**Краткий обзор различных видов сетевых атак**

Ниже рассмотрены некоторые наиболее опасные виды сетевых атак. Этот обзор не следует считать исчерпывающим, так как полный перечень занял бы *целый* том. Некоторые классы атак, например, использующие *переполнение* буферов, являются составной частью многих видов вредоносных атак. Атаки переполнения имеют, в свою *очередь*, много разновидностей. Одна из наиболее опасных предполагает ввод в *диалоговое окно*, помимо текста, присоединенного к нему исполняемого кода. Такой ввод может привести к записи этого кода поверх исполняемой программы, что рано или поздно вызовет его *исполнение*. Последствия нетрудно себе представить.

"Пассивные" атаки с помощью, например, *sniffer*, особенно опасны, так как, во-первых, практически не детектируемы, во-вторых, предпринимаются из локальной сети (внешний *Firewall* бессилен).

***Вирусы*** — вредоносные программы, способные к самокопированию и к саморассылке. Еще в декабре 1994 года я получил предупреждение о распространении сетевых *вирусов* (good times и xxx-1) *по* *Интернет*:

"there are two virus infected messages circulated in the internet. one is

called "good times" and the other "xxx-1". do not read !! do not download !!!

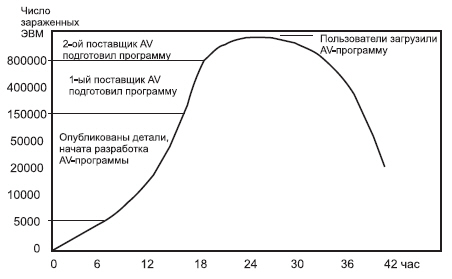
delete right away !!!!"

(Не читайте!! Не загружайте!!! Немедленно уничтожайте!!!!)

С момента создания до момента обнаружения *вируса* проходят часы, дни, недели, а иногда и месяцы. Это зависит от того, насколько быстро проявляются последствия заражения. Чем это время больше, тем большее число ЭВМ оказывается заражено. После выявления факта заражения и распространения новой разновидности *вируса* требуется от пары часов (например, для Email\_Worm.Win32.Bagle.bj) до трех недель (W32.Netsky.N@mm) на выявление сигнатуры, создания противоядия и включения его сигнатуры в базу данных противовирусной программы. Временная *диаграмма жизненного цикла* *вируса* представлена на [рис. 12.1](https://intuit.ru/studies/courses/1124/201/lecture/5221?page=1#image.12.1) ("*Network Security*", v.2005, *Issue* 6, June 2005, p 16-18). Только за 2004 год зарегистрировано 10000 новых сигнатур *вирусов*. Червь *Blaster* заразил 90% машин за 10 минут. За это время антивирусная *группа* должна обнаружить *объект*, квалифицировать и разработать средство противодействия. Понятно, что это нереально. Так что антивирусная *программа* является не столько средством противодействия, сколько *успокоительным*. Эти же соображения справедливы и для всех других видов атак. Когда *сигнатура атаки* становится известной, сама *атака* обычно не опасна, так как уже выработаны средства противодействия и *уязвимость* перекрыта. Именно *по* этой причине такое внимание уделяется системе управления программными обновлениями (пэтчами).

Некоторые *вирусы* и черви имеют встроенные SMTP-программы, предназначенные для их рассылки, и люки для беспрепятственного проникновения в зараженную машину. Новейшие версии снабжены средствами подавления активности других *вирусов* или червей. Таким образом могут создаваться целые сети зараженных машин ( *BotNet* ), готовых *по* команде начать, например, *DDoS* -атаку. Для управления такими машинами-зомби может использоваться протокол **IRC** (*Internet* *Relay* *Chart*). Эта система рассылки сообщений поддерживается большим числом серверов и поэтому такой канал обычно трудно отследить и запротоколировать. Этому способствует также то, что большинство систем более тщательно контролируют *входной* трафик, а не выходной. Следует иметь в виду, что зараженная машина может служить, помимо *DoS-атак*, для сканирования других ЭВМ и рассылки *SPAM*, для хранения нелегальных программных продуктов, для управления самой машиной и кражи документов, хранящихся там, для выявления паролей и ключей, используемых хозяином. *Ущерб* от *вируса* *Blaster* оценивается в 475000$.

**К сожалению, пока не придумано надежных средств обнаружения новых***вирусов* **(сигнатура которых не известна)**.



**Рис. 12.1.**Диаграмма жизни вируса при благоприятном сценарии

В 2005 году выявлена еще одна *угроза* – распространение *вирусов* и *сетевых червей* с помощью программ-роботов поисковых систем (*bots*), базирующихся на *IRC*.

Программы *bots* не всегда опасны, некоторые их разновидности применяются для сбора данных, в частности, о предпочтениях клиентов, а в поисковой системе Google они работают для сбора и индексации документов. Но в руках хакера эти программы превращаются в опасное оружие. Наиболее известная *атака* была предпринята в 2005 году, хотя подготовка и "первые опыты" начались в сентябре 2004 года. *Программа* искала машины со специфическими уязвимостями, в частности, LSASS (*Local* *Security* *Authority* *Subsystem* *Service*, *Windows*). Подсистема LSASS, призванная способствовать обеспечению безопасности, оказалась сама уязвимой для атак типа переполнения буфера. Хотя *уязвимость* уже ликвидирована, число машин с необновленной версией остается значительным. После вторжения *хакер* обычно использует *IRC* для выполнения нужных ему операций (открытие определенного порта, рассылка *SPAM*, *запуск* сканирования других потенциальных жертв). Новой особенностью таких программ является их встраивание в операционную системы таким образом ( *rootkit* ), что они не могут быть обнаружены, так как размещаются в зоне ядра ОС. Если антивирусная программы попытается получить *доступ* к определенной области памяти с целью выявления вредоносного кода, *rootkit* перехватывает такой *запрос* и отправляет тестирующей программе уведомление, что все в порядке. Что еще хуже, bot-программы могут модифицировать содержимое *EPROM*. Если хакеру удается проникнуть через *Firewall*, то под ударом оказываются практически все машины локальной сети. Некоторые разновидности этих программ используют *порт* 445, который *Microsoft* зарезервировала для совместного использования файлов, принтеров и других ресурсов. Число модификаций этих вредоносных программ быстро растет.

