**Лекция 9 (Продолжение)**

**Технологии нижнего уровня защиты информации в локальных сетях: межсетевые экраны**

Межсетевой экран (брандмауэр, Firewall) — программно-аппаратная система межсетевой защиты, которая отделяет одну часть сети от другой и реализует набор правил для прохождения данных из одной части в другую. Границей является раздел между локальной корпоративной сетью и внешними Internet-сетями или различными частями локальной распределенной сети. Экран фильтрует текущий трафик, пропуская одни пакеты информации и отсеивая другие.

Межсетевой экран (МЭ) является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена (Internet Security Protocol — IPSec) МЭ является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от НСД. Отметим, что большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС UNIX — особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol — TCP/IP) имеет "бреши" в защите [Левин М., 2001].

К числу таких служб и протоколов относятся:

* служба сетевых имен (Domain Name Server — DNS);
* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* служба эмуляции удаленного терминала Telnet;
* простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP);
* протокол передачи файлов (File Transfer Protocol);
* графическая оконная система X Windows.

Настройки МЭ, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах — запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" МЭ и использовать запрещенные сервисы через нестандартные порты (User Data Protocol — UDP), которые не запрещены политикой безопасности.

Функциональные возможности МЭ охватывают следующие разделы реализации информационной безопасности:

* настройку правил фильтрации;
* администрирование доступа во внутренние сети;
* фильтрацию на сетевом уровне;
* фильтрацию на прикладном уровне;
* средства сетевой аутентификации;
* ведение журналов и учет.

Программно-аппаратные компоненты МЭ можно отнести к одной из трёх категорий: фильтрующие маршрутизаторы, шлюзы сеансового уровня и шлюзы уровня приложений. Эти компоненты МЭ — каждый отдельно и в различных комбинациях — отражают базовые возможности МЭ и отличают их один от другого.

Фильтрующий маршрутизатор (Filter Router — FR) фильтрует IP-пакеты по параметрам полей заголовка пакета: IP-адрес отправителя, IP-адрес адресата, TCP/UDP-порт отправителя и TCP/UDP-порт адресата. Фильтрация направлена на безусловное блокирование соединений с определенными хостами и/или портами — в этом случае реализуется политика первого типа.

Формирование правил фильтрации является достаточно сложным делом, к тому же обычно отсутствуют стандартизированные средства тестирования правил и корректности их исполнения. Возможности FR по реализации эффективной защиты ограничены, так как на сетевом уровне эталонной модели OSI обычно он проверяет только IP-заголовки пакетов. К достоинствам применения FR можно отнести невысокую стоимость, гибкость формирования правил, незначительную задержку при передаче пакетов. Недостатки FR достаточно серьезны, о них следует сказать более подробно:

* отсутствует аутентификация конкретного пользователя;
* указанную выше аутентификацию по IP-адресу можно "обойти" путем замещения информации пользователя информацией злоумышленника, использующего нужный IP-адрес;
* внутренняя сеть "видна" из внешней сети;
* правила фильтрации сложны в описании и верификации, они требуют высокой квалификации администратора и хорошего знания протоколов TCP/UDP;
* нарушение работы ФМ приводит к полной незащищенности всех компьютеров, которые находятся за этим МЭ.

Шлюз сеансового уровня (Session Level Gateway — SLG) —активный транслятор TCP соединения. Шлюз принимает запрос авторизованного клиента на предоставление услуг, проверяет допустимость запрошенного сеанса (Handshaking), устанавливает нужное соединение с адресом назначения внешней сети и формирует статистику по данному сеансу связи. После установления факта, что доверенный клиент и внешний хост являются "законными" (авторизованными) участниками сеанса, шлюз транслирует пакеты в обоих направлениях без фильтрации. При этом часто пункт назначения оговаривается заранее, а источников информации может быть много (соединение "один-ко-многим") — это, например, типичный случай использования внешнего Web-ресурса.

