет внутренних хостов, и может быть запротоколирован более эффективно, чем стандартные средства протоколирования хоста;
- **оптимальное соотношение между ценой и эффективностью**, поскольку дополнительные программы или оборудование для аутентификации или протоколирования нужно устанавливать только на прикладном шлюзе;

Защита информации от удаленных атак

- **простые правила фильтрации,** так как правила на маршрутизаторе с фильтрацией пакетов будут менее сложными, чем они были бы, если бы маршрутизатор сам фильтровал прикладной трафик и отправлял его большому числу внутренних систем.
- Маршрутизатор должен только пропускать прикладной трафик к прикладному шлюзу и блокировать весь остальной трафик.

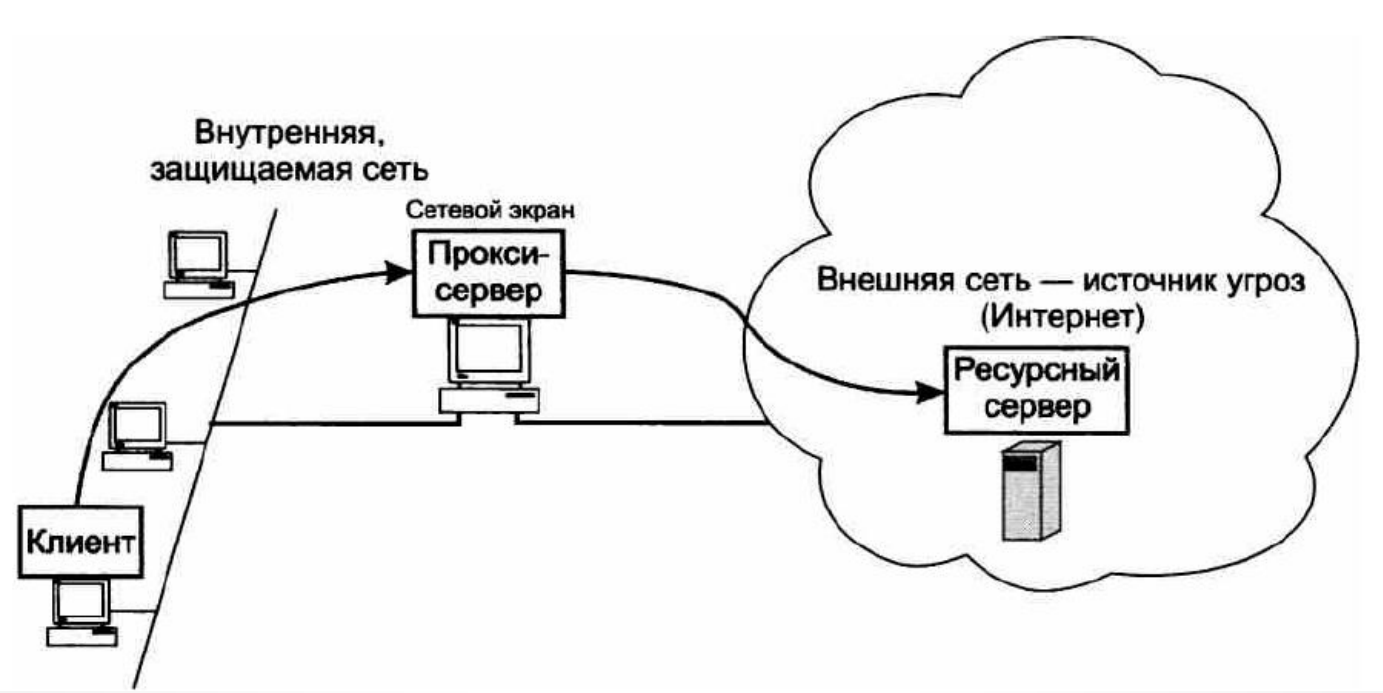
Прокси-серверы

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.