В настоящее время в мире постоянно активно от 3 до 3,5 миллиона таких программ. Каждый день с помощью этой атаки поражается до 250000 IP-адресов. Простота компрометации машин достигла такого уровня, что один из хакеров продавал взломанные машины *по* цене 4 *цента*. Всего же ему удалось заработать 58357 долларов меньше чем за 12 месяцев. Это при том, что более 11000 хакеров находятся постоянно под непрерывным наблюдением спецслужб США.

В основном жертвами становятся домашние машины, но среди жертв оказались такие компании, как Сaterpiller, *CNN*, eBay, DuPont и *Microsoft*. Без преувеличения можно утверждать, что это самая серьезная *угроза* сетевой безопасности.

Следует постоянно помнить, что дополнительные WEB-сервисы (*FTP*, *DNS*, *доступ* к DB и т.д.) создают новые *угрозы безопасности*. Уязвимости обнаруживаются время от времени в широко используемых программах, например, *Internet* Explorer, *Outlook* и *Outlook* Express. Эти атаки для проникновения в систему используют *переполнение* буферов.

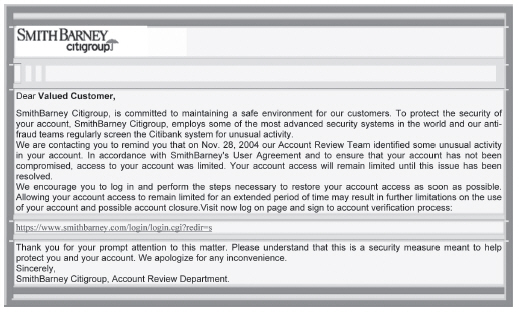
WEB-страницы иногда имеют скрытые ссылки на конфиденциальные данные. Именно на это рассчитывают хакеры.

*Практика показывает, что 80% усилий тратится на противодействие внешним атакам, а 70% атак, наносящих ущерб, производится из локальной сети*.

***Phishing*** (*password* harvesting *fishing*) – получение паролей, PIN-кодов и пр. (последующая *кража* информации). Этот вид атаки начинается с рассылки почтовых сообщений, содержащих ссылку на известный *ресурс* (или имитирующий такую ссылку). *Дизайн* WEB-страницы обычно копируется с воспроизводимого ресурса. На фальсифицируемой странице может быть, например, написано, что банк, где вы имеете счет, проводит акцию *по* проверке безопасности доступа. Вам предлагается ввести номер вашей кредитной карты и PIN-код. Если вы это сделаете, злоумышленники сообщат, что все в порядке, а с вашего счета через некоторое время пропадут деньги. Но если это не сопряжено с банком, опасность такой атаки нисколько не уменьшается. Получив *доступ* к вашему акаунту, злоумышленники получат *доступ* к конфиденциальной информации и т.д. (смотри [http://antiphishing.org/APWG\_Phishing\_Activity\_Report\_ April\_2005.pdf](http://antiphishing.org/APWG_Phishing_Activity_Report_%20April_2005.pdf)). Число атак типа *phishing* за апрель 2005 года составило 2854, месячный рост — около 15%, и тенденция увеличения числа таких атак сохраняется. Мошенники могут объявлять себя сотрудниками Красного Креста, собирающими помощь для жертв землетрясения или урагана, и т.д..

Владелец сервера или рабочей станции может получить сообщение, например, из компании *Microsoft*, какого-то известного поставщика антивирусных программ или определенной службы ФБР или МВД. Оформление сообщения может быть выполнено в соответствии со стилем и снабжено традиционными символами этой фирмы. В этом уведомлении утверждается, что в рамках компании *по* проверке сети *Интернет* обнаружено, что машина получателя производит рассылку зараженных *spyware* сообщений или сама заражена каким-либо *вирусом*. Чтобы минимизировать *ущерб*, компания предлагает бесплатно скопировать программу *по* локализации и удалению *spyware*. При этом "благодетели" могут попросить на время копирования отключить антивирусную защиту, если таковая имеется. Если получатель данного уведомления последует данному совету, он обнаружит и ликвидирует на своей машине какое-то число вредных программ. Но с очень высокой вероятностью на его машине обоснуется *троянский конь* или другая *программа* *spyware*.

*Хакер* может прикинуться сотрудником организации и написать, что он забыл *пароль*. Служба администратора часто присылает новый *пароль*, не проверяя *личность* человека, приславшего *запрос*. Терминалы иногда стоят в общедоступных помещениях, а сотрудник может ненадолго отойти от дисплея, не прерывая сессию, — посторонний может сесть на его *место*, поменять *пароль* или загрузить троянского коня, получив *доступ* в систему. *Злоумышленник* может подсмотреть *пароль* и через плечо работающего легального пользователя. Хорошей практикой является отсутствие документов (и тем более паролей!) на вашем рабочем столе. Длительная пауза в работе должна автоматически запирать *дисплей*. Критическая *информация* в *laptop* или *notebook* должна быть зашифрована. Одним из возможных средств атак является использование **IDN** (*International* *Domain Name*). Дело в том, что в системах, поддерживающих *IDN*, допускается использование букв национальных алфавитов, а, например, некоторые буквы латинского и русского алфавитов пишутся идентично. Этим могут воспользоваться злоумышленники, они могут зарегистрировать имена, которые выглядит как имена известной фирмы, например, *microsoft*.*com*, где некоторые буквы заменены на русские, так что это внешне не заметно, например, буквы "с" или "о". Тогда при ошибочной замене одной или нескольких букв на русские клиент попадет не на *сайт* компании *Microsoft*, а на внешне не отличимый от него *сайт* злоумышленника. В среднем электронные мошенничества наносят *ущерб* порядка 895$, частота же таких преступлений достаточно быстро растет. Пример подобного сообщения представлен ниже (я получил это сообщение на свой *адрес* в ЦЕРН (Женева)):



*Анализ* инцидента показал, что произведена полная подмена страниц. *Утилита* *Traceroute* указывала на вроде бы легальный *адрес* в США...

