Тема 7

Информационная безопасность
при работе в сети Интернет

Содержание темы

- Обзор инцидентов в сфере информационной безопасности.
- Методы и средства защиты информации от удаленных атак.
- Компьютерные вирусы и механизмы борьбы с ними.
- Безопасность в социальных сетях.
- Рекомендации по защите персонального компьютера при работе в сети Интернет.

Kaspersky Security Bulletin 2016

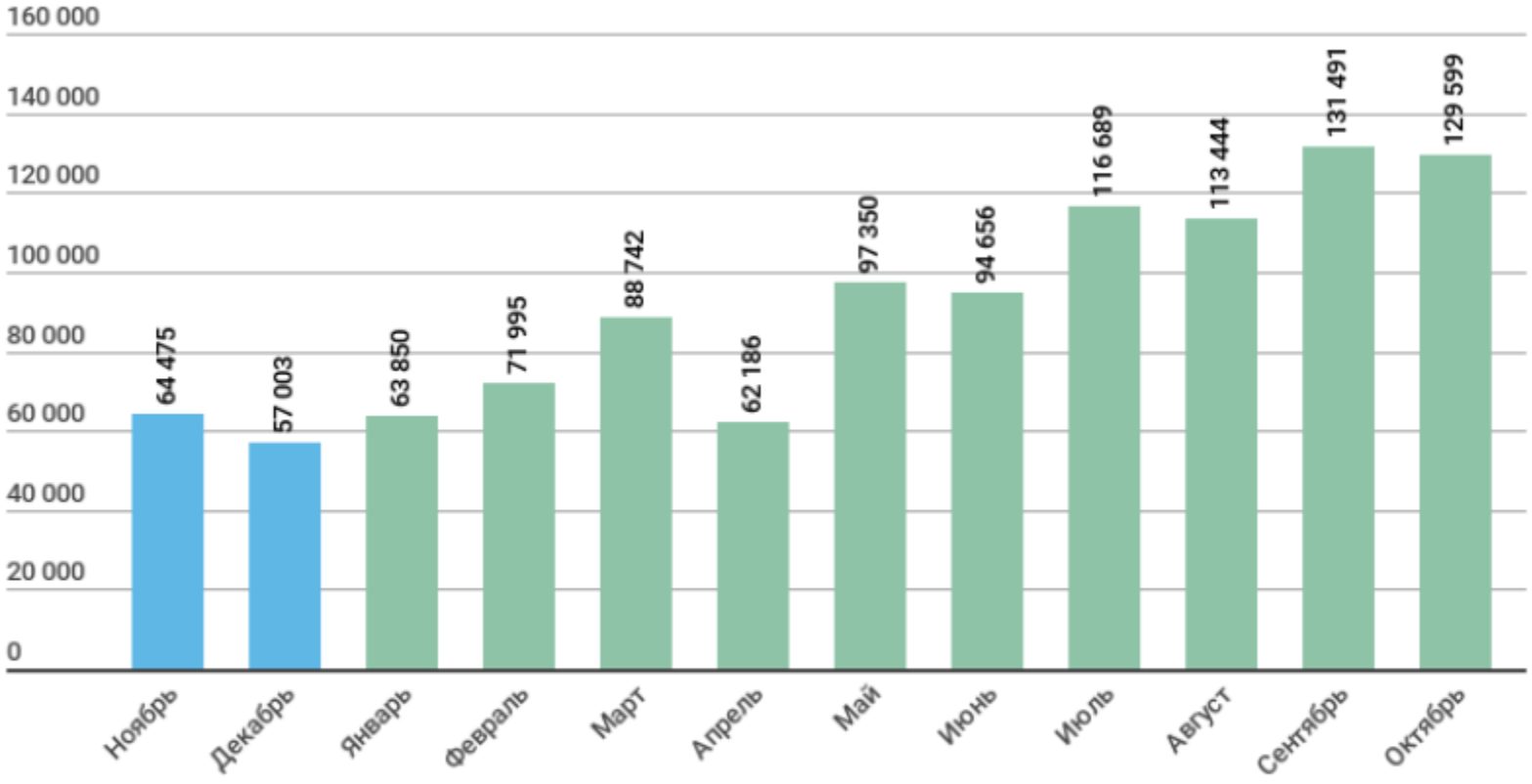
Kaspersky Security Bulletin 2017

Kaspersky Security Bulletin 2018

ЦИФРЫ ГОДА

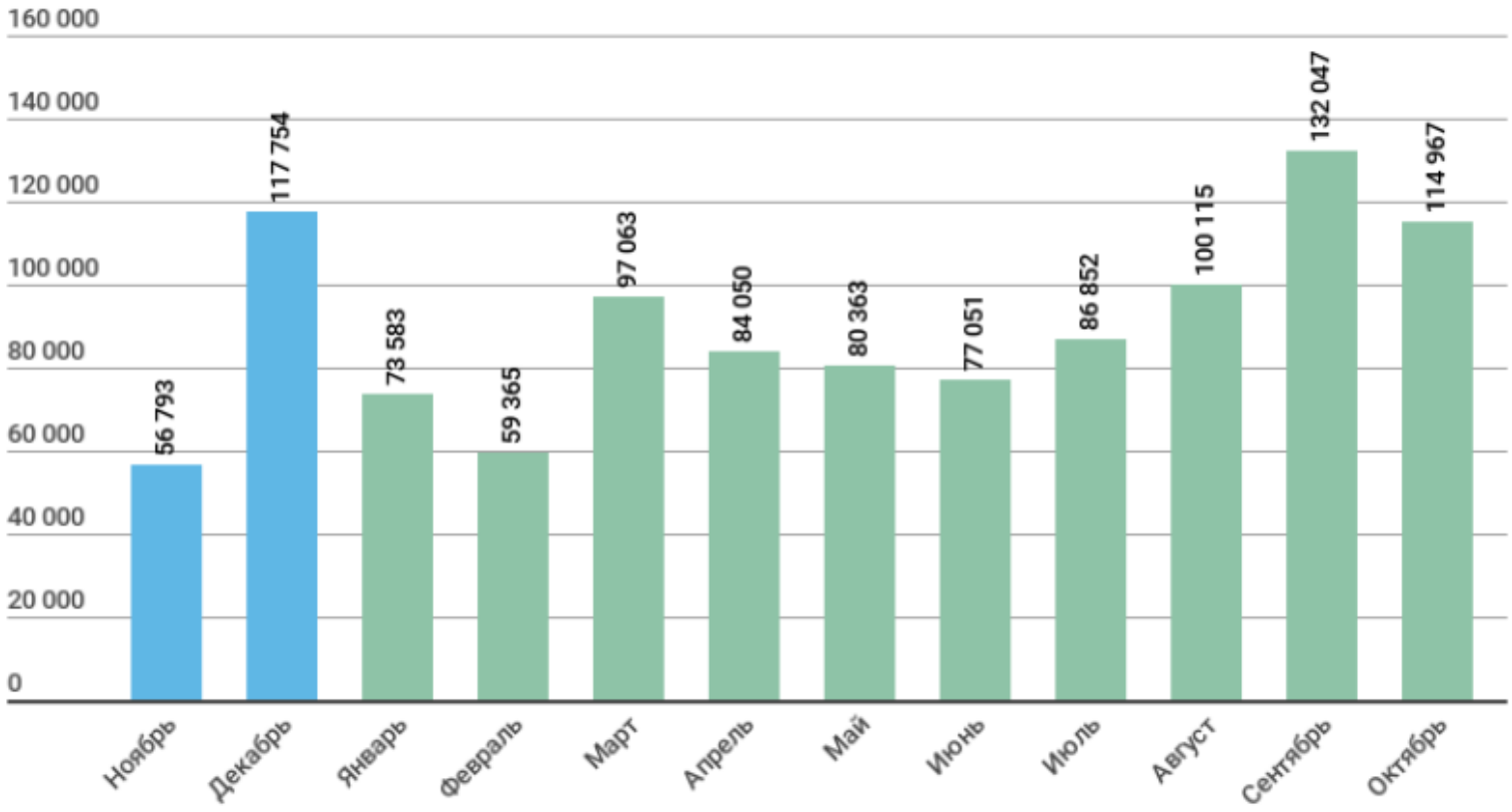
- В течение года 30,01% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.
- Решения «Лаборатории Касперского» отразили **1 876 998 691** атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Зафиксирован **554 159 621** уникальный URL, на которых происходило срабатывание веб-антивируса.
- Нашим веб-антивирусом зафиксировано **21 643 946** уникальных вредоносных объектов.
- Атаки шифровальщиков отражены на компьютерах **765 538** уникальных пользователей.
- За отчетный период майнерами были атакованы **5 638 828** уникальных пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **830 135** пользователей.