Используя различные порты, можно создавать различные конфигурации соединений, обслуживая одновременно всех пользователей, имеющих право на доступ к ресурсам сети. Существенным недостатком SLG является то, что после установления связи пакеты фильтруются только на сеансовом уровне модели OSI без проверки их содержимого на уровне прикладных программ. Авторизованный злоумышленник может спокойно транслировать вредоносные программы через такой шлюз. Таким образом, реализация защиты осуществляется, в основном, на уровне квитирования (Handshaking).

Шлюз уровня приложений (Application Layer Gateway — ALG). Для компенсации недостатков FR и SLG шлюзов в межсетевые экраны встраивают прикладные программы для фильтрации пакетов при соединениях с такими сервисами, как Telnet и FTP и пр. Эти приложения называются Proxy-службами, а устройство (хост), на котором работает служба, называется шлюзом уровня приложений. Шлюз исключает прямое взаимодействие между авторизованным пользователем и внешним хостом. Зафиксировав сетевой сеанс, шлюз останавливает его и вызывает уполномоченное приложение для реализации запрашиваемой услуги — Telnet, FTP, WWW или E-mail. Внешний пользователь, который хочет получить услугу соединения в сети, соединяется вначале с ALG, а затем, пройдя предусмотренные политикой безопасности процедуры, получает доступ к нужному внутреннему узлу (хосту). Отметим явные преимущества такой технологии:

* уполномоченные приложения вызывают только те службы, которые прописаны в сфере их действия, исключая все остальные, которые не отвечают требованиям информационной безопасности в контексте запрашиваемой услуги;
* уполномоченные приложения обеспечивают фильтрацию протокола — например, некоторые ALG могут быть настроены на фильтрацию FTP соединения и запрещают при этом выполнение команды <FTP put>, что однозначно не позволяет передавать информацию на анонимный FTP-сервер;
* шлюзы прикладного уровня, как правило, фиксируют в специальном журнале выполняемые сервером действия и в случае необходимости сообщают сетевому администратору о возможных коллизиях и попытках проникновения;
* структура внутренней сети не видна из Internet-сети, шлюз осуществляет надежную аутентификацию и регистрацию, правила фильтрации просты, так как экран пропускает прикладной трафик, предназначенный только для шлюза прикладного уровня, блокируя весь остальной.

Как показывает практика, защита на уровне приложений позволяет дополнительно осуществлять другие проверки в системе защиты информации — а это снижает опасность "взлома" системы, имеющей "прорехи" в системе безопасности.

Межсетевые экраны можно разделить по следующим основным признакам:

* по исполнению: программный и программно-аппаратный;
* по используемой технологии: контроль состояния протокола (Stateful Inspection Protocol) или с использованием модулей посредников (Proxy Server);
* по функционированию на уровнях эталонной модели OSI (Open System Interconnection): шлюзы экспертного, прикладного, сеансового уровней, пакетный фильтр;
* по схеме подключения: схема единой защиты сети; схема с закрытым и не защищаемым открытым сегментами сети; схема с раздельной защитой закрытого и открытого сегментов сети.

На [рис. 6.16](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=3#image.6.16) показан вариант защиты локальной сети на базе программно-аппаратного решения — межсетевого экрана Cisco 2610 & PIX Firewall 520 компании Cisco Systems [Соколов А. В., Шаньгин В. Ф., 2002]. Отличительной особенностью этой модели является специальная ОС реального времени, а высокая производительность реализуется на базе алгоритма адаптивной безопасности (Adaptive Security Algorithm — ASA).



**Рис. 6.16.**Использование комплекса "маршрутизатор-файервол" в системах защиты информации при подключении к Internet

Приведенное решение имеет несомненные достоинства: высокая производительность и пропускная способность до 4 Гб/сек; возможность поддержки до 256 тысяч одновременных сессий; объединение преимуществ пакетного и прикладного шлюзов, простота и надежность в установке и эксплуатации, возможность сертификации в Государственной технической комиссии РФ.