Разновидностью такого рода атак является *атака* через *DNS* (или каким-то иным способом), когда страница известного *URL* подменяется страницей злоумышленника (*spoofing*). Большую угрозу могут представлять фальсификации серверов обновления (*WINDOWS*, антивирусных библиотек и т.д.), так как при таком "обновлении" в ЭВМ жертвы может быть записана любая вредоносная *программа*. Сходную угрозу может представлять интерактивная *игра*, которая, например, при переходе с одного уровня на другой, предлагает загрузить некоторый программный *модуль*.

Самой авторитетной организацией *по* противодействию фишингу является *APWG* (Anti- *Phishing* *Working Group* — <http://www.antiphishing.org/>). Эта структура мониторирует появление подставных сайтов, используемых для фишинга.

Проверить *сайт* на "благонадежность" (отсутствие фишинговых ловушек) можно с помощью <http://linkscanner.explabs.com/linkscanner/>.

Существуют и другие угрозы, например, так называемая "Молдавская *связь*". Суть этой уловки, использованной впервые одним из провайдеров в Молдове, заключается в том, что в каком-то депозитарии или web-странице приводится *ссылка* на некоторый привлекательный *объект*, например, набор эротических картинок. Но для их просмотра предлагается скопировать себе специальную программу. При запуске оговоренной программы *канал связи* с местным провайдером разрывается и устанавливается *связь* через *модем* с другим удаленным провайдером. Это особенно опасно для людей, подключенных к *Интернет* через *модем*, так как может стоить им многие сотни долларов за пользование междугородним телефоном.

***Троянский конь*** — *программа*, записывающая все нажатия клавиш на терминале или мышке, способна записывать *screenshot*’ы и передавать эти данные удаленному хозяину. Если на ЭВМ оказался установленным общеизвестный *троянский конь*, машина становится уязвимой. Именно с этим связано сканирование хакерами номеров портов известных троянских коней. Многие современные *вирусы* и черви могут загружать в зараженную ЭВМ троянского коня (или программу *spyware* ), целью которого может быть получение не только паролей, но также номеров кредитных карт и PIN-кодов. В некоторых случаях зараженная машина может стать источником DoS-атаки. В 2005 году *троянский конь* был отловлен на правительственном WEB-сервере КНР. Обнаружить извне троянского коня или черный ход методом сканирования портов становится достаточно сложно. *Хакер* устраивает так, что сначала нужно послать *запрос* на соединение через *порт* Р1 (отклика не посылается), затем через *порт* Р2 и т.д., и только после n-ого запроса через *порт* Pn программой, установленной на машине жертвы, посылается отклик и открывается *доступ* извне.

*Spyware*. Эта разновидность программ не обязательно вредоносна. Некоторые разработчики *software* встраивают такие программы в свои продукты, чтобы отслеживать предпочтения своих клиентов. К сожалению, не все эти программы столь безобидны. Некоторые программы *spyware* в соответствии со своим названием отслеживают действия хозяина машины, куда эта *программа* внедрена (нажатия клавиш, посещаемые сайты, конфиденциальную информацию и т.д.) и передают результаты своему хозяину. Например, вы через *Интернет* вошли на *сайт* своего банка и осуществили платеж. При этом вам пришлось ввести номер кредитной карты и PIN-код. Если на вашей машине установлен *троян*, эта *информация* может стать известной хозяину троянского коня. Исследования, проведенные в 2004 году, показали, что 90% РС имеют какой-то вид *spyware* (это не обязательно троянские кони).

В среднем каждая ЭВМ содержит в себе до 26 разновидностей *spyware* программ (возможно, это и преувеличение, но если вы не предпринимали специальных мер, как *минимум* одна такая *программа* в вашей ЭВМ имеется). Следует учитывать, что *spyware* ( *adware* или *malware*) имеют примерно те же возможности, что и *троянский конь*, но встраиваются в другие программы и распространяется несколько другими методами. Кроме того, в отличие от троянских коней эти программы часто не обнаруживаются антивирусными программами. (Смотри <http://www.earthlink.net/about/press/pr_spyAudit>, http://www.ssppyy.com и securityresponse.symantec.com.)

*Spyware* может попасть к вам вместе с поздравительной открыткой. Если хотя бы один *пользователь* откроет такую открытку, вся система окажется скомпрометированной. 80% данных *spyware* отсылает своему хозяину *по* почте (*порт*=25), некоторые разновидности этих программ содержат в себе почтовый *сервер*.

Заражение *spyware* может осуществиться традиционно через почту, IM (*Instant Messaging*) или в результате посещения скомпрометированного сайта. Некоторые компании, стремящиеся заполучить клиентов, разрешают инсталляцию кодов на свои серверы, чтобы отслеживать клиентов. Такие коды заражают посетителей. Особенностью некоторых видов *spyware* является их тесная *связь* с операционной системой, что часто мешает их удалению и очистки от них ЭВМ. Относительно новым источником заражений становятся блог-серверы. В настоящее время нет единого решения проблемы *spyware*. Наиболее эффективной является комбинация образования и технологических средств. Нужно объяснить сотрудникам, что не следует посещать неавторизованные сайты или брать домой свой служебный *laptop*, так как дома их дети или родственники могут с помощью этого компьютера заглянуть на сомнительный *сервер* и заразить машину. Это может в свою *очередь* привести к заражению ЭВМ локальной сети компании, защищенной *Firewall*. Нельзя также полагаться на традиционные антивирусные средства защиты.