Kaspersky Security Bulletin 2018



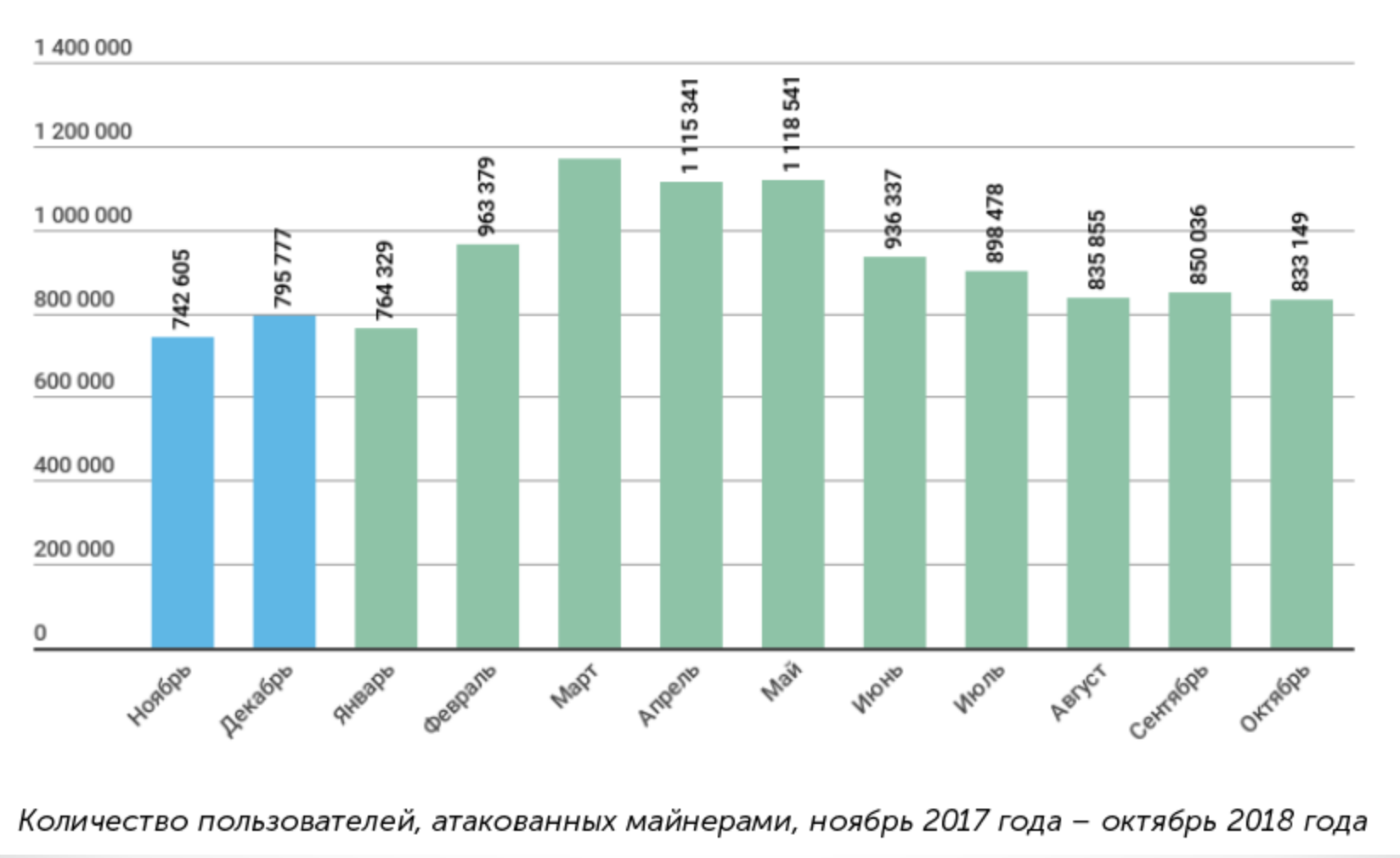
Количество пользователей, атакованных банковским вредоносным ПО, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



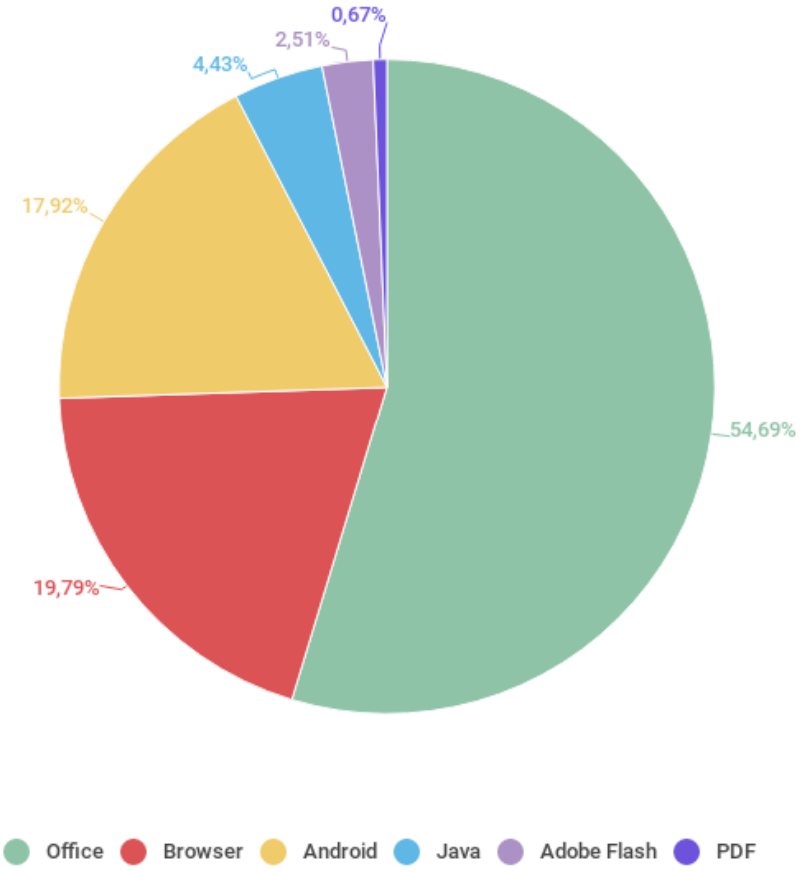
Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



