Только атаки дилетантов нацелены на машины. Атаки профессионалов нацелены на людей.

Б. Шнайер

## Компьютерная и информационная безопасность

### Компьютерная и информационная безопасность

***Компьютерная безопасность*** — меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет). Поле деятельности системных администраторов охватывает все процессы и механизмы, с помощью которых цифровое оборудование, информационное поле и услуги защищаются от случайного или несанкционированного доступа, изменения или уничтожения данных, и приобретает всё большее значение в связи с растущей зависимостью от компьютерных систем в развитом сообществе.

***Информационная безопасность*** — это процесс обеспечения конфиденциальности, целостности и доступности информации. Конфиденциальность: обеспечение доступа к информации только авторизованным пользователям. Целостность: Обеспечение достоверности и полноты информации и методов ее обработки. Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Зачастую, люди путают эти два понятия. Внесём ясность.

***Компьютерная безопасность*** - это безопасность компьютера, его программного обеспечения, информации, заложенной в нём. Она связана конкретно с компьютерами и техникой. А ***информационная безопасность*** - это защищенность информационных ресурсов (документов и массивов документов какой-либо организации, например), а также защита прав личности и государства в информационной сфере (например, от разглашения гос. тайн или от пиратства) и много чего другого.

На самом деле, если рассуждать строго, ***компьютерная безопасность*** - это меры, направленные на исключение нарушения работоспособности компьютера (или компьютеров) или управления компьютером (или компьютерами) сторонними лицами. Доступ к компьютеру злоумышленника ещё не означает кражу информации. Информация может быть зашифрована или находиться на недоступном для злоумышленника носителе. ***Специалист по информационной безопасности*** работает в конкретном направлении, составляя нечто подобное плану защиты информации, воплощают это в жизнь как правило уже другие люди, в зависимости от распределения обязанностей организации. ***Специалист по компьютерной безопасности*** это частный случай ***специалиста по информационной безопасности***. Чаще всего тот, кто занимается вопросами компьютерной безопасности, он же их и воплощает в жизнь, поэтому ***специалист по компьютерной безопасности*** - больше теоретик, ***по информационной*** – практик.

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач. ­­­­­­­­­

В силу развитых технологий не стоит безответственно относиться к своим личным данным, цифровым данным, которые при определённых обстоятельствах оказывают влияние на нашу судьбу.  Уже ни для кого не секрет, что электронные девайсы, которыми пользуется человек в современном мире для передачи информации, подвержены многим уязвимостям, а также и они сами и информация представляют огромный интерес для злоумышленников и правительств.

Аргумент "мне нечего скрывать" не считается весомым, так как даже с первого взгляда безобидная информация может поведать о каждом конкретном индивидууме многое: личные предпочтения, круг общения, перемещения и прочие вещи, которые в умелых руках могут стать отличным инструментом для достижения тех или иных целей в отношении этого индивидуума.

Ну и по поводу размещения информации в сети интернет. Не выкладывайте свои личные данные, никаких фотографий, никакой привязки аккаунтов к реальному вашему номеру телефона (для этого существуют сервисы подобные этим: **http://receivesmsonline.com/** **http://www.vsms24.com/web/index.php**), никакой установки игровых клиентов на компьютер с важными данными и никакой серьёзной переписки в чатах этих онлайн-игр. (Но следует помнить и о том, что спецслужбы при необходимости могут сохранять коммуникации на том лишь основании, что они зашифрованы, а затем хранить зашифрованное сообщение вечно или по крайней мере до тех пор, пока его не расшифруют. О незашифрованных данных известно, что все логи посещений сайтов сохраняются, а система СОРМ может записывать ваш незашифрованный трафик.)

### Уничтожение и шифрование данных

Также необходимо помнить о безвозвратном удалении следов информации с жёсткого диска, для чего целесообразнее применять CCleaner, PrivaZer, wipefile. И вот ещё список того, что желательно уничтожать:

*Информация на компьютере:*

* **Неиспользуемые пароли и данные к аккаунтам.** Удалить невосстанавливаемым программным методом.
* **Закладки в браузере.** Внимательно просмотреть и выявить все ненужное.
* **Браузеры.** Очистить всю историю и любые другие данные, сохраненные сайтами.
* **Неиспользуемые контакты.** Просмотреть и удалить неиспользуемые контакты: icq, jabber, skype, другие im-приложения, почтовые программы и сервисы.
* **Связка gpg-ключей.** Просмотреть все связки и удалить неиспользуемые, забытые и неизвестные публичные и секретные ключи.
* **Сообщения.** Удалить ненужные и старые сообщения в почтовых программах, icq, jabber-клиентах, skype и прочих программах обмена сообщениями.
* **Документы.** Просмотреть папки хранения документов — старые, неиспользуемые и ненужные удалить невосстанавливаемым программным методом.
* **Бекапы.** Просмотреть места хранения бекапов и удалить старые невосстанавливаемым программным методом.
* **Скачанное.** Очистить локальную папку для скачивания файлов.
* **Неиспользуемое свободное место на дисках.** Для очистки использовать программы Ccleaner и Bleachbit.
* **Пароли.** Решить, где лучше сменить пароли.