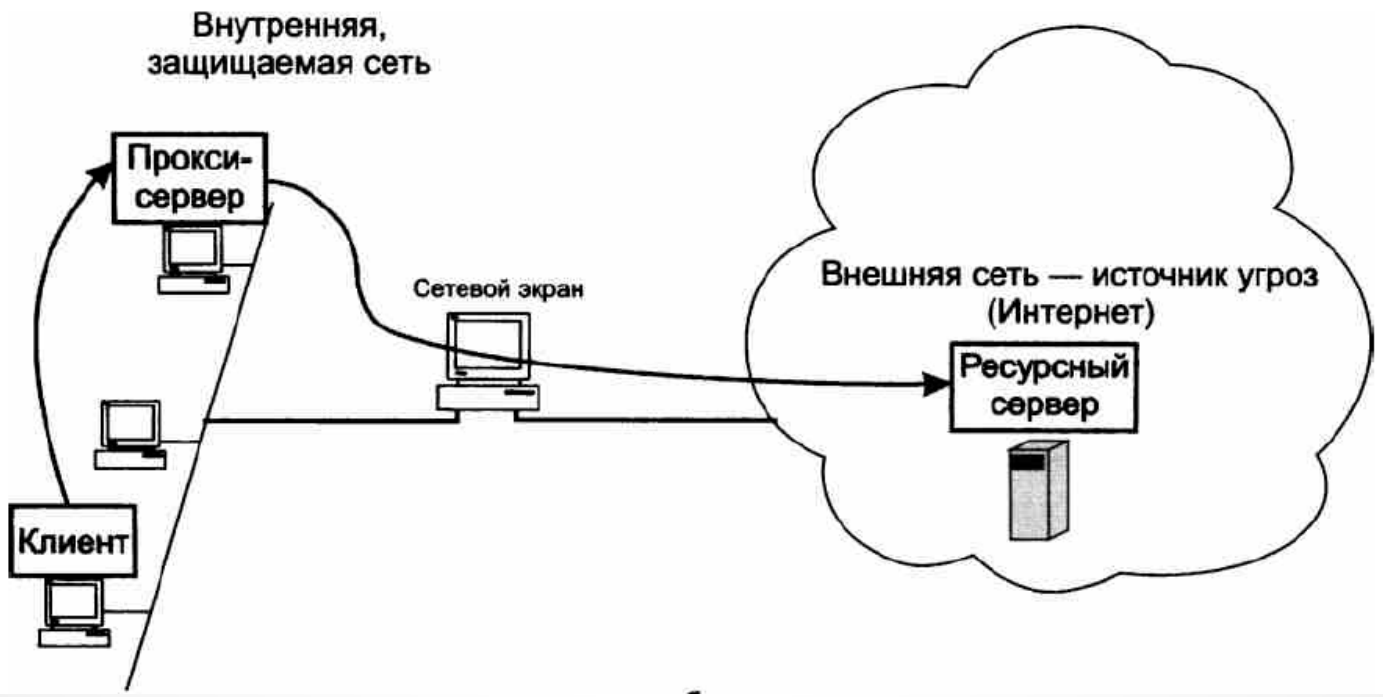
Прокси-серверы

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:

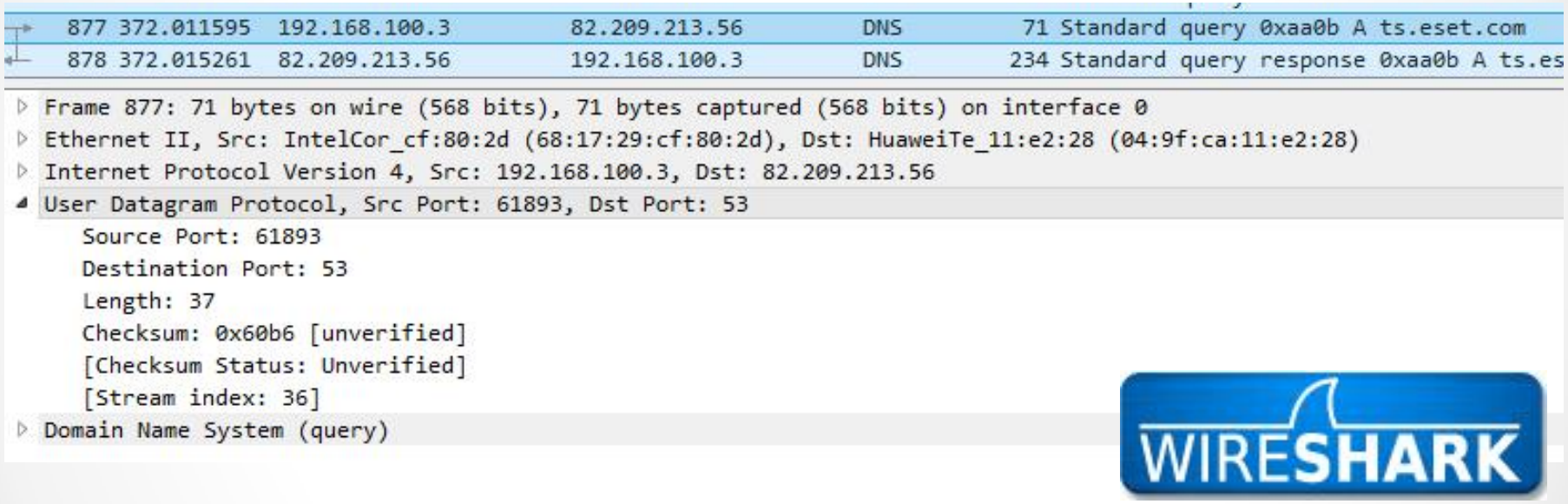
- **анализаторы протоколов** (**сетевые сниферы**) – захватывают трафик локальных сетей и представляют его администратору для анализа;
- **маршрутизаторы**, поддерживающие **протокол NetFlow**, собирают обобщенные данные о трафике глобальных сетей и передают его NetFlow, для поиска атак и угроз;