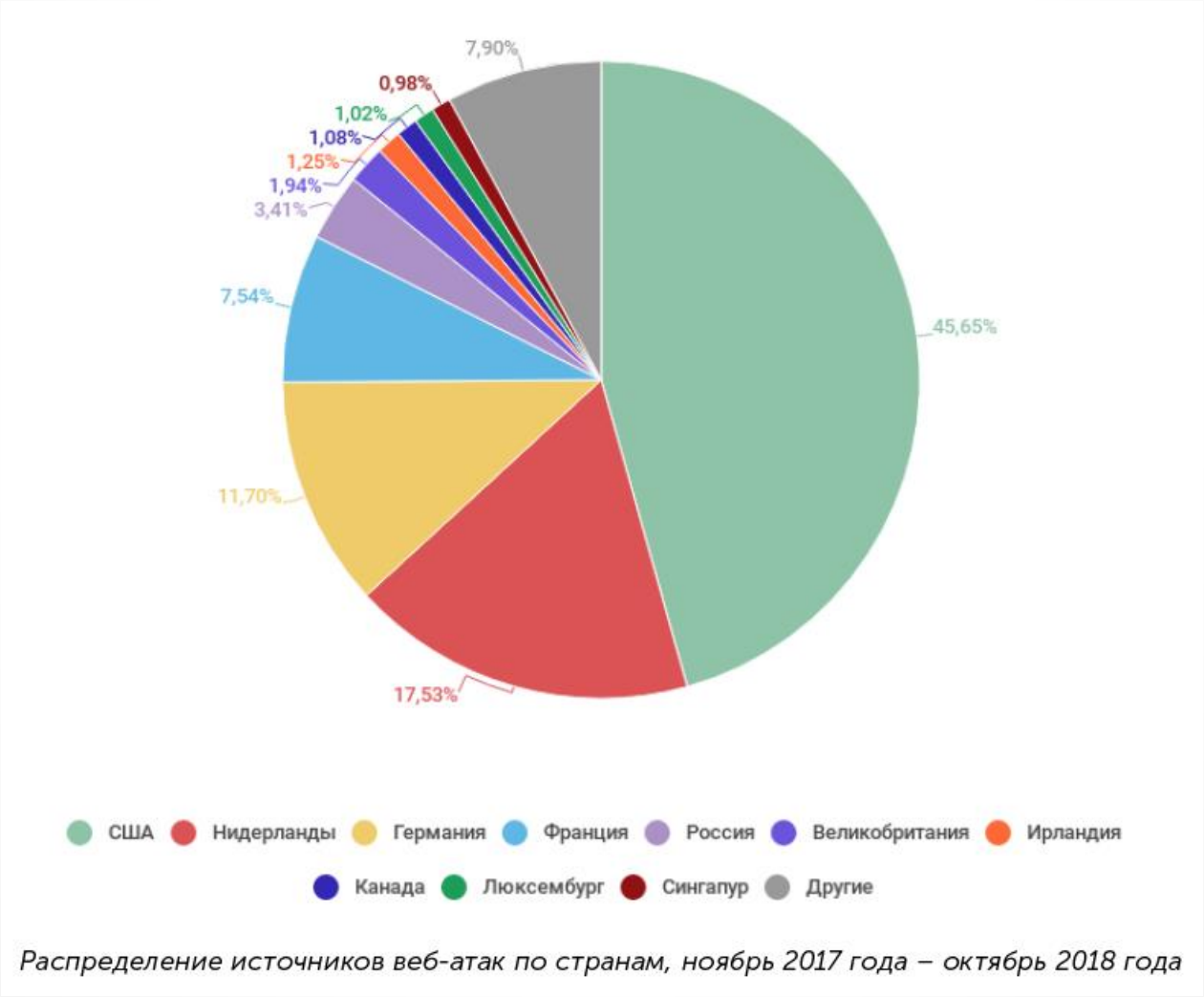
Количество пользователей, атакованных майнерами, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



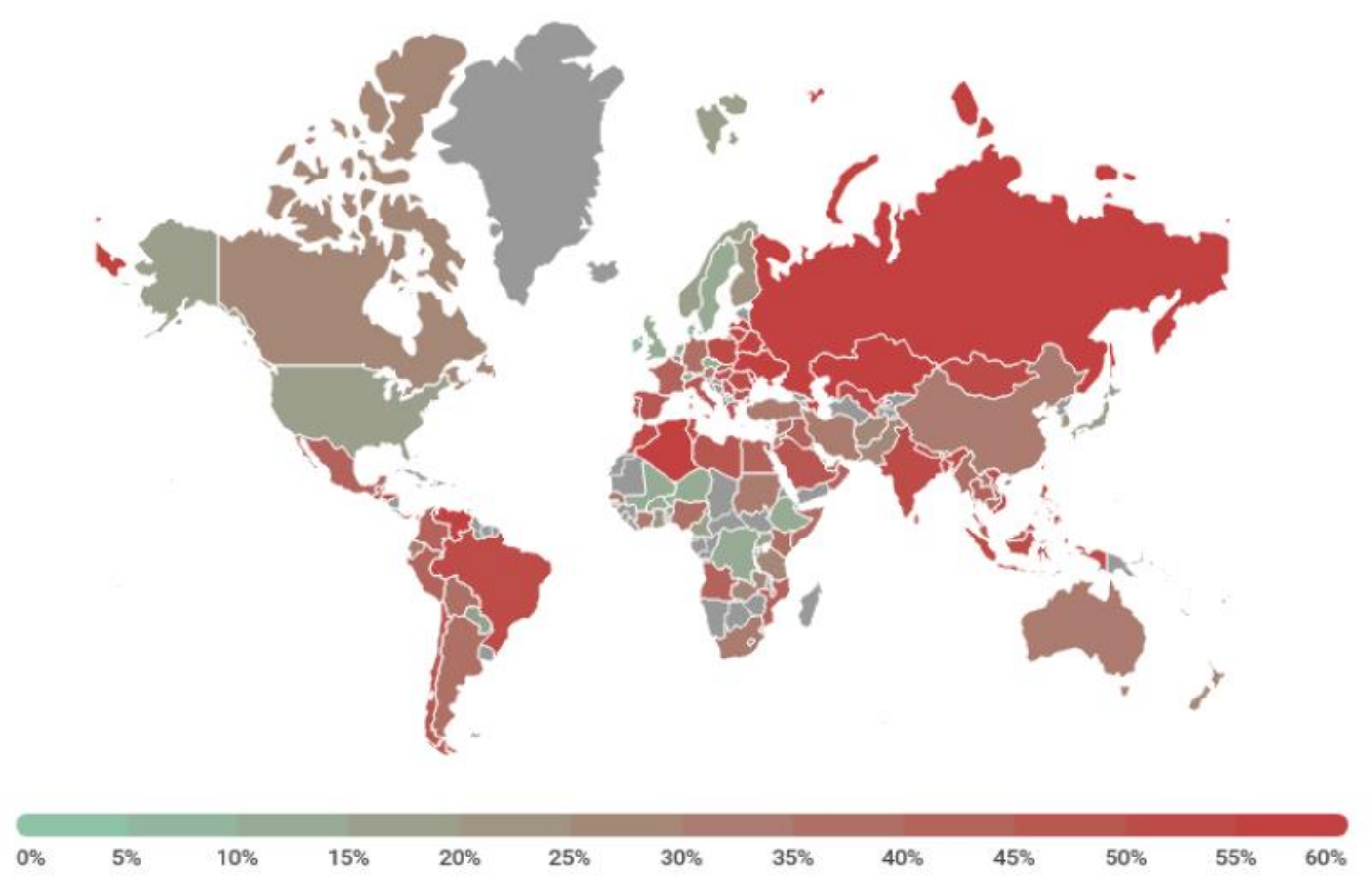
Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



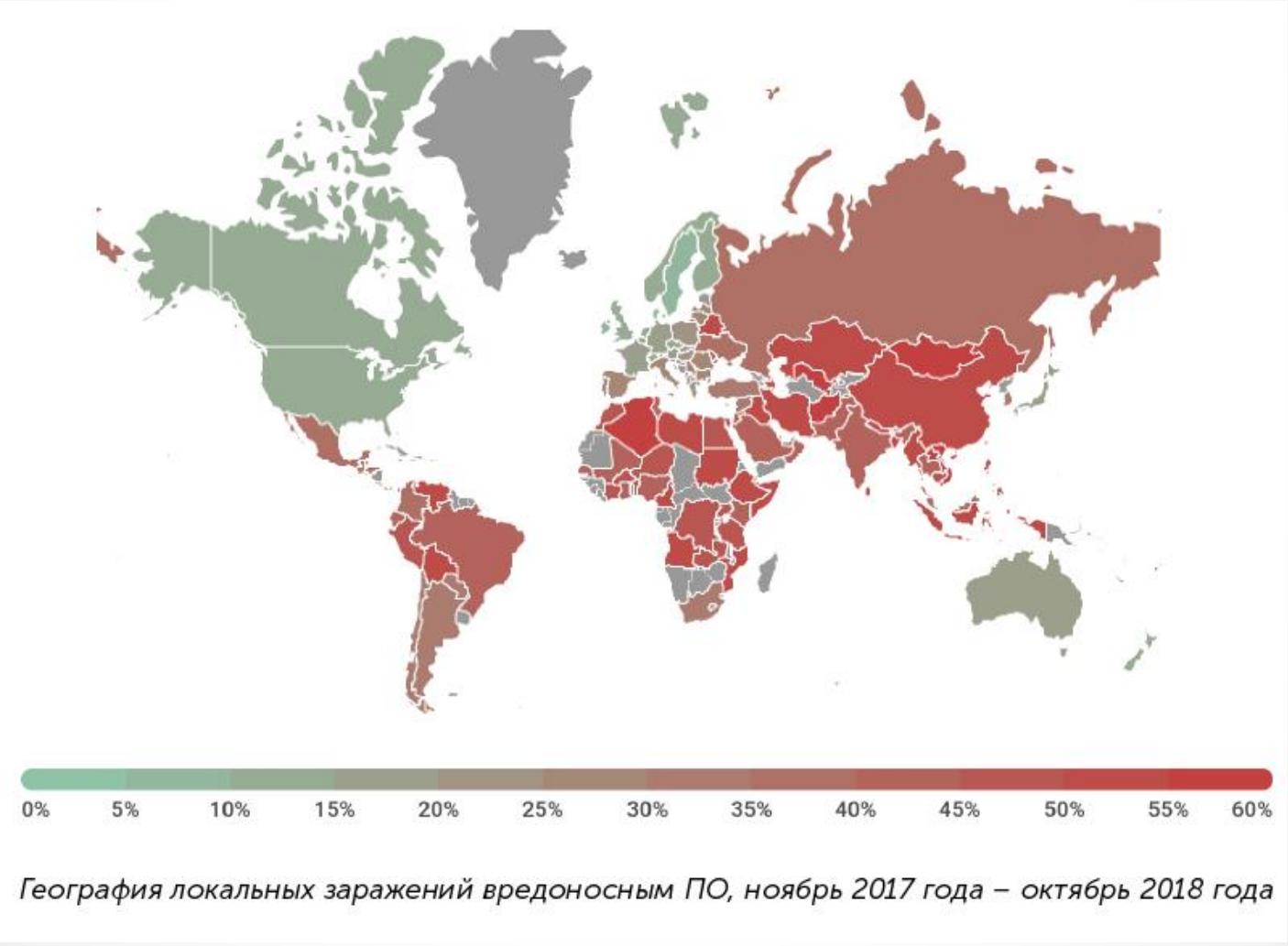
Распределение источников веб-атак по странам, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