*Интернет:*

* "**Личка".** Просмотреть все посещаемые форумы и остальные социальные сервисы и удалить все личные сообщения.
* **Сообщения.** Удалить старые и ненужные сообщения в почтовых сервисах.

*Средства общения, мобильные компьютеры*

* **Контакты.** Пройтись по контактам в телефонах и удалить ненужные.
* **Сообщения.** Удалить все СМС и другие сообщения на смартфоне/планшете.
* **Документы.** Найти и удалить ненужные и забытые документы и книги на смартфоне/планшете.
* **Закладки в браузере.** Внимательно просмотреть и выявить все ненужное.
* **Браузеры.** Очистить всю историю и любые другие данные, сохраненные сайтами.
* **Неиспользуемые контакты в im-приложениях**. Просмотреть и удалить неиспользуемые контакты: icq, jabber, skype, другие im-приложения, почтовые программы и сервисы.
* **Приложения.** Выявить и удалить старые и ненужные приложения, а также информацию, оставленную ими.
* **Пароли.** Решить, где лучше сменить пароли.

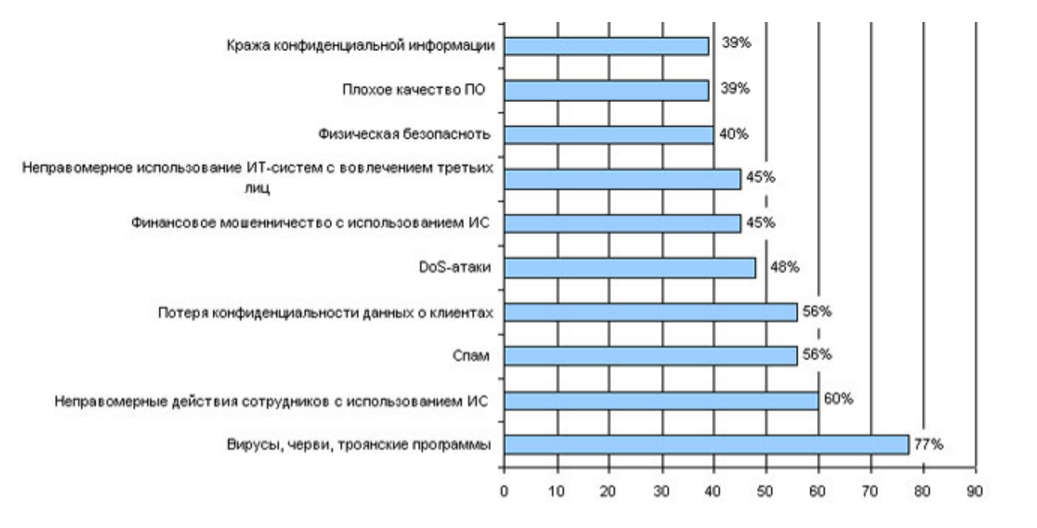
*Материальное*

* **Флешки и другие носители информации.** Проверить все носители информации в пределах досягаемости и уничтожить (разломать, сжечь и т.п.) информацию на них по своему усмотрению.
* **Телефоны, модемы, Wi-Fi модули и другие средства коммуникации.** Использованные, старые, ненужные и по-другому "засвеченные" средства коммуникации физически сломать и выбросить минимум в трех кварталах (километрах) от их местоположения.
* **СИМ-карты.** Выявить и уничтожить (разломать, сжечь и т.п.) все забытые и неиспользуемые СИМ-карты и другие карты доступа.
* **Документы.** Выявить ненужные и забытые документы, записки, заметки, записные книжки и уничтожить (лучше сжечь).

Желательно "не оставлять следов": использование кредитных карт, мобильных телефонов даёт возможность отследить ваше передвижение, покупки, контакты. Нужно иметь в виду, что каждое использование компьютера также оставляет следы.

Также следует упомянуть о необходимости шифрования данных. Ведь оно защищает нашу частную информацию и анонимность. Эта защита важна для каждого. Более того, в последние годы вопрос конфиденциальности в сети становится очень актуальным, учитывая сканирование наших электронных писем. Сегодня самым известным и простым алгоритмом, который используется в системах защиты информации организаций и предприятий, является DES (Data Encryption Standart). Он необходим для защиты от незаконного доступа к важной информации в организациях. Особенности алгоритма DES — используется ключ длиной 56 бит; зашифровать можно сообщение с помощью одной программы, а расшифровать — используя любую другую программу, соответствующую DES; высокая скорость обработки достигается за счёт несложного алгоритма и высокой стойкости. Data Encryption Standart подходит для шифрования и аутентификации данных.