- **системы 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.

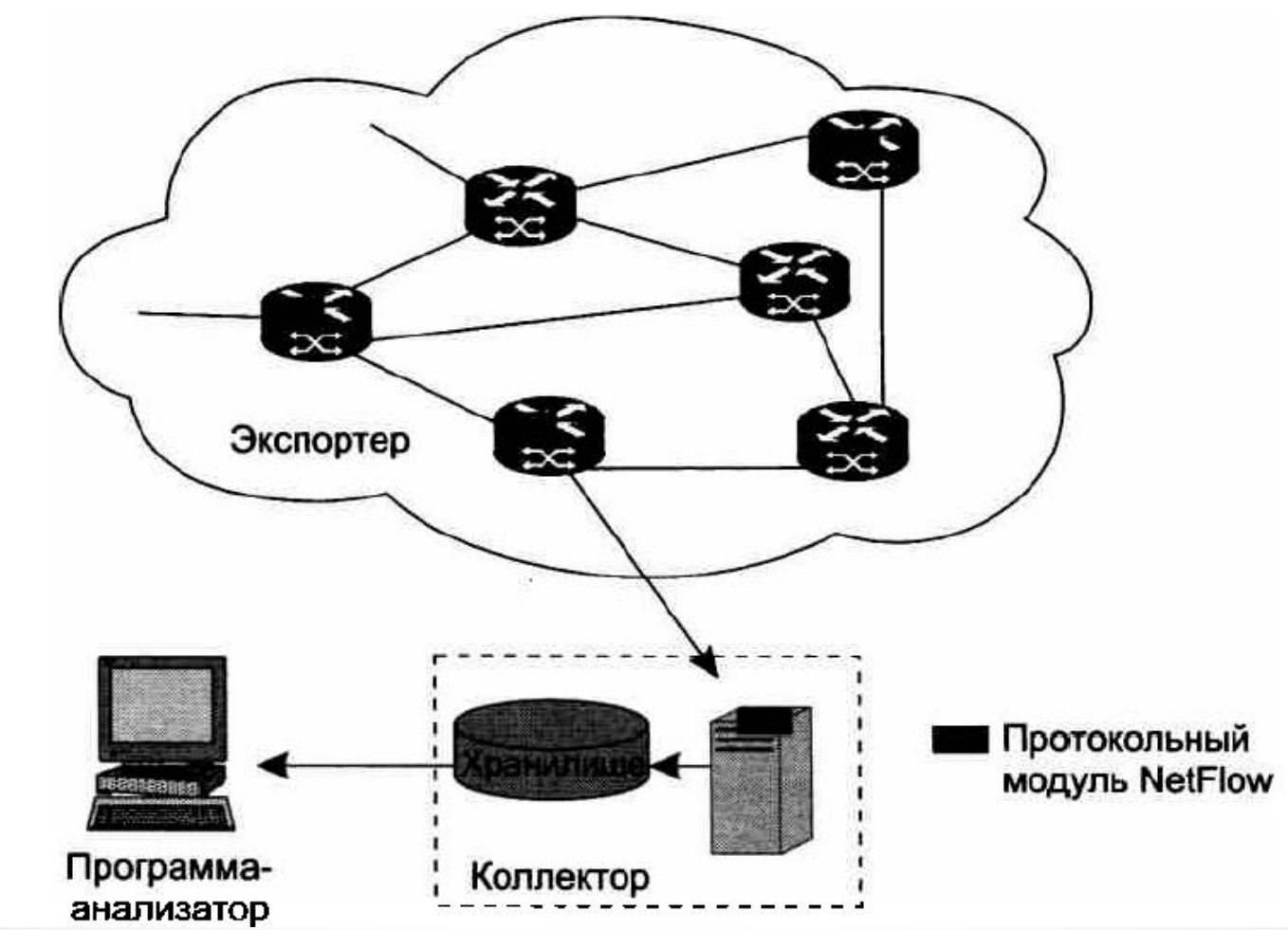
Поддерживающие протокол NetFlow сетевые узлы не только выполняют свою основную работу – передачу пакетов в соответствии с адресом назначения, но и собирают статистику о проходящих через них потоках данных и периодически отправляют их в **коллекторы** для хранения и обработки такой информации.