География веб-атак вредоносного ПО, ноябрь 2017 года – октябрь 2018 года

Kaspersky Security Bulletin 2018



География локальных заражений вредоносным ПО, ноябрь 2017 года – октябрь 2018 года

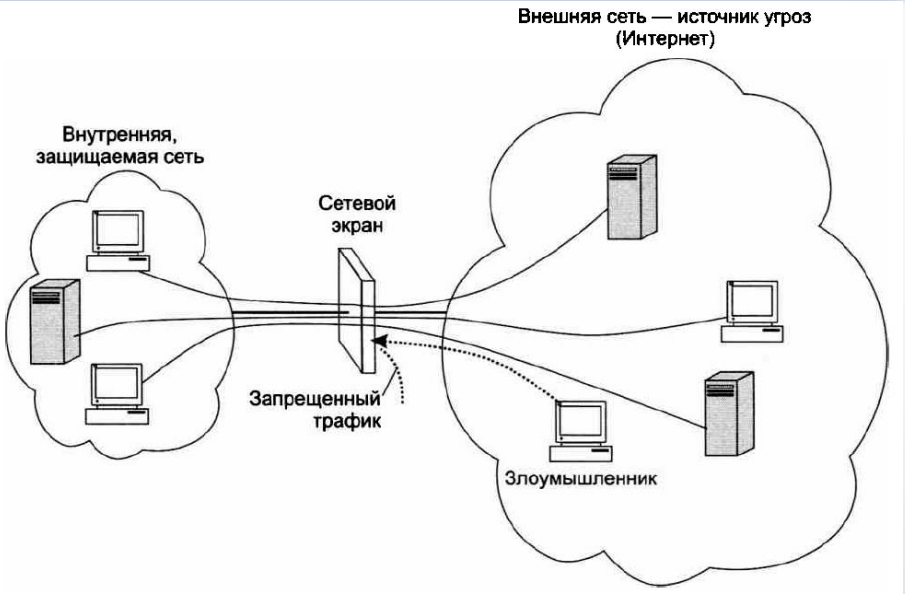
Защита информации от удаленных атак

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.

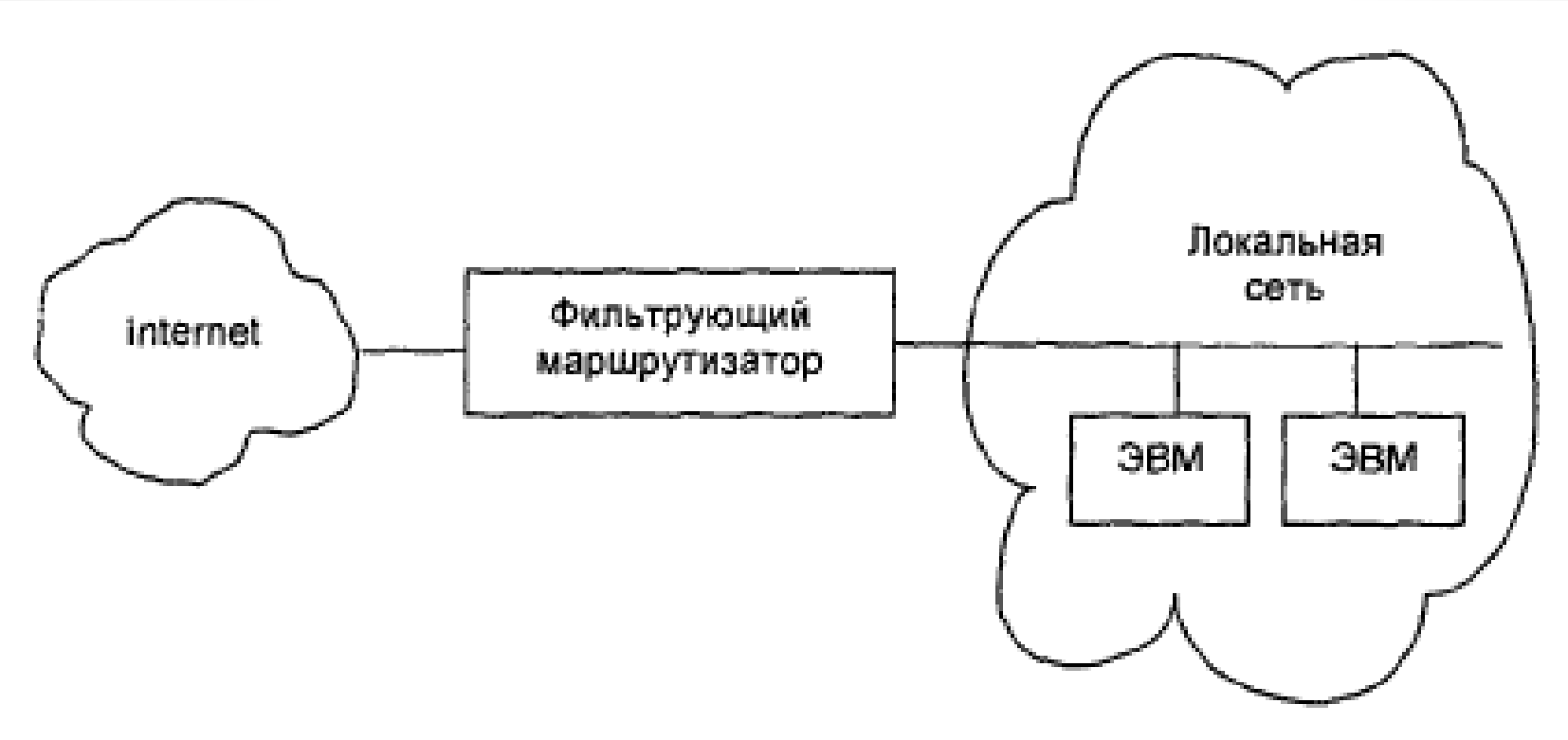
Защита информации от удаленных атак

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.