В заключение отметим, что межсетевые экраны, естественно, не решают всех вопросов информационной безопасности распределенных КИС и локальных сетей — существует ряд ограничений на их применение и ряд угроз, от которых МЭ не могут защитить. Отсюда следует, что технологии МЭ следует применять комплексно — с другими технологиями и средствами защиты.

**Концепция защищенных виртуальных частных сетей**

При выходе локальной сети в открытое Internet-пространство возникают угрозы двух основных типов: несанкционированный доступ (НСД) к данным в процессе их передачи по открытой сети и НСД к внутренним ресурсам КИС. Информационная защита при передаче данных по открытым каналам реализуется следующими мерами:

* взаимная аутентификация сторон;
* прямое и обратное криптографическое преобразование данных;
* проверка достоверности и целостности полученных данных.

Организация защиты с использованием технологии виртуальных частных сетей (Virtual Private Network — VPN) подразумевает формирование защищенного "виртуального туннеля" между узлами открытой сети, доступ в который невозможен потенциальному злоумышленнику. Преимущества этой технологии очевидны: аппаратная реализация довольно проста, нет необходимости создавать или арендовать дорогие выделенные физические сети, можно использовать открытый дешевый Internet, скорость передачи данных по туннелю такая же, как по выделенному каналу.

В настоящее время существует четыре вида архитектуры организации защиты информации на базе применения технологии VPN [Соколов А. В., Шаньгин В. Ф., 2002].

Локальная сеть VPN (Local Area Network-VPN). Обеспечивает защиту потоков данных и информации от НСД внутри сети компании, а также информационную безопасность на уровне разграничения доступа, системных и персональных паролей, безопасности функционирования ОС, ведение журнала коллизий, шифрование конфиденциальной информации.

Внутрикорпоративная сеть VPN (Intranet-VPN). Обеспечивает безопасные соединения между внутренними подразделениями распределенной компании.

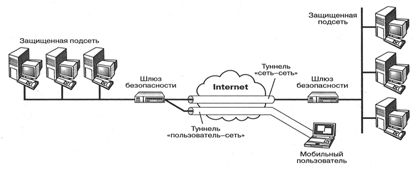
Для такой сети подразумевается:

* использование мощных криптографических средств шифрования данных;
* обеспечение надежности работы критически важных транзакционных приложений, СУБД, электронной почты, Telnet, FTP;
* скорость и производительность передачи, приема и использования данных;
* гибкость управления средствами подключения новых пользователей и приложений.

Сети VPN с удаленным доступом (Internet-VPN). Обеспечивает защищенный удаленный доступ удаленных подразделений распределённой компании и мобильных сотрудников и отделов через открытое пространство Internet ([рис. 6.17](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=3#image.6.17)).

Такая сеть организует:

* адекватную систему идентификации и аутентификации удалённых и мобильных пользователей;
* эффективную систему управления ресурсами защиты, находящимися в географически распределенной информационной системе.

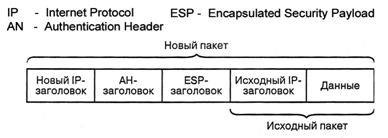


**Рис. 6.17.**Туннельная схема организации VPN сети

Межкорпоративная сеть VPN (Extranet-VPN). Обеспечивает эффективный защищённый обмен информацией с поставщиками, партнёрами, филиалами корпорации в других странах. Такая сеть предусматривает использование стандартизированных и надёжных VPN-продуктов, работающих в открытых гетерогенных средах и обеспечивающих максимальную защищенность конфиденциального трафика, включающего аудио и видео потоки информации — конфиденциальные телефонные переговоры и телеконференции с клиентами.

Можно выделить два основных способа технической реализации виртуальных туннелей:

* построение совокупности соединений (Frame Relay или Asynchronous Transfer Mode) между двумя нужными точками единой сетевой инфраструктуры, надежно изолированной от других пользователей механизмом организации встроенных виртуальных каналов;
* построение виртуального IP-туннеля между двумя узлами сети на базе использования технологии туннелирования, когда каждый пакет информации шифруется и "вкладывается" в поле нового пакета специального вида (конверт), который и передается по IP-туннелю — при этом пакет протокола более низкого уровня помещается в поле данных пакета более высокого уровня ([рис. 6.18](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=3#image.6.18)).