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.

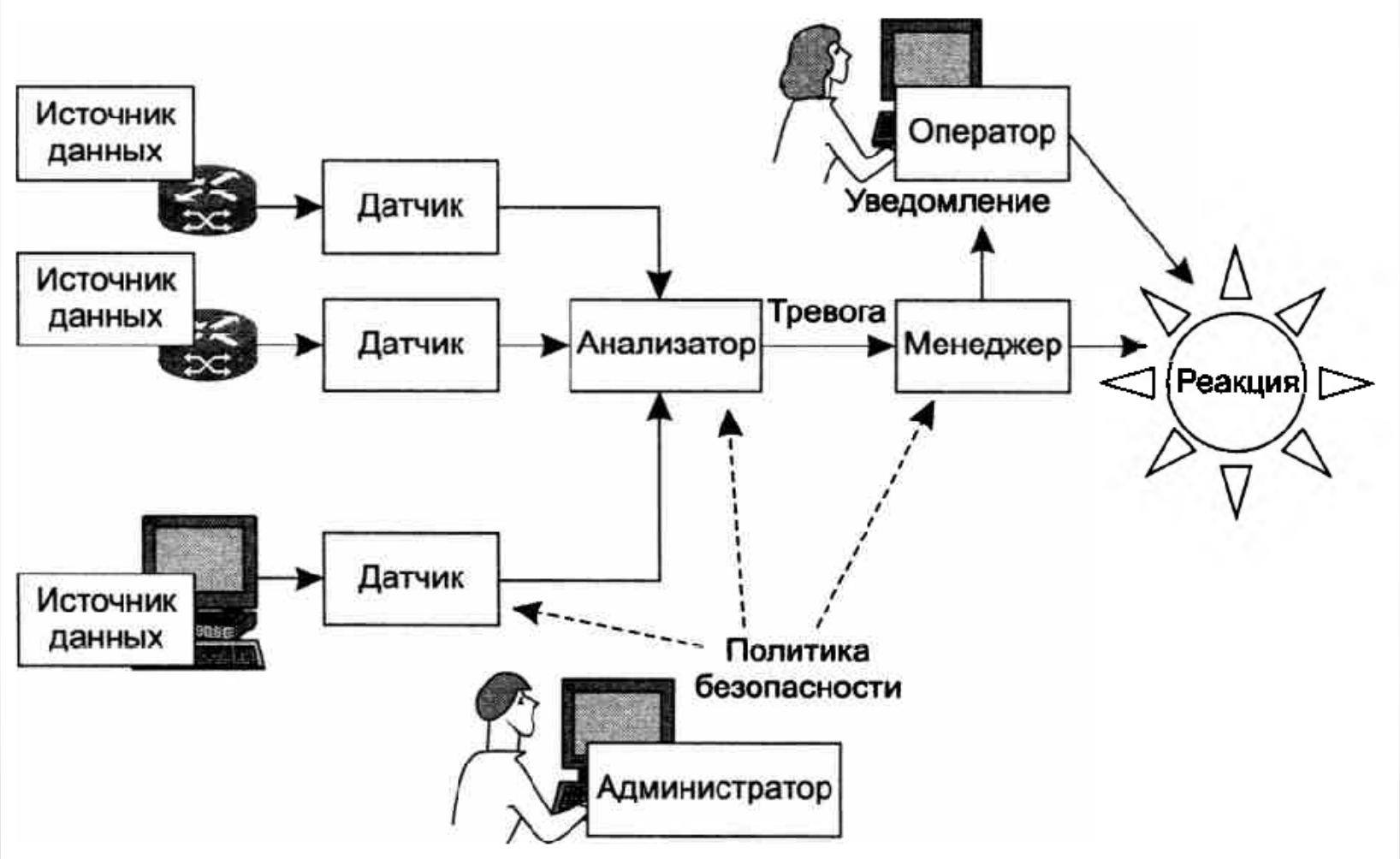
В отличие от файерволов и прокси-серверов, которые строят защиту сети исключительно на основе анализа сетевого трафика, системы обнаружения вторжений учитывают в своей работе различные подозрительные **события**, происходящие в системе.

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.**

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:

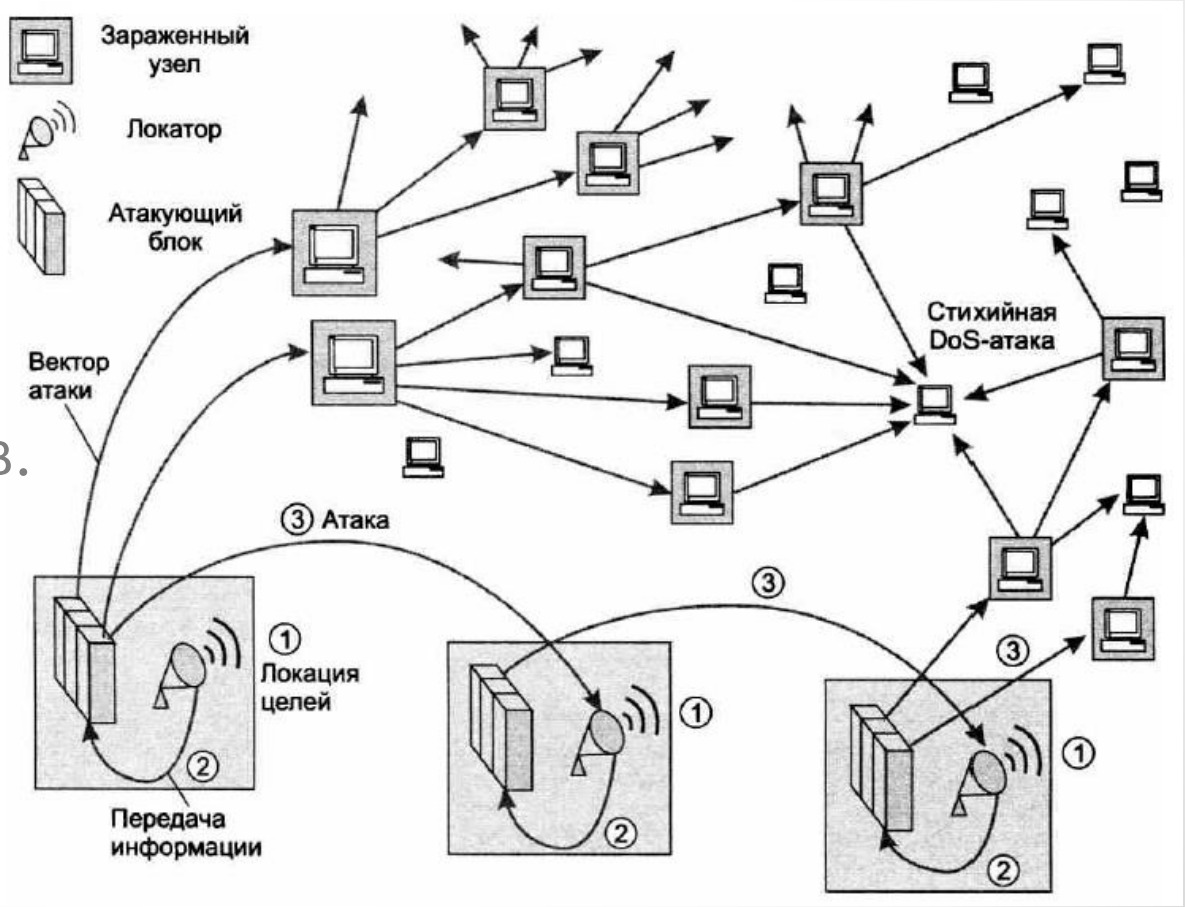
- **атакующий блок** состоит из нескольких модулей (векторов атаки), каждый из которых рассчитан на поражение конкретного типа уязвимости. Этот блок открывает «входную дверь» атакуемого хоста и передает через нее свою копию;
- **блок поиска целей** (**локатор**) собирает информацию об узлах сети, а затем 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.