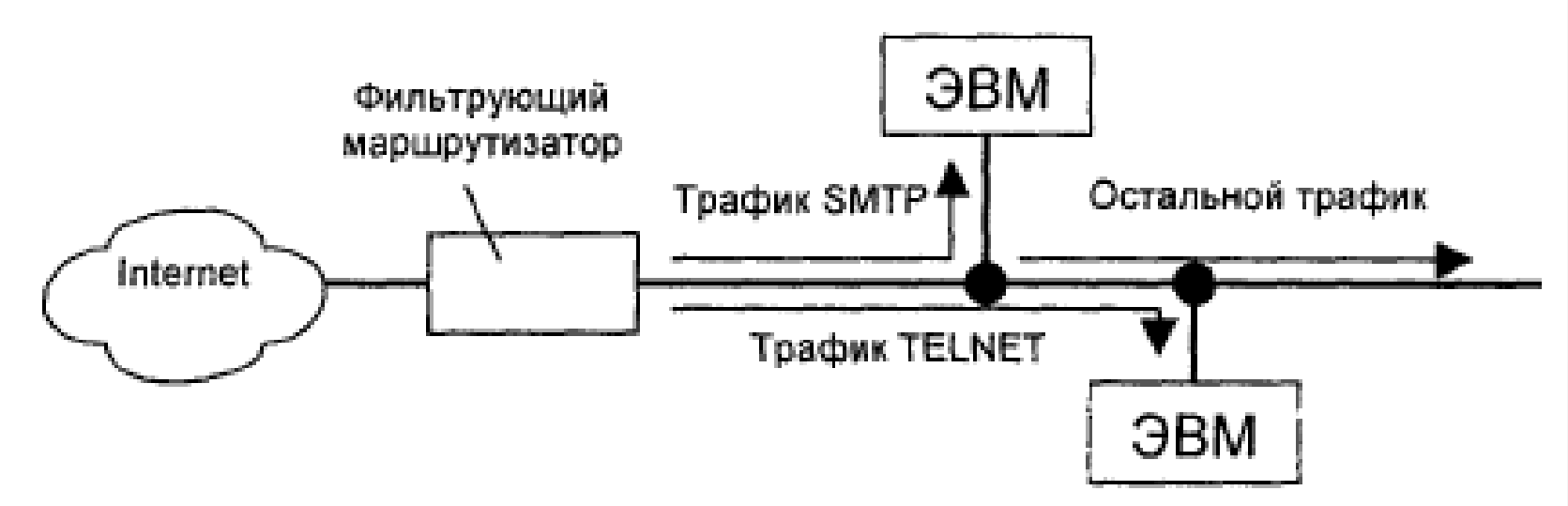
Защита информации от удаленных атак

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

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

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.

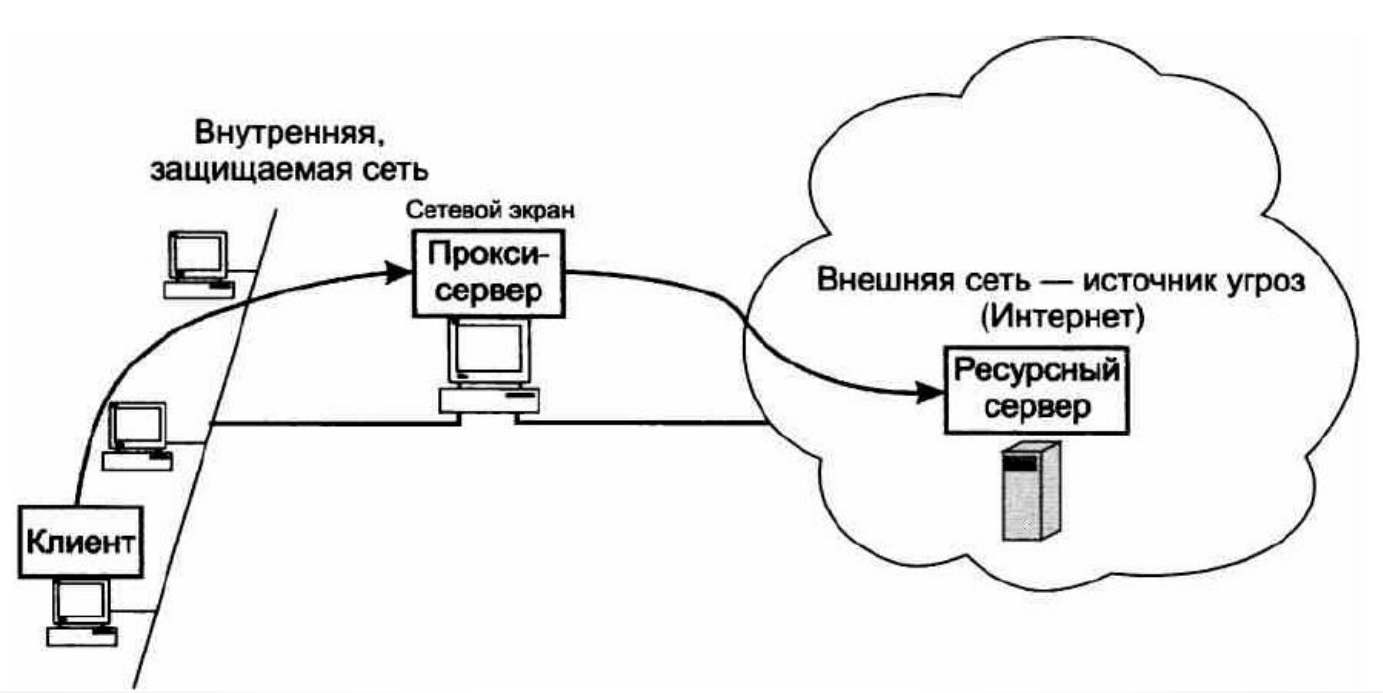
Прокси-серверы

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.

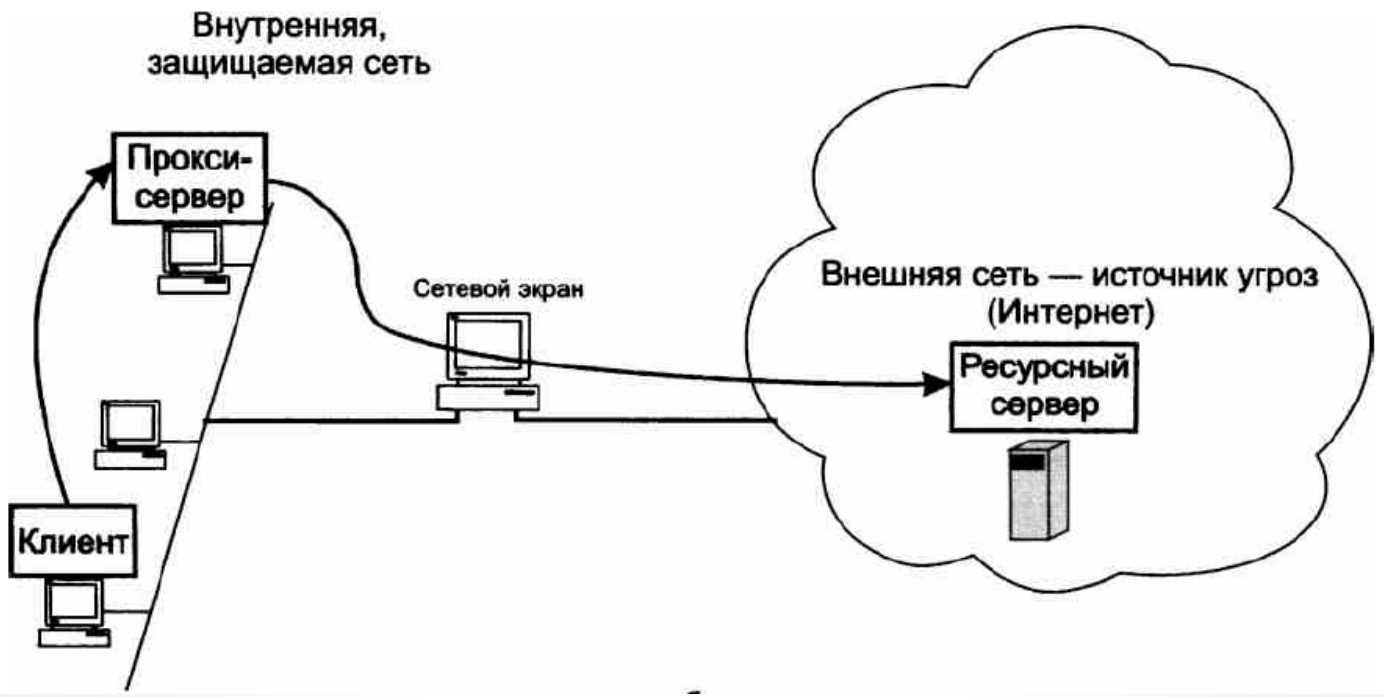
Прокси-серверы

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.