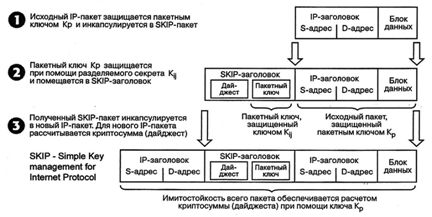
**Рис. 6.18.**Схема пакета, подготовленного к отправке по туннелю

VPN-туннель обладает всеми свойствами защищенной выделенной линии, проходящей через открытое пространство Internet. Особенность технологии туннелирования состоит в том, что она позволяет зашифровать не только поле данных, а весь исходный пакет, включая заголовки. Это важная деталь, так как из заголовка исходного пакета злоумышленник может извлечь данные о внутренней структуре сети — например, информацию о количестве локальных сетей и узлов и их IP-адресах.

Зашифрованный пакет, называемый SKIP-пакетом, инкапсулируется в другой пакет с открытым заголовком, который транспортируется по соответствующему туннелю ([рис. 6.19](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=3#image.6.19)).

При достижении конечной точки туннеля из внешнего пакета извлекается внутренний, расшифровывается, и его заголовок используется для дальнейшей передачи во внутренней сети или подключенному к локальной сети мобильному пользователю. Туннелирование применяется не только для обеспечения конфиденциальности внутреннего пакета данных, но и для его целостности и аутентичности, механизм туннелирования часто применяется в различных протоколах формирования защищенного канала связи. Технология позволяет организовать передачу пакетов одного протокола в логической среде, использующей другой протокол.

Таким образом, можно реализовать взаимодействие нескольких разнотипных сетей, преодолевая несоответствие внешних протоколов и схем адресации.



**Рис. 6.19.**Структура SKIP-пакета

Средства построения защищенной VPN достаточно разнообразны — они могут включать маршрутизаторы с механизмом фильтрации пакетов (Filtering Router), многофункциональные межсетевые экраны (Multifunction Firewall), промежуточные устройства доступа в сеть (Proxy Server), программно-аппаратные шифраторы (Firmware Cryptograph). По технической реализации можно выделить следующие основные виды средств формирования VPN:

* специализированные программные решения, дополняющие стандартную операционную систему функциями VPN;
* программно-аппаратное устройство на базе специализированной ОС реального времени, имеющее два или несколько сетевых интерфейсов и аппаратную криптографическую поддержку;
* средства VPN, встроенные в стандартный маршрутизатор или коммутатор;
* расширение охвата защищаемой зоны канала передачи и приёма данных за счет дополнительных функций межсетевого экрана.

Туннели VPN создаются для различных типов конечных пользователей: это может быть локальная сеть (Local Area Network — LAN) со шлюзом безопасности (Security Gateway) или отдельные компьютеры удаленных или мобильных пользователей с сетевым программным обеспечением для шифрования и аутентификации трафика — клиенты VPN ([рис. 6.17](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27505?page=3#image.6.17)). Через шлюз безопасности проходит весь трафик для внутренней корпоративной сети. Адрес шлюза VPN указывается как внешний адрес входящего туннелируемого пакета, а расшифрованный внутренний адрес пакета является адресом конкретного хоста за шлюзом.

Наиболее простым и относительно недорогим способом организации VPN-канала является схема, в соответствии с которой защищенный туннель прокладывается только в открытой сети для транспортировки зашифрованных пакетов. В качестве конечных точек туннеля выступают провайдеры Internet-сети или пограничные межсетевые экраны (маршрутизаторы) локальной сети. Защищенный туннель формируется компонентами виртуальной сети, функционирующим на узлах, между которыми он создается. В настоящее время активно функционирует рынок VPN-средств — приведем некоторые примеры популярных и широко используемых решений для каждого класса продуктов.