Существует множество программных средств, способных обнаружить известные версии *spyware* или блокировать *связь* этих программ с хозяином (например, R3000). Но, выбирая такое программное средство, нужно быть осторожным, особенно в отношении малоизвестных источников, некоторые из этих программ сами могут оказаться разновидностями *spyware*. Здесь, так же, как в случае антивирусных программ, остается незакрытой возможность заражения новой версией *spyware*, которая пока не попала в базу данных программы детектирования.

Проверка моей машины с помощью программы *BPS* *spyware* показала, что там содержится около 2000 таких программ (машина не сканировалась на предмет *spyware* ); всего *по* результатам сканирования удалено 17825 объектов – большинство из них – это *cookie*), но с момента инсталляции ОС на машине работала антивирусная *программа*. Последние полгода там работал ZoneAlarm. Полная очистка ЭВМ от *spyware*, размещенных в файлах, в cookies, в реестре и т.д., заняла достаточно много времени.

#### SPAM

Слово " *SPAM* " — это компьютерный жаргон. На самом деле, спам — это такие консервы, вроде китайского колбасного фарша, популярного в годы застоя. Расшифровывается это слово как *SPiced* hAM — перченая ветчина. Слово это придумано (и зарезервировано) корпорацией Hormel.

В начале 1970-х английские анархисты Monty Python сочинили сюрреальный скетч о спаме. Действие происходит в кафе, в котором меню состоит из спама, яичницы с беконом из спама, спама с яичницей, и беконом из спама, яичницы со спамом и сосиской из спама, сосиски из спама, спама и помидоров со спамом... (тут официантку прерывает компания викингов, сидящих за соседним столиком. Викинги поют: спам, спам, спам! вкусный спа-а-ам!)

До 1994 года Интернет был сетью сугубо не коммерческой, а пользователями Интернета были студенты и профессора университетов. С 1994-1995 доступ к Интернет был открыт человеку с улицы, то есть торговцу. Каналы информации UseNet, прежде заполненные научными дискуссиями, порнографией или пустым трепом, были украшены сотней сообщений под заголовком типа "make money fast". Такие сообщения стали называть спамом.

Начав с конференций UseNet, спаммеры переключились на е-майл (электронную почту). Составив списки из миллионов адресов, спаммеры рассылают коммерческую рекламу сомнительных продуктов, сайтов и полулегальных услуг. В последнее время, впрочем, распространённым продуктом рекламы являются программы для рассылки спама. Купив такую программу, желающие могут разослать по 100 и более миллионам адресов предложение купить у них какой-нибудь товар. Спам практически ничего не стоит для отправителя — временем и деньгами за него расплачивается сплошь и рядом жертва рассылки.

Согласно исследованиям GVU, только 9,2% пользователей читают спам-сообщения. При этом данная цифра сформирована благодаря пользователям-новичкам, а из тех, кто провел в сети более 3 лет, спам читают лишь 5,4 %. 12% пользователей сети пишут возмущенные письма по обратному адресу, а 1,5 % пользователей производят вендетту (это могут быть "почтовые бомбы" в адрес злоумышленника, жалоба провайдеру и т.д.).

Что касается меня лично, я спам не читаю, и это уже вынужденная мера, так как я получаю более 300 сообщений в сутки. Специальная программа фильтрует мою почту и укладывает такие сообщения в специальный ящик с названием " *SPAM* ". Конечно, можно их там прочесть, но гораздо быстрее нажать последовательно клавиши "Ctrl A" и "Del". Некоторые распространители спама настолько обнаглели, что предлагали год назад за 20 долларов исключить мой адрес из списка рассылки. Но ведь есть более дешевый способ — автоматически уничтожать такие сообщения, а не укладывать в специальный ящик. Если же вы заплатите хотя бы раз, вам посыпятся такого рода предложения от десятков подобных "фирм".

Спамерным атакам подвергаются не только корпоративные пользователи сети, но и владельцы домашних PC, имеющих выход в Internet. Этот факт существенно осложняет борьбу со спамом и вовлекает в неё не только самих пользователей, но и широкую общественность. В частности, 1 марта 1999 года Открытым Форумом Интернет-Сервис-Провайдеров был одобрен документ "Нормы пользования сетью" [http://www.ofisp.org](http://www.ofisp.org/) (Acceptable Use Policy), который регламентирует нормы работы в сети, в том числе, накладывает ограничения на *информационный шум* (спам) и обязателен для всех пользователей, а в июле минувшего года Палата Представителей США одобрила меры по борьбе со спамом. Согласно законопроекту, электронное послание должно иметь реальный обратный адрес для того, чтобы получатели спама могли заблокировать его отправителя; нарушение этого закона грозит злоумышленнику штрафом в размере до $150.000. Почему СПАМ — это действительно плохо? С практической точки зрения эта проблема раскладывается на несколько компонент (RFC 2505):

1. Объём, т.е. пользователи получают огромное количество спамсообщений в свои почтовые ящики.
2. В 99% процентах случаев содержание таких писем не коррелирует с интересами адресатов.
3. Для получателей СПАМ стоит реальных денег. Например, те, кто имеют выход в сеть через модем и платят за время, проведенное в Интернет, вынуждены тратить деньги на фильтрацию полезных писем.
4. СПАМ также стоит денег и для тех, кто поддерживает и отвечает за корректную работу почтовых серверов. Предположим, что злоумышленник послал письмо объёмом 10 килобайт 10 000 пользователям на одну ЭВМ. Несложно подсчитать, сколько места займут его все его сообщения, а именно 100 мегабайт. А что произойдёт, если спамер не один и отправляет не по одному письму?
5. Большинство спамеров идут на всевозможные уловки, чтоб адресат взглянул хоть краем глаза на их сообщение. Например, пишут письмо таким образом, чтоб получатель подумал, что его с кем-то перепутали, или же помечают письмо так, что якобы внутри него содержится информация, запрашиваемая адресатом. Разумеется, о морали и этике здесь не может идти и речи.