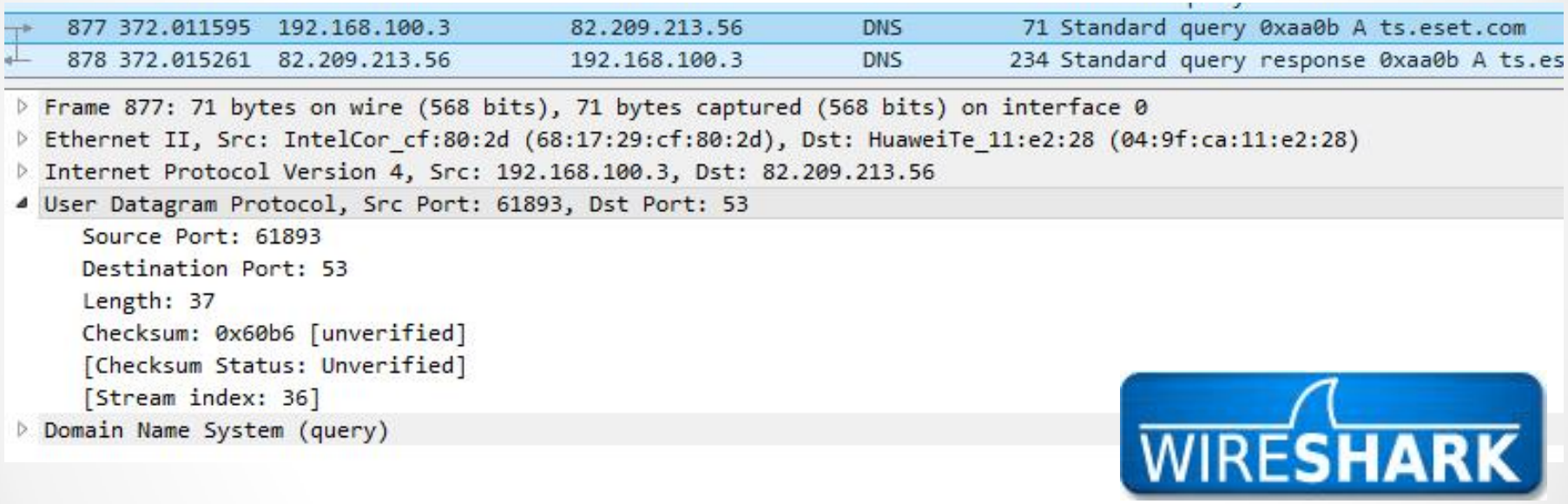


Системы и средства мониторинга трафика

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



Системы и средства мониторинга трафика

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

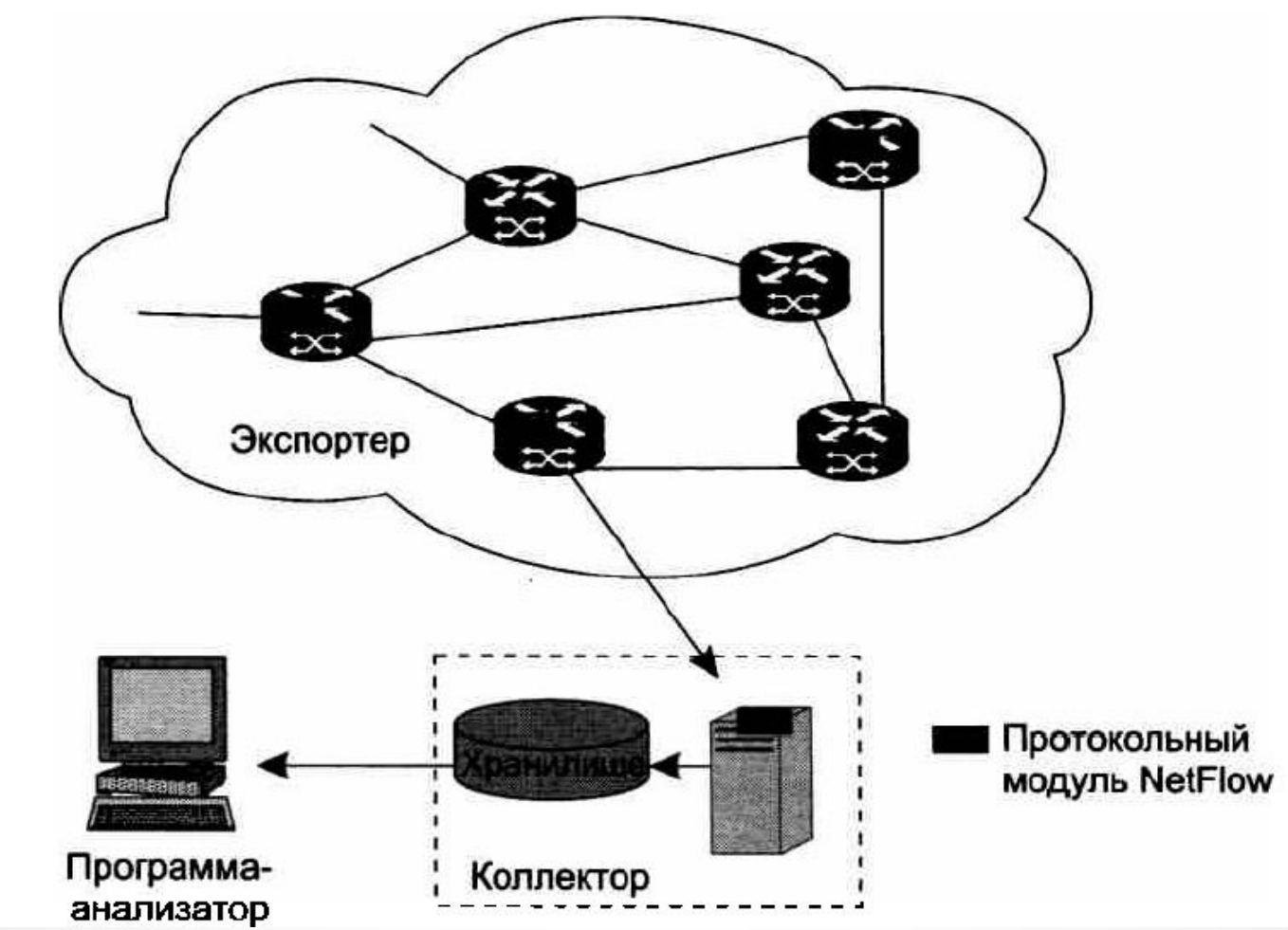
Поддерживающие протокол NetFlow сетевые узлы не только выполняют свою основную работу – передачу пакетов в соответствии с адресом назначения, но и собирают статистику о проходящих через них потоках данных и периодически отправляют их в **коллекторы** для хранения и обработки такой информации.

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 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.

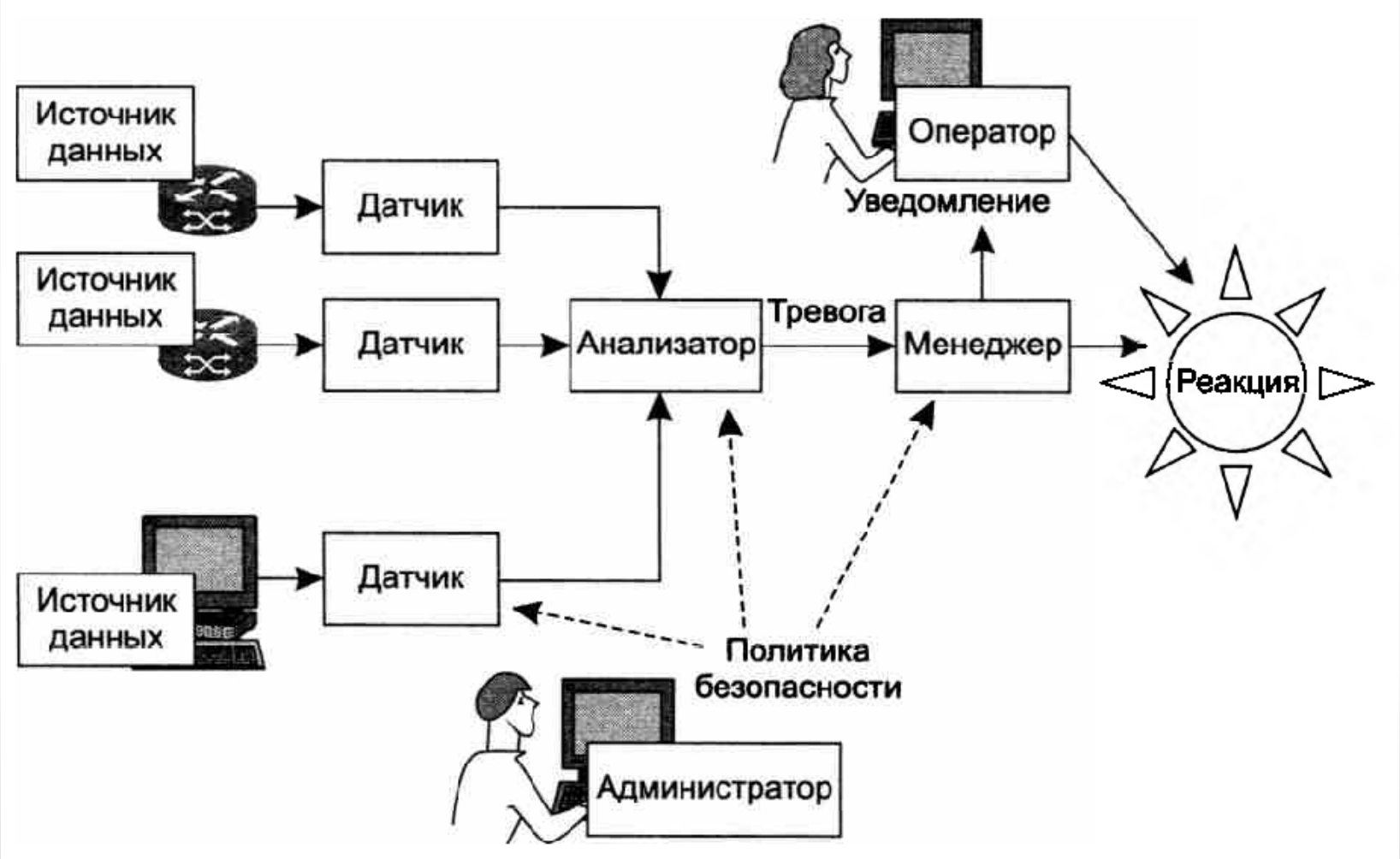
В отличие от файерволов и прокси-серверов, которые строят защиту сети исключительно на основе анализа сетевого трафика, системы обнаружения вторжений учитывают в своей работе различные подозрительные **события**, происходящие в системе.