VPN на базе сетевых операционных систем. Для формирования виртуальных защищённых туннелей в IP сетях сетевая операционная система Windows NT использует протокол PPTP (Point-to-Point Transfer Protocol). Туннелирование информационных пакетов производится инкапсулированием и шифрованием (криптоалгоритм RSA RC4) стандартных блоков данных фиксированного формата (РРР Data Frames) в IP-дейтаграммы, которые и передаются в открытых IP-сетях. Данное решение является недорогим, и его можно эффективно использовать для формирования VPN-каналов внутри локальных сетей, домена Windows NT или для построения Internet- и Extranet- VPN для небольших компаний малого и среднего бизнеса для защиты не критичных приложений.

VPN на базе маршрутизаторов. В России лидером на рынке VPN-продуктов является компания Cisco Systems. Построение каналов VPN на базе маршрутизаторов Cisco осуществляется средствами ОС версии Cisco IOS 12.х. Для организации туннеля маршрутизаторы Cisco используют протокол L2TP канального уровня эталонной модели OSI, разработанного на базе "фирменных" протоколов Cisco L2F и Microsoft PPTP, и протокол сетевого уровня IPSec, созданного ассоциацией "Проблемная группа проектирования Internet (Internet Engineering Task Force — IETF). Эффективно применяется Cisco VPN Client, который предназначен для создания защищенных соединений Point-to Point между удаленными рабочими станциями и маршрутизаторами Cisco — это позволяет построить практически все виды VPN-соединений в сетях.

VPN на базе межсетевых экранов. Эта технология считается наиболее сбалансированной и оптимальной с точки обеспечения комплексной безопасности КИС и её защиты от атак из внешней открытой сети. В России нашел широкое применение программный продукт Check Point Firewall-1/VPN-1 компании Check Point Software Technologies. Это решение позволяет построить глубоко комплексную эшелонированную систему защиты КИС.

В состав продукта входят: Check Point Firewall-1, набор средств для формирования корпоративной виртуальной частной сети Check Point VPN-1, средства обнаружения атак и вторжений Real Secure, средства управления полосой пропускания информационных пакетов Flood Gate, средства VPN-1 Secure Remote, VPN-1 Appliance и VPN-1 Secure Client для построения Localnet/Intranet/Internet/Extranet VPN-каналов. Весь набор продуктов Check Point VPN-1 построен на базе открытых стандартов IPSec, имеет развитую систему идентификации и аутентификации пользователей, взаимодействует с внешней системой распределения открытых ключей PKI, поддерживает централизованную систему управления и аудита.

На российском рынке можно указать два продукта, получивших достаточно широкую известность — это криптографический комплекс "Шифратор IP пакетов" производства объединения МО ПН ИЭИ ([http://www.security.ru](http://www.security.ru/)) и ряд программных продуктов ЗАСТАВА компании ЭЛВИС+ ([http://www.elvis.ru](http://www.elvis.ru/)). Самым быстрорастущим сегментом рынка систем информационной безопасности по исследованиям IDC, Price Waterhouse Cooper и Gartner Group являются системы блокировки корпоративных каналов связи. Быстрее всего растут продажи систем защиты от утечек внутренней информации (Intrusion Detection and Prevention — IDP), которые позволяют контролировать трафик электронной почты и доступ к внешним Internet-ресурсам.

**Антивирусная защита**

История появления вирусописательства чрезвычайно интересна — она ещё ждёт своего дотошного исследователя! До сих пор нет единого мнения относительно момента, который можно было бы считать официальным днём появления вируса, как не существовало и критериев, под которые можно было бы подвести то или иное ПО и отличить исследовательские эксперименты от целенаправленно написанной программы с вредоносными функциями.

В 1949 году Джон фон Нейман (John von Naumann), выдающийся американский математик венгерского происхождения, сделавший важный вклад в квантовую физику, квантовую логику, функциональный анализ, теорию множеств, информатику, экономику и другие отрасли науки, разработал математическую теорию создания самовоспроизводящихся программ. Это была первая попытка создать теорию такого явления, но она не вызвала большого интереса у научного сообщества, так как не имела видимого прикладного значения.