Признаки спам

* Заголовки <Received> образуют последовательную цепочку, начиная от верхней части сообщения и заканчивая нижней частью.
* Любые заголовки <Received>, расположенные ниже заголовка <Date>, — поддельные.
* Следует обращать внимание на любой заголовок <Received>, в котором имена двух узлов не совпадают. Вероятно, почтовое сообщение было ретранслировано через первый узел (узел, имя которого заключено в круглые скобки, является действительным источником сообщения).
* Заголовок <Received>, имеющий старую дату, вероятнее всего, подделан.
* Сетевая часть заголовка <From> должна согласоваться с последним заголовком <Received>.
* Домен заголовка <Message-Id> должен совпадать с доменом заголовка <From>.
* Следует проверить, нет ли в заголовках <Received> признаков того, что сообщение ретранслировано через посторонний узел.
* Убедитесь, что все перечисленные узлы действительно существуют в базе данных DNS
* Поле <From> не должно быть пустым.
* Обилие в тексте опечаток и прочих искажений может также указывать на нелегальную природу сообщения, так как программа рассылки может работать без контроля подтверждений, чтобы скрыть истинный адрес рассылки, или такие модификации вносит сама программа рассылки, чтобы замаскировать массовую рассылку идентичного текста.

В последнее время появилось достаточное число коммерческих и общедоступных программ фильтрации *SPAM*.

*SPAM* составляет до 90% полного объема почтовых сообщений. Рассылка *SPAM* стала достаточно доходной частью полукриминального бизнеса. Это сопряжено с потерями сетевых ресурсов, о времени получателей я уже не говорю. Часть таких сообщений часто заражена *вирусами*, червями или троянскими конями. Эффективность современных фильтров *SPAM* достигает 90%. При этом следует учитывать, что фильтры сильно загружают серверы DNS. Для минимизации *SPAM* обычно рекомендуется иметь несколько почтовых адресов, например, один для частной переписки, один для деловой и один для информационных обменов, подписки и пр. Это облегчает распознавание *SPAM*. Полезно самому создавать уникальные адреса для каждого вида обменов и время от времени их менять (см. [email.about.com/library/weekly](https://intuit.ru/studies/courses/1124/201/lecture/email.about.com/library/weekly). Это легко делать в случае подписных листов. Рекомендуется удалить свой почтовый адрес из своего WEB-сервера. Не рекомендуется покупать что-либо по рекомендациям *SPAM* -рассылок, тем более что в 95% случаях это могут оказаться недобросовестные поставщики. (Смотри также <http://email.about.com/cs/spamfiltering>, [email.about.com/library/howto/htnegativespamfilter.htm](https://intuit.ru/studies/courses/1124/201/lecture/email.about.com/library/howto/htnegativespamfilter.htm), [spam.abuse.net/spam/](https://intuit.ru/studies/courses/1124/201/lecture/spam.abuse.net/spam/) и <http://www.scambusters.org/stopspam/stop-spam.html>.)

***SCAM*** — мошеннический трюк, заключающийся в том, чтобы, ссылаясь на авторитетных лиц, втереться в доверие и извлечь коммерческую выгоду. Первооткрывателями этого вида мошенничества были адресаты из Нигерии. (Смотри [en.wikipedia.org/wiki/Scam](https://intuit.ru/studies/courses/1124/201/lecture/en.wikipedia.org/wiki/Scam).)

Все перечисленные программы создавались людьми специально для нанесения вреда, их мотивации — предмет изучения психологов и социологов. Но есть потенциально опасные объекты, не создаваемые специально для нанесения вреда. Это, прежде всего, программы, разработанные не профессионалами и содержащие ошибки. Следует иметь в виду, что любая ошибка в программе опасна сама по себе, но она может также стать объектом атаки хакера. По этой причине бездумное использование не сертифицированных программ несет в себе достаточно высокий уровень риска.

В организациях с 10000 сотрудников сплошь и рядом имеется до 16000 акаунтов за счет уже давно не используемых (люди уволились). Такие неиспользуемые акаунты могут стать объектом атаки, тем более что их создание может относиться ко времени, когда безопасности паролей не уделялось должного внимания. По этой причине администратор должен требовать регулярного обновления паролей и удалять устаревшие, неиспользуемые акаунты.

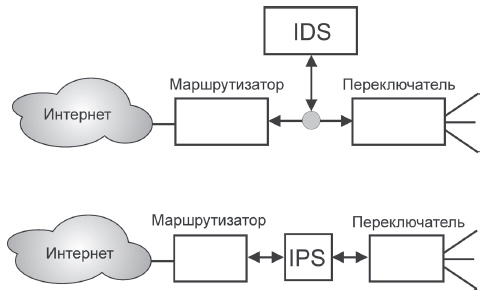
При разработке новых устройств и программ надо уже на стадии проектирования встраивать в них средства безопасности. Должны быть созданы специальные курсы обучения тому, как писать безопасные программы, например, CGI.