Системы обнаружения вторжений

Типовая система IDS включает следующие функциональные элементы:

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

Системы обнаружения вторжений



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:

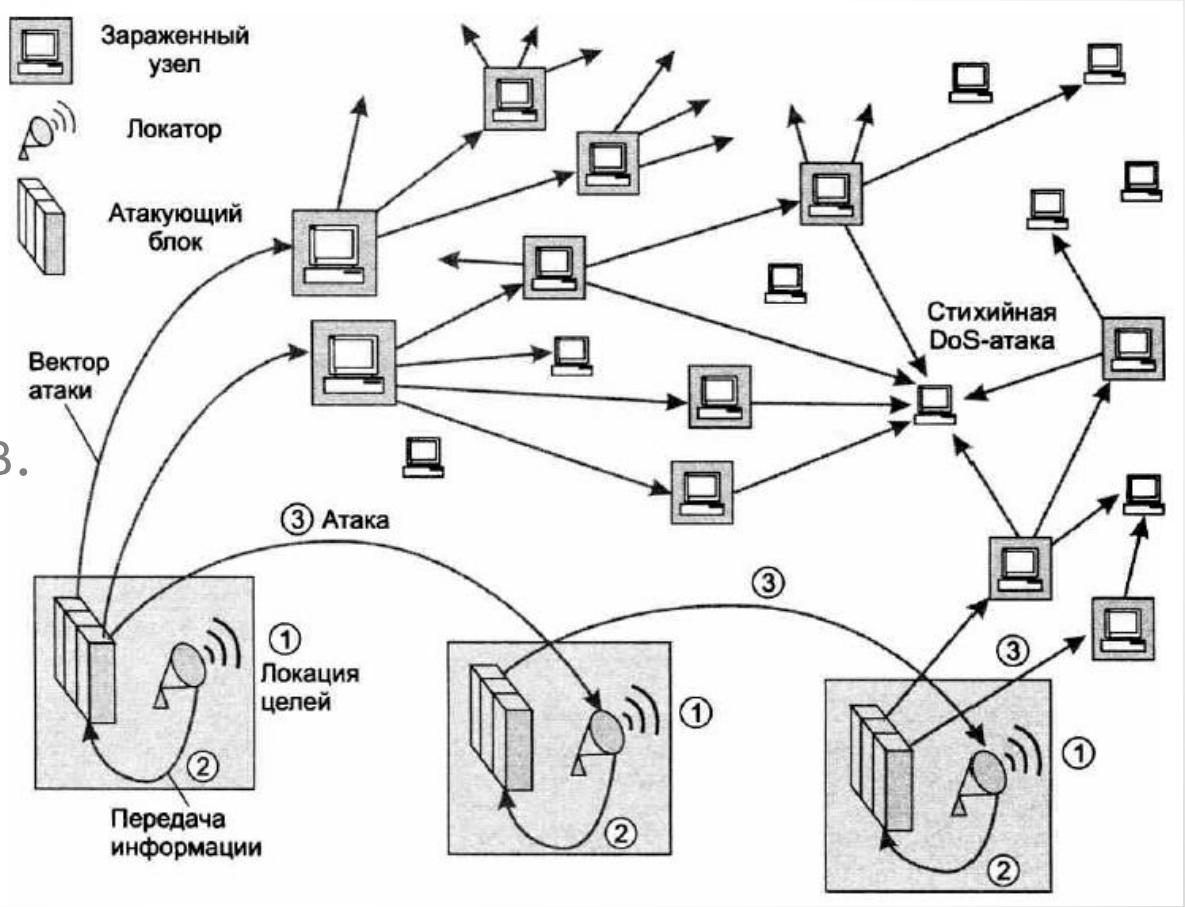
- **атакующий блок** состоит из нескольких модулей (векторов атаки), каждый из которых рассчитан на поражение конкретного типа уязвимости. Этот блок открывает «входную дверь» атакуемого хоста и передает через нее свою копию;
- **блок поиска целей** (**локатор**) собирает информацию об узлах сети, а затем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



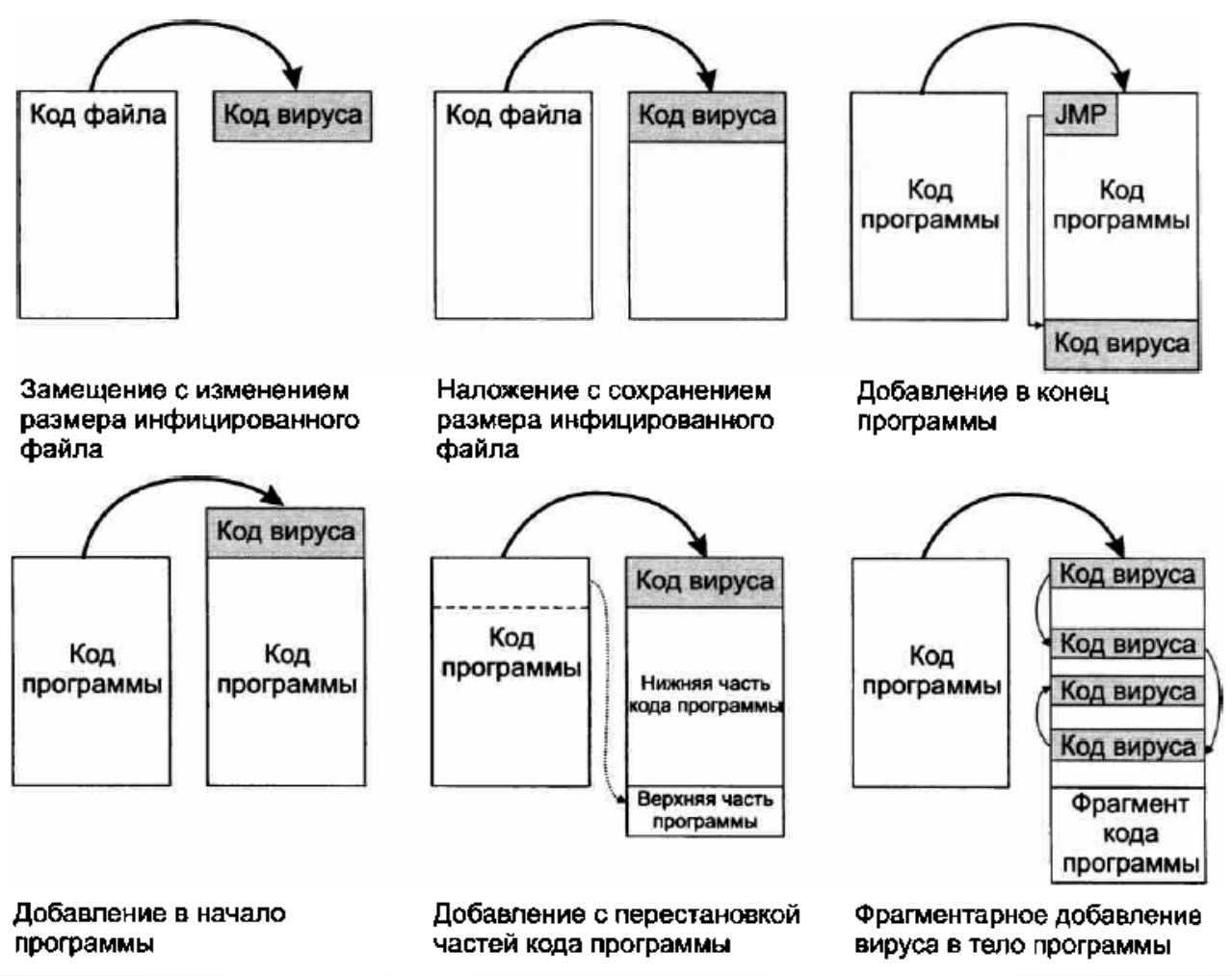
Вредоносное программное обеспечение

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.