Нет согласия и по поводу происхождения названия "компьютерный вирус". По одной из версий это случилось 10 ноября 1983 года, когда аспирант Университета Южной Калифорнии (University of Southern California) Фред Коэн (Fred Cohen) во время семинара по безопасности в Лехайском университете (Пенсильвания, США) продемонстрировал на системе VAX 11/750 программу, способную внедряться в другие программные объекты. Эту программу можно с полным правом считать одним из первых прототипов компьютерного вируса.

Коэн внедрил написанный им код в одну из Unix-команд, и в течение пяти минут после запуска её на вычислительной машине получил контроль над системой. В четырёх других демонстрациях полного доступа удавалось добиться за полчаса, оставив поверженными все существовавшие в то время защитные механизмы.

Существует версия, что термином "вирус" назвал копирующую саму себя программу научный руководитель Фреда, один из создателей криптографического алгоритма RSA Леонард Эдлеман (Leonard Adleman).

Годом позже, на 7-й конференции по безопасности информации, Ф.Коэн дает научное определение термину "компьютерный вирус", как программе, способной "заражать" другие программы при помощи их модификации с целью внедрения своих копий и выполнения заданных действий. Отметим, что Ф.Коэн определённо не был новатором в этой области. Теоретические рассуждения о распространяющихся копированием с компьютера на компьютер программах и практическая реализация успешно осуществлялись и раньше. Однако именно презентация Ф.Коэна заставила специалистов серьёзно заговорить о потенциальном ущербе от преднамеренных атак. Всего через пятнадцать лет распространение вредоносного программного обеспечения приобрело угрожающие масштабы, радикально снизить которые не представляется возможным.

В некотором смысле опередил Ф. Коэна 15-летний школьник из Пенсильвании Рик Скрента (Rich Skrenta). Его излюбленным занятием было подшучивание над товарищами путём модификаций кода игр для Apple II, которые приводили к внезапному выключению компьютеров или выполняли другие действия. В 1982 году он написал Elk Cloner — самовоспроизводящийся загрузочный вирус, инфицировавший Apple II через гибкий магнитный диск. Во время каждой 50-й перезагрузки ПК появлялось сообщение со словами: "Он завладеет вашими дисками, он завладеет вашими чипами. Да, это Cloner! Он прилипнет к вам как клей, он внедрится в память. Cloner приветствует вас!"

Программа Р.Скрента не вышла далеко за пределы круга его друзей. Лавры достались "шедевру" программистской мысли, появившемуся несколькими годами позже. Программу Brain ("Мозг") создали в 1988 году двое братьев — выходцев из Пакистана, которым приписывается инфицирование ПК через созданные ими нелегальные копии программы для мониторинга работы сердца. Вирус содержал уведомление об авторском праве с именами и телефонами братьев, поэтому пользователи заражённых машин могли обратиться к напрямую к вирусописателям за "вакциной". За первой версией Brain последовало множество модификаций, преследовавших сугубо коммерческий интерес.

В 1988 году аспирант Корнельского университета (Cornell University) Роберт Теппен Моррис младший (Robert Tappan Morris Jr.), приходившийся сыном главному научному сотруднику Агентства национальной безопасности США (National Security Agency), выпустил в свет первый широко распространившийся компьютерный червь, хотя экспериментальные работы в этой области проводились с конца 1970-х годов. Этот тип программ чаще всего не производит никаких деструктивных манипуляций с файлами пользователя и ставит целью как можно более быстрое и широкое распространение, снижая эффективность работы сетей.

По некоторым оценкам, от 5% до 10% подключённых в то время к Сети машин, по большей части принадлежавших университетам и исследовательским организациям, были атакованы им. Червь использовал уязвимости нескольких программах, в том числе Sendmail. Р.Т.Моррис стал первым человеком, осуждённым по обвинению в преступлениях в компьютерной сфере, и получил 3 года условно. Однако это не помешало ему впоследствии стать профессором Массачусетского технологического института (MIT).