Существует много методов обмануть *IDS* (*Intrusion Detection System*) — скажем, перегрузив его. Некоторые *IDS* имеют механизмы улучшения эффективности, и это может быть использовано хакером, например, многие *IDS* игнорируют параметры, передаваемые в запросе GET. Можно обмануть *IDS*, используя медленное сканирование. Существует известная *сигнатура атаки*, содержащая в себе определенную строку в URL-запросе. Если представить ее в альтернативной кодировке с использованием символов %, *IDS* эту строку не распознает. Настройка *IDS* должна выполняться с учетом реальных угроз конкретной сети. Полагаться на то, что сервис-провайдер имеет свою систему *IDS*, ни в коем случае нельзя. Следует также учитывать, что поставляемые вместе с *IDS* программы анализа журнальных файлов, требуют хорошей настройки. Настройка *IDS* сильно зависит от используемой ОС. Одним из способов атак является шестнадцатеричное кодирование параметров HTTP-запросов или использование для этих целей уникодов. Идея атаки заключается в том, что дешифровка такого представления параметров может в определенных случаях производится некорректно, и это открывает хакерам дополнительные возможности. Еще одним недостатком *IDS* являются *ложные тревоги*, которые при достаточно высокой частоте могут, в конце концов, притупить внимание администратора к реальным угрозам.

*IDS* предоставляет информацию для сетевого администратора, чтобы он, если сочтет нужным, предпринял определенные меры. Иногда оказывается, что действия администратора уже запоздали. Исследования показывают, что запаздывание в 10 часов дает 80% для успеха хакера, при 20 часах вероятность вторжения оказывается равной 95%, при 30 часах задержки — успех хакера гарантирован, каким бы искусным ни был администратор. При нулевой задержке реакции на подготовку атаки хороший администратор не оставляет никаких шансов хакеру.

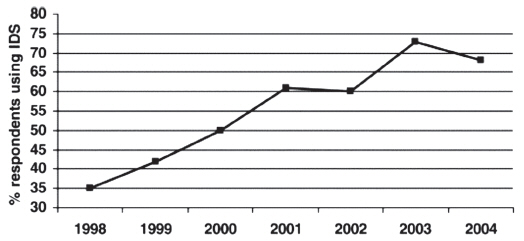
*Быстрая реакция на угрозу сокращает возможный ущерб не только для атакуемого объекта, но иногда и для всего Интернет сообщества (может сократиться число пораженных сетевых объектов)*.

Именно эти обстоятельства повышают интерес к системам *IPS* (*Intrusion* *Protection System*) или IMS (*Intrusion* Management system). В сетевом контексте можно считать, что такие системы комбинируют в себе свойства *IDS* и *Firewall*. В случае отдельной ЭВМ такая система мониторирует все системные и API-вызовы и блокирует те, которые могут нанести вред. Схема подключения *IDS* и *IPS* показана на [рис. 12.2](https://intuit.ru/studies/courses/1124/201/lecture/5221?page=3#image.12.2). Хотя *IPS* существуют уже несколько лет, применение их ограничено.



**Рис. 12.2.**Схема подключения IDS и IPS (IDS or IPS: what is best, Maria Papadaki and Steven Furnell, Network Security v2004, Issue 7, июль 2004, стр. 15-19)

*IDS* пригодна лишь для того, чтобы понять, насколько ситуация тревожна. Для улучшения положения нужны дополнительные действия. Положение *IDS* на рынке услуг демонстрирует [рис. 12.3](https://intuit.ru/studies/courses/1124/201/lecture/5221?page=4#image.12.3), из него видно, что интерес к *IDS* становится ограниченным (смотри также <http://www.nwfusion.com/newsletters/frame/2003/1013wan2.html> и <http://www.nwfusion.com/reviews/2003/1013idsalert.html>).



**Рис. 12.3.**Вариация числа используемых IDS по годам (та же статья, что и для рис. 12.2)

Так как *IPS* /IMS базируются на *IDS*, они наследуют все ее недостатки (нечувствительны к неизвестным сигнатурам атак, дают *ложные тревоги* и пр.). Эти системы блокируют лишь атаки, которые детектируются с высокой степенью достоверности. Кроме того, они требуют тонкой настройки высококвалифицированными администраторами. В случае отказа *IPS* (или успешной атаки) сеть или ЭВМ, которую она защищает, лишится доступа к внешней сети (см. [рис. 12.2](https://intuit.ru/studies/courses/1124/201/lecture/5221?page=3#image.12.2)).

Еще одной, достаточно новой угрозой является IM (*Instant Messaging*). Хотя большинство систем IM (*MSN*, Yahoo IM, *AIM* и др.) имеют стандартные номера портов, блокировать доступ для этого сервиса, закрыв эти порты, нельзя, так как системы могут воспользоваться другими номерами портов, например, 80, 23, 20 и т.д.. Возможно, некоторые читатели сталкивались с самопроизвольным появлением на экране их дисплея окна, приглашающего сыграть в "бесплатном" казино, — это одно из проявлений подобных атак. Некоторые пользователи могут полагать, что они в безопасности, так как не используют e-mail, но это не так. Для защиты от этого вида атак нужно специализированное программное обеспечение. К такому классу уязвимостей следует отнести и сервис ICQ.

Так как **беспроводные сети** находят все более широкое применение, а безопасность таких каналов оставляет желать лучшего, возможен перехват трафика с помощью средств типа *sniffer*. Высокой безопасности можно не получить даже в случае применения VPN и двухфакторной аутентификации (SecurID). Для хакера такие объекты атаки привлекательны тем, что им не нужно устанавливать соединение с каким-либо объектом в локальной сети, не оставляя следов в *Firewall* или *IDS*. Обычный просмотр WEB-страниц может помочь украсть индивидуальные параметры. Пользователи корпоративной сети при работе с WEB-страницами (просмотр требует аутентификации) могут получить уведомление: "Your connection to the network has been *lost* — please reenter your username and password" (Сетевое соединение разорвано, пожалуйста, введите еще раз ваше имя и пароль). Инициатором такого сообщения может быть злоумышленник, который рассчитывает получить ваши аутентификационные параметры. Беспроводные средства облегчают атаки и стационарных объектов. Клиент, купивший карту доступа, получает *динамический адрес*, и его локализацию и идентичность достаточно трудно установить. Существуют специальные средства для выявления приборов 802.11, например, Kismet или *Air* *Defense* (разновидность *IDS* ). Но такие средства используются как во благо, так и во вред: они могут помочь обнаружить плохо сконфигурированные точки доступа. Для таких сетей особенно актуальна проблема однозначной идентификации пользователя, где бы он ни находился. Обычно портативные ЭВМ после включения пытаются установить соединение с известными им беспроводными точками подключения (их число может превышать сотню), и атакер может сформировать точку доступа, имитирующую один из таких узлов, для установления соединения с данной ЭВМ и получения параметров доступа. В последнее время появились экраны, работающие по технологии стелз и способные экранировать радиоволны определенных частот. Это позволяет обезопасить беспроводные локальные сети, сохраняя работоспособность мобильных телефонов. Данная технология может помочь исключить интерференцию систем, работающих на идентичных частотах.