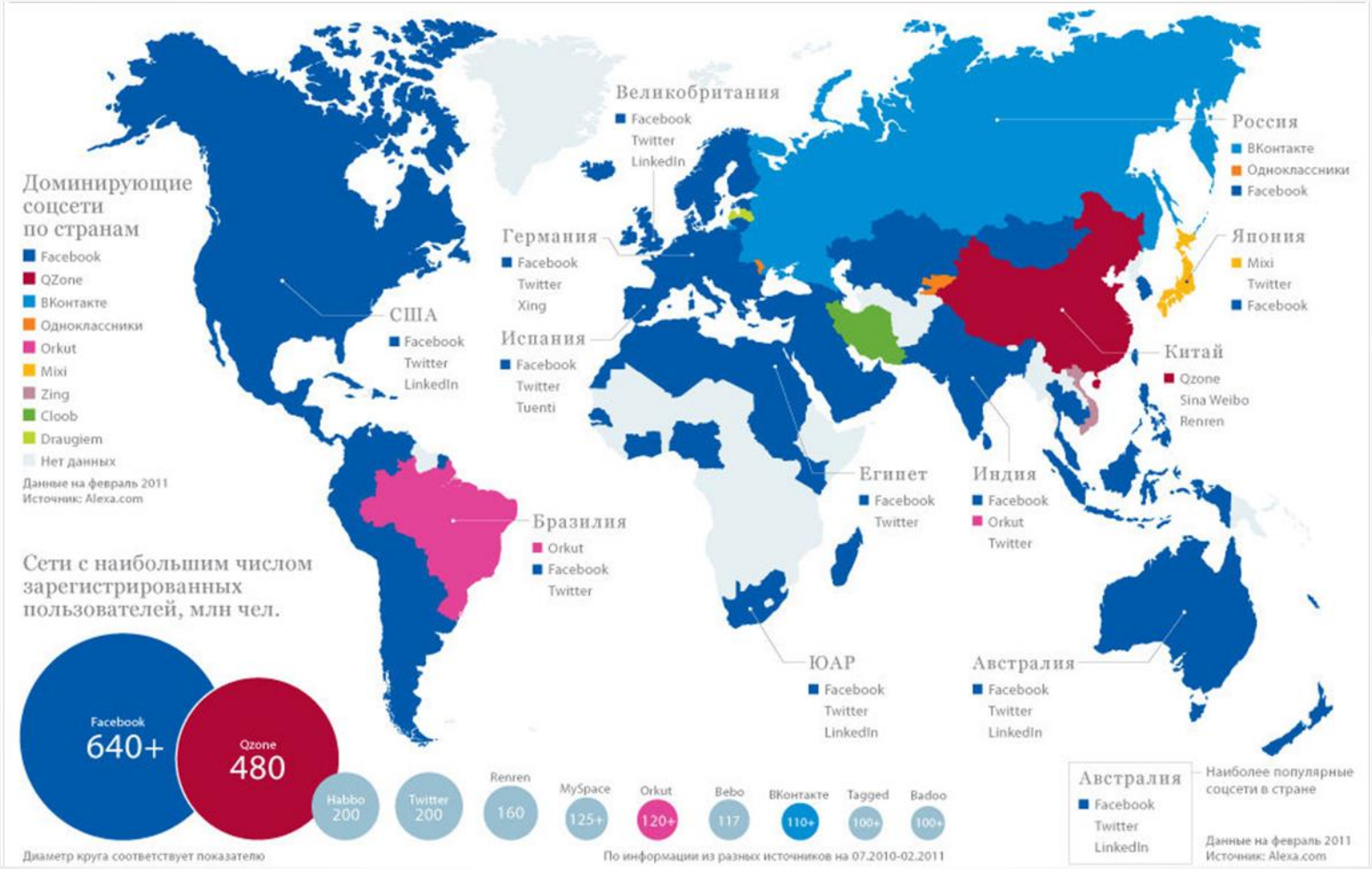
Пользователь может не знать, что его компьютер заражен ботом, потому что компьютеру этого пользователя бот не причиняет вреда, его цели находятся где-то в Интернете.

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.

Безопасность в социальных сетях



Безопасность в социальных сетях

Безопасность в социальных сетях

ИНФОРМАЦИОННЫЙ ВЗРЫВ – ГЕНЕРАЦИЯ КОНТЕНТА В МИРЕ:

- Классические СМИ – 1 млн. документов в сутки;
- Пользовательский контент (твиты, блоги, форумы, соцсети, отзывы, комментарии) – свыше 1 млрд. в сутки;
- Ежегодный прирост – 25%.

Безопасность в социальных сетях

92% – уровень доверия к социальным сетям

47% – уровень доверия к ТВ, радио, прессе

Рекомендации

Чтобы обезопасить себя и сохранить свою личную информацию конфиденциальной, необходимо соблюдать некоторые правила:

1. **Электронная почта.** Для того чтобы зарегистрироваться в социальных сетях, необходимо иметь отдельную электронную почту. Нельзя проходить регистрацию и указывать адрес рабочей почты или почты, которая связана с важными услугами – электронные кошельки, банковские услуги или оплата коммунальных платежей.

Рекомендации

Чтобы обезопасить себя и сохранить свою личную информацию конфиденциальной, необходимо соблюдать некоторые правила:

1. **Электронная почта.** Для того чтобы зарегистрироваться в социальных сетях, необходимо иметь отдельную электронную почту.

Нельзя проходить регистрацию и указывать адрес рабочей почты или почты, которая связана с важными услугами – электронные кошельки, банковские услуги или оплата коммунальных платежей.

Рекомендации

2. **Пароль.** Именно он является первой линией защиты для злоумышленников.

Для каждого сервиса необходимо использовать **отдельный пароль** и держать его в сохранности.

Необходимо подобрать базовое слово, которое можно дополнять другими символами или цифрами для каждой социальной сети в отдельности.

Рекомендации

3. **Минимизация информации, которая публикуется в социальной сети.**

Возможно, и стоит поделиться свежей фотографией с друзьями, но не нужно демонстрировать всему миру свою личную жизнь.

4. **При переходе на ссылки из посторонних источников необходимо быть максимально внимательным.** Особенно если они получены от незнакомых людей.

Рекомендации

5. **Не нужно использовать социальные сети в качестве главного хранилища информации и фотографий**.

Необходимо помнить, что это не персональный сайт, это ресурс, который принадлежит другим владельцам и обычно в набор стандартных инструментов не включены резервные копии.

6. **В социальных сетях не рекомендуется добавлять незнакомых людей.**

Злоумышленники могут создавать вымышленные аккаунты для получения той информации, которая доступна только пользователям из списка друзей.

Рекомендации

7. **Посещать социальные сети с рабочего места нельзя.**

Любая соцсеть – это распространение вирусов и других шпионских программ, что может привести к заражению не только персонального компьютера, но и всей корпоративной сети.

Это чревато потерей тех информационных данных, которые составляют коммерческую тайну организации.

Рекомендации

8. **Нельзя отправлять важные данные и документы посредством социальных сетей.**
9. **Нельзя публиковать фото документов.**

Нынешние соцсети содержат огромный функционал, который позволяет сделать личную информацию доступной только для определенного круга лиц. Чтобы активировать эту защиту, необходимо настроить конфиденциальность в собственном аккаунте.