Следующий большой шаг вредоносное ПО совершило в 90-х годах с ростом спроса на персональные компьютеры и количества пользователей электронной почты. Электронные коммуникации предоставили гораздо более эффективный путь инфицирования ПК, чем через носители информации. Образцом скорости распростанения стал вирус Melissa в 1999 году, внедрившийся в 250 тыс. систем. Однако он был безвреден, за исключением того, что каждый раз при совпадении времени и даты — например, 5:20 и 20 мая — на экране возникала цитата из The Simpsons.

Годом позже появился Love Bug, известный также как LoveLetter. За короткое время вирус облетел весь мир! Он был написан филиппинским студентом и приходил в электронном сообщении с темой "I Love You". Как только пользователь пытался открыть вложение, вирус через Microsoft Outlook пересылал себя по всем адресам в списке контактов. Затем скачивал троянскую программу для сбора интересующей филиппинца информации. LoveLetter атаковал около 55 миллионов ПК и заразил от 2,5 до 3 миллионов. Размер причинённого им ущерба оценивался в 10 миллиардов, но студент избежал наказания, поскольку Филиппины не имели в то время законодательной базы для борьбы с киберпреступниками [Борн Денис, [http://www.wired.com](http://www.wired.com/)].

Лавинообразное распространением вирусов стало большой проблемой для большинства компаний и государственных учреждений. В настоящее время известно более миллиона компьютерных вирусов и каждый месяц появляется более 3000 новых разновидностей ["Энциклопедия Вирусов", <http://www.viruslist.com/ru/viruses/encyclopedia>.].

Компьютерный вирус — это специально написанная программа, которая может "приписывать" себя к другим программам, т.е. "заражать их", с целью выполнения различных нежелательных действий на компьютере, в вычислительной или информационной системе и в сети.

Когда такая программа начинает работу, то сначала, как правило, управление получает вирус. Вирус может действовать самостоятельно, выполняя определенные вредоносные действия (изменяет файлы или таблицу размещения файлов на диске, засоряет оперативную память, изменяет адресацию обращений к внешним устройствам, генерирует вредоносное приложение, крадет пароли и данные и т.д.), или "заражает" другие программы. Зараженные программы могут быть перенесены на другой компьютер с помощью дискет или локальной сети.

Формы организации вирусных атак весьма разнообразны, но в целом практически их можно "разбросать" по следующим категориям:

* удаленное проникновение в компьютер — программы, которые получают неавторизованный доступ к другому компьютеру через Internet (или локальную сеть);
* локальное проникновение в компьютер — программы, которые получают неавторизованный доступ к компьютеру, на котором они впоследствии работают;
* удаленное блокирование компьютера — программы, которые через Internet (или сеть) блокируют работу всего удаленного компьютера или отдельной программы на нем;
* локальное блокирование компьютера — программы, которые блокируют работу компьютера, на котором они работают;
* сетевые сканеры — программы, которые осуществляют сбор информации о сети, чтобы определить, какие из компьютеров и программ, работающих на них, потенциально уязвимы к атакам;
* сканеры уязвимых мест программ — программы, проверяют большие группы компьютеров в Интернет в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки;
* "вскрыватели" паролей — программы, которые обнаруживают легко угадываемые пароли в зашифрованных файлах паролей;
* сетевые анализаторы (sniffers) — программы, которые слушают сетевой трафик; часто в них имеются возможности автоматического выделения имен пользователей, паролей и номеров кредитных карт из трафика;
* модификация передаваемых данных или подмена информации;
* подмена доверенного объекта распределённой вычислительной сети (работа от его имени) или ложный объект распределённой ВС (РВС).
* "социальная инженерия" — несанкционированный доступ к информации иначе, чем взлом программного обеспечения. Цель — ввести в заблуждение сотрудников (сетевых или системных администраторов, пользователей, менеджеров) для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы.

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

**Сетевые черви**

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия КЧ между собой являются способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, "стелс" и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам).