Если нет насущной потребности, следует дезактивировать вход USB на уровне BIOS (или setup). Заметной уязвимостью обладают все переносные ЭВМ. Человек, получивший к такой ЭВМ доступ, за несколько минут может установить новый пароль (с помощью загрузочного диска) и скопировать оттуда любую информацию или установить там троянского коня. Особую категорию составляют домашние ЭВМ. Многие компании одобряют работу своих сотрудников дома (экономится электричество, рабочее место и пр.), удобно это и работникам (экономится время в пути и бензин). При подключении к офисной сети предпринимаются достаточно серьезные меры безопасности, но эта же машина может использоваться детьми, подключающимися к самым разным сайтам, среди которых могут быть ЭВМ злоумышленников. При этом нет никакой гарантии, что в такую машину не попадет *троянский конь* или другая вредоносная программа. После же подключения к сети компании такая машина может стать *источником угрозы* для других ЭВМ локальной сети. Покидая рабочее место, целесообразно выйти из ОС (произвести процедуру *Logoff*), но все ли это делают? Поэтому после 30-60 сек пассивности ЭВМ должна сама выполнить эту процедуру. Многие компании в случае успешной сетевой атаки скрывают этот факт, чтобы сохранить доверие клиентов. Это приводит к тому, что число жертв увеличивается (такой же атаке подвергаются другие, не предупрежденные об угрозе).

Сигнатуры современных атак могут быть достаточно изощренными. Это может быть не просто попытка установить соединение с определенным портом, а вполне определенная последовательность попыток соединений, приводящая к соединению. Это характерно для доступа к некоторым люкам, специально оставленным хакером в какой-то программе. Такая схема исключает детектирование окон уязвимости простым поиском открытых портов (так работают некоторые программы поиска вторжений). Подробности этой техники смотри по адресу [http://www.portknocking.org](http://www.portknocking.org/).

Наибольшую угрозу представляют атаки с помощью программ, специально написанных для вторжения в конкретную ЭВМ или сеть. К сожалению, большинство разработчиков приложений не учитывает требования безопасности. Сертификация программ, как правило, не включает в себя аспект безопасности (попыток вторжения). Следует разделять уязвимости "врожденные" и специально созданные хакером. Эти два вида бывает трудно отличить, если вы покупаете нелегальное программное обеспечение. Хороший хакер готовит вторжение, начиная с тщательной разведки объекта атаки. Это не обязательно сканирование или попытки подбора пароля. Такую информацию хакер может получить из описаний разработанных на сервере-мишени программных продуктов (требования к ОС, версии и т.д.) Он может послать запросы на серверы *Whois*, посылая команды finger или почтовому серверу и пр. В отдельности такие запросы не говорят ни о чем. Но, если собирать статистику о клиентах сети (используемые запросы, ping, *traceroute*, сканирования определенных портов и т.д.), то по совокупности этих данных можно с приемлемой вероятностью прогнозировать угрозу.

При стратегическом планировании в сфере сетевой безопасности следует учитывать тенденцию в направлении распределенных систем и более широкого внедрения беспроводных систем. Оба эти фактора значительно усложняют решение проблем.

**Основные уязвимости**

Начинать следует с выявления возможно намеренных или случайных уязвимостей:

1. процессора ЭВМ;
2. BIOS, контроллеров внешних устройств, интерфейсов и пр.;
3. программного обеспечения ОС;
4. прикладного программного обеспечения, включая программы защиты;
5. программного обеспечения аппаратных сетевых устройств и систем аутентификации;
6. сетевых протоколов и их программных реализаций.

Первые два пункта крайне важны, именно с обеспечения неуязвимости этих объектов следовало бы начинать разработку комплексной системы безопасности. К сожалению, это пока не достижимо *по* финансовым и технологическим причинам.

Несколько слов о методах противодействия. Большинство наиболее серьезных атак предполагают две фазы:

1. исследование будущего объекта вторжения (определение типа и версии ОС, перечня загруженных приложений, максимально возможная информация о пользователях и т.д.);
2. собственно вторжение (ему может предшествовать многодневное создание программы, использующей известные или специально для этого случая найденные слабости программного обеспечения атакуемого).

В этом случае, если зафиксирована *активность* первой фазы, надо, не дожидаясь второй, перекрыть *доступ* с выявленного IP-адреса (хотя это и не гарантирует безопасности, так как *хакер* может варьировать свой IP-*адрес*) и, если возможно, перекрыть *доступ* *по* используемому хакером порту.