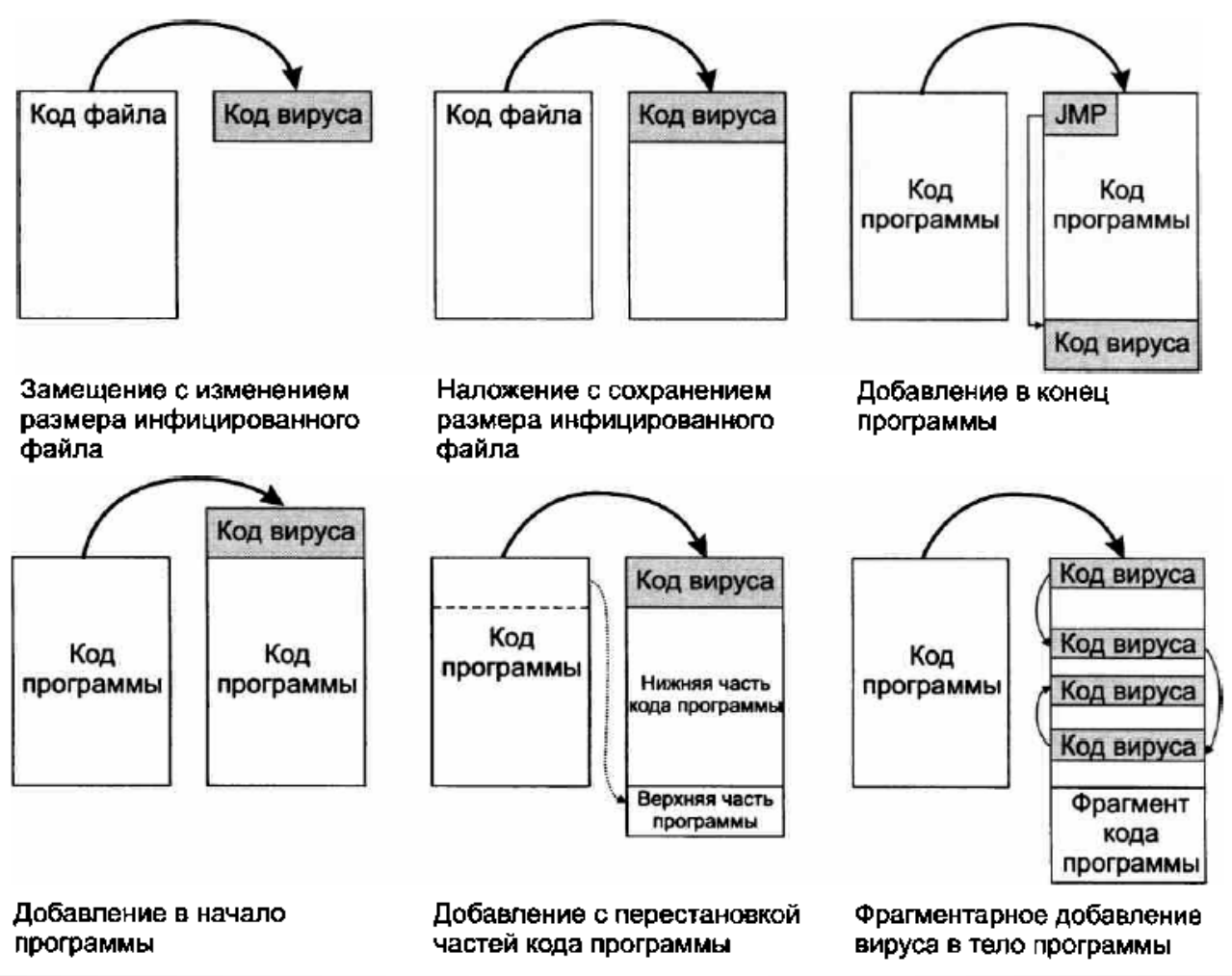
Вредоносное программное обеспечение

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.

Концепция ИБ РБ

Постановление

Совета Безопасности Республики Беларусь

18 марта 2019 г. № 1 г.Минск

О Концепции информационной безопасности Республики Беларусь

Совет Безопасности Республики Беларусь п о с т а н о в л я е т:

1. Утвердить Концепцию информационной безопасности Республики Беларусь (прилагается).

2. Государственным органам и иным организациям в практической деятельности руководствоваться положениями Концепции информационной безопасности Республики Беларусь.

3. Государственному секретарю Совета Безопасности Республики Беларусь отражать результаты реализации Концепции информационной безопасности Республики Беларусь в ежегодном докладе Президенту Республики Беларусь о состоянии национальной безопасности и мерах по ее укреплению.

Президент
Республики Беларусь А.Лукашенко

21

Концепция ИБ РБ

ГЛАВА 1
МИРОВОЕ ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ

Индустрия телекоммуникации стала одной из наиболее динамичных и перспективных сфер мировой экономики. С процессами информатизации все больше связываются национальные экономические интересы и перспективы инвестиций.

Концепция ИБ РБ

ГЛАВА 10
ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

40. Механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки. Через информационное пространство осуществляется преднамеренная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей в экстремистскую и террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала. Информационный фактор играет все более значительную роль в межгосударственных конфликтах и неявных действиях, направленных на нарушение суверенитета, территориальной целостности стран и снижение темпов их развития. В результате информационных воздействий существенно меняются социальные связи человека в обществе, стиль мышления, способы общения, восприятие действительности и самооценка.

Концепция ИБ РБ

ГЛАВА 10
ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к фейковым сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

Концепция ИБ РБ

ГЛАВА 15
ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.

Во многих национальных вооруженных силах создаются и развиваются кибервойска, а проведение кибероперацій предусматривается в доктринальных и стратегических документах. Одновременно рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий.

Концепция ИБ РБ

ГЛАВА 15
ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

60. Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Выработка правовых, процедурных, технических и организационных мер против кибервоздействий на информационные ресурсы отстает от формирования реальных и потенциальных угроз их осуществления.