Пример — E-mail-Worm — почтовые черви. К данной категории червей относятся те из них, которые для своего распространения используют электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте). В первом случае код червя активизируется при открытии (запуске) зараженного вложения, во втором — при открытии ссылки на зараженный файл. В обоих случаях эффект одинаков — активизируется код червя.

Для отправки зараженных сообщений почтовые черви используют различные способы. Наиболее распространены:

* прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;
* использование сервисов MS Outlook;
* использование функций Windows MAPI.

Различные методы используются почтовыми червями для поиска почтовых адресов, на которые будут рассылаться зараженные письма. Почтовые черви:

* рассылают себя по всем адресам, обнаруженным в адресной книге MS Outlook;
* считывает адреса из адресной базы WAB;
* сканируют "подходящие" файлы на диске и выделяет в них строки, являющиеся адресами электронной почты;
* отсылают себя по всем адресам, обнаруженным в письмах в почтовом ящике (при этом некоторые почтовые черви "отвечают" на обнаруженные в ящике письма).

Многие черви используют сразу несколько из перечисленных методов. Встречаются также и другие способы поиска адресов электронной почты. Другие виды червей: IM-Worm — черви, использующие Internet-пейджеры, IRC-Worm — черви в IRC-каналах, Net-Worm — прочие сетевые черви.

**Классические компьютерные вирусы**

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: последующего запуска своего кода при каких-либо действиях пользователя или дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

* при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
* вирус скопировал себя на съёмный носитель или заразил файлы на нем;
* пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макроязыки (макросы) для автоматизации выполнения повторяющихся действий. Эти макроязыки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макроязыках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

**Скрипт-вирусы**

Следует отметить также скрипт-вирусы, являющиеся подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

**Троянские программы**

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

Троянские программы многообразны и различаются между собой по тем действиям, которые они производят на зараженном компьютере:

* Backdoor — троянские утилиты удаленного администрирования.
* Trojan-PSW — воровство паролей.
* Trojan-AOL — семейство троянских программ, "ворующих" коды доступа к сети AOL (America Online). Выделены в особую группу по причине своей многочисленности.
* Trojan-Clicker — Internet-кликеры. Семейство троянских программ, основная функция которых — организация несанкционированных обращений к Internet-ресурсам (обычно к Web-страницам). Достигается это либо посылкой соответствующих команд браузеру, либо заменой системных файлов, в которых указаны "стандартные" адреса Internet-ресурсов (например, файл hosts в MS Windows).
* Trojan-Downloader — доставка прочих вредоносных программ.
* Trojan-Dropper — инсталляторы прочих вредоносных программ. Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для "подсовывания" на компьютер-жертву вирусов или других троянских программ.
* Trojan-Proxy — троянские прокси-сервера. Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.
* Trojan-Spy — шпионские программы. Данные троянцы осуществляют электронный шпионаж за пользователем зараженного компьютера: вводимая с клавиатуры информация, снимки экрана, список активных приложений и действия пользователя с ними сохраняются в какой-либо файл на диске и периодически отправляются злоумышленнику. Троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.
* Trojan — прочие троянские программы. В данной категории также присутствуют "многоцелевые" троянские программы, например, те из них, которые одновременно шпионят за пользователем и предоставляют proxy-сервис удаленному злоумышленнику.
* Trojan ArcBomb — "бомбы" в архивах. Представляют собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные — зависание или существенное замедление работы компьютера или заполнение диска большим количеством "пустых" данных. Особенно опасны "архивные бомбы" для файловых и почтовых серверов, если на сервере используется какая-либо система автоматической обработки входящей информации — "архивная бомба" может просто остановить работу сервера.
* Trojan-Notifier — оповещение об успешной атаке. Троянцы данного типа предназначены для сообщения своему "хозяину" о зараженном компьютере. При этом на адрес "хозяина" отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п. Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением к веб-странице "хозяина", ICQ-сообщением. Данные троянские программы используются в многокомпонентных троянских наборах для извещения своего "хозяина" об успешной инсталляции троянских компонент в атакуемую систему.