Существует несколько классов атак реального времени (посылка одного или нескольких пакетов блокирует работу ЭВМ) — это большинство *DoS-атак* и некоторое число атак-хулиганств, использующих обнаруженные ошибки программ: например, ICMP-пинг пакетом, *длина* которого проставлена равной 65536 *байт*, хотя его реальная *длина* во много раз меньше, *атака* типа Teardrop, атаки с неверной фрагментацией пакетов или некорректными заголовками и т.д. Для противодействия этим атакам нет универсальных средств; в одном случае это *конфигурирование* входного шлюза (маршрутизатора), в другом – своевременное обновление версии ОС или драйверов (например, баз данных). Но большинство известных атак такого типа уже не представляют опасности, так как найдены средства их нейтрализации. Не следует, впрочем, расслабляться, могут обнаружиться новые уязвимости такого рода. Следует относиться к этим атакам достаточно серьезно, так как они могут являться частью сценария вторжения (например, DoS-атаки часто используются для перехвата ТСР-соединения).

Здесь уместно отметить достаточно типичную ситуацию. Изобретение или обнаружение хакером уязвимости, *регистрация* этого факта жертвами и разработка средств противодействия отстоят друг от друга на месяцы. Это временное окно представляет наибольшую опасность. Именно в такой ситуации *IDS*, *регистрирующая аномалии*, может оказаться наиболее эффективной.

*Оптимальным решением для эффективной системы IDS* *является сочетание сигнатурного анализа и поиска аномалий, например, с привлечением техники нечеткой логики (Fuzzy Logic)*.

*Безопасность* — комплексное понятие: это и ограничение нежелательного доступа, и сохранность информации, и живучесть самой сети. Актуальность проблемы подтверждает количество RFC-документов, опубликованных за последнее время [1-14, 18] *по* данной тематике (см. библиографию в конце данного раздела).

Точкой уязвимости могут быть загружаемые через *сеть* рабочие станции или Х-терминалы. Процедура загрузки предполагает использование *протоколов RARP*, *TFTP* и *BOOTP*. Все они практически не имеют сколько-нибудь серьезной защиты. Наиболее уязвим протокол *RARP*. Здесь желательно позаботиться о том, чтобы *номер порта* *UDP* выбирался ЭВМ, осуществляющей загрузку, случайным образом. В противном случае *хакер* может легко перехватить процедуру обмена и загрузить нужную ему конфигурацию программного обеспечения, обеспечив себе широкие ворота для проникновения. *BOOTP* предлагает дополнительные возможности защиты в виде 4-байтного случайного кода идентификатора процедуры ( *transaction ID* ). Это весьма мешает хакеру прервать процедуру и инициировать новую сессию загрузки ( *rebooting* ). Должны быть предприняты все меры, чтобы начатая процедура загрузки была своевременно завершена. Пребывание системы в промежуточном состоянии заметно облегчает разнообразные атаки.

Но даже *Firewall* не может предотвратить атаки со стороны хакеров, работающих внутри локальной сети. Здесь к их услугам огромный арсенал. Это, прежде всего, использование сетевого интерфейса для приема всех пакетов, следующих *по* сегменту (6-ой режим работы интерфейса), а также программные продукты типа tcpdump, *sniffer* или Etherfind. Такой режим легко позволяет перехватывать незашифрованные пароли, определять используемые номера портов или *ISN* (при этом *хакер* остается невидимым). К счастью, такой комфорт для хакера предоставляется лишь в пределах его логического сегмента, что стимулирует использование мостов, переключателей и локальных маршрутизаторов, которые ограничивают зону, где *хакер* может осуществлять перехваты. *По* этой же причине рекомендуется авторизованным администраторам работать с консоли, а не c удаленного терминала.

Еще одним инструментом взлома может оказаться протокол *ARP*. *Хакер* может послать большое число широковещательных запросов, содержащих несуществующий IP-*адрес*. ЭВМ при получении такого запроса должна его обработать и может попытаться его переадресовать какому-то серверу. Всё это уже само *по* себе нежелательно, так как порождает большой паразитный трафик. Помимо этого *хакер* может попытаться послать широковещательный отклик, сообщая свой MAC-*адрес* в качестве адреса места назначения. Это может при определенных условиях предоставить возможность перехвата трафика между ЭВМ, пославшей первичный *запрос*, и истинным узлом назначения. Таким образом, постоянный *мониторинг* широковещательных запросов следует считать одной из составных частей системы безопасности локальной сети (см. также Robert T. Morris, A *Weakness* in the 4.2bsd Unix *TCP/IP* *Software*, *Computer* *Science* *Technical Report* N 117, at &t *Bell laboratories*), тем более, что такой *мониторинг* не порождает дополнительного трафика.

Следует учитывать, что в случае предоставления сервером нескольких услуг сложность обеспечения безопасности может расти экспоненциально. Фильтрующие маршрутизаторы для поддержания новых протоколов должны быть модифицированы. Некоторые протоколы в действительности трудно фильтровать безопасным образом (например, услуги *RPC* и *UDP*), и при фильтрации появляется больше окон уязвимости внутренней сети. Услуги, предоставляемые на той же машине, могут взаимодействовать катастрофическим образом. Например, разрешение анонимного *FTP* на некоторой машине, которая выполняет функцию WWW-сервера, может позволить атакеру записать в область анонимного *FTP* некоторый *файл*, после чего запустить его посредством HTTP-сервера.

Определенного успеха в деле повышения защиты сети можно добиться, используя ограничения допуска. Маршрутизаторы и ЭВМ, имеющие *контроль доступа*, сверяют *адрес* отправителя запроса со списком доступа. Если *адрес* содержится в разрешительном списке, *доступ* реализуется, в противном случае *запрос* отвергается. Повторные попытки доступа с адресов, не содержащихся в разрешительном списке, следует рассматривать как атаки. Не следует игнорировать требования к безопасности систем *SNMP*. Желателен переход на версию 3.

Странная *активность* в системе в необычное время суток, в необычные дни или с неизвестного удаленного терминала должна вызывать пристальное внимание.

*Реальное число различных сигнатур атак давно перевалило за 2500*.

Дополнительные данные можно найти на сервере <http://book.itep.ru/6/intrusion.htm>.