### Угрозы безопасности информационных систем

Известны следующие источники угроз безопасности информационных систем:

### Средства защита информации от несанкционированного доступа

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур: *идентификация, аутентификация* и *авторизация*.

**Идентификация** - присвоение пользователю (объекту или субъекту ресурсов) уникальных имен и кодов (идентификаторов).

**Аутентификация** - установление подлинности пользователя, представившего идентификатор или проверка того, что лицо или устройство, сообщившее идентификатор является действительно тем, за кого оно себя выдает. Наиболее распространенным способом аутентификации является присвоение пользователю пароля и хранение его в компьютере.

**Авторизация** - проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними. Авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам.

### Защита информации в компьютерных сетях

Локальные сети предприятий очень часто подключаются к сети Интернет. Для защиты локальных сетей компаний, как правило, применяются межсетевые экраны - брандмауэры (firewalls). Экран (firewall) - это средство разграничения доступа, которое позволяет разделить сеть на две части (граница проходит между локальной сетью и сетью Интернет) и сформировать набор правил, определяющих условия прохождения пакетов из одной части в другую. Экраны могут быть реализованы как аппаратными средствами (различные устройства, системы, платформы), так и программными.

Межсетевой экран, сетевой экран, файрвол или брандмауэр — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита сети или отдельных её узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

#### Проблемы, не решаемые фаерволом

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

* не защищает узлы сети от проникновения через «люки» (англ. back doors) или уязвимости ПО;
* не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
* не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, *антивирусы*.

Но зачем Linux антивирус нужен вообще, ведь она практически не подвержена вирусным атакам? А ответ очень прост: многие линуксоиды пользуются не только Linux, но ставят, или оставляют на компьютере, второй системой Windows. Поэтому антивирус нужен, чтобы сканировать раздел Windows, когда она не работает, на возможность заражения. Многие вирусы могут легко прятаться от антивируса, но их намного легче обнаружить именно тогда, когда Windows спит. Именно так поступаю некоторые антивирусы в Windows: они перезагружают Windows и начинают её сканировать перед загрузкой. Но даже если у вас не стоит второй системой Windows, вам может потребоваться Linux антивирус, чтобы не стать разносчиком вирусов. Простая ситуация: вы взяли у друга флешку, скопировали нужные вам файлы, а в них вирус. Вам хоть бы что, и это здорово. Но вы передаёте эти файлы третьему человеку, у которого Windows, и заражаете его этими вирусами. Ну и третий вариант - это сервер, на котором стоит Linux. Но вот в офисе все работают на Windows, и вам просто необходимо мониторить интернет трафик на наличие вирусов. И в этом случае Linux антивирус хорошее решение, так как он может прекрасно работать в режиме командной строки.

Считается, что Unix-системы намного лучше защищены от компьютерных вирусов, в сравнении с операционными системами Windows. В принципе, до сих пор нет ни одного широко распространенного вируса для Linux, в то время как в среде Windows просто кишит всякой заразой. в Linux очень быстро исправляют уязвимости.

Существует мнение, что вирусов на Linux мало потому, что его доля на рынке операционных систем крайне мала, поэтому и создают вирусы для Windows, из-за его большой популярности и распространенности. Будь Linux популярнее, и для него так же написали бы кучу вирусов. Но это не так. Если взять самое популярное программное обеспечение для web-серверов, то это будет Apache. По состоянию на 2013 год доля Apache на web-серверах составляет почти 45%, а доля IIS от Microsoft — 23.10% рынка. Из этого следует, что атаки хакеров должны быть активнее к большему числу интернет-ресурсов на Apache, и должно наблюдаться больше червей, вирусов и других вредоносных программ, которые будут нацелены на Apache и те операционные системы, под управлением которых он работает, чем на Windows и IIS. Но в жизни дела обстоят иначе. Уже много времени целью для сетевых червей и всевозможных атак есть IIS от Microsoft.

#### Основные достоинства Linux, в плане безопасности:

* для \*nix-платформ создано крайне мало вирусов;
* существует большое количество разных Linux-дистрибутивов. Одни работают с .deb пакетами, другие с .RPM пакетами. Создание вируса, который будет одинаково хорошо работать во всех из них очень затруднительно;
* в разных дистрибутивах по умолчанию инсталлированы разные наборы, по-разному скомпилированного программного обеспечения, что также уменьшает вероятность массового заражения вирусом;
* программы, которые скачаны из интернета, в Linux по умолчанию не являются исполняемыми. Сперва их нужно сделать таковыми;
* главным источником ПО в Linux являются проверенные (официальные) репозитории. Это дает право утверждать, что вероятность попадания вирусов в эти источники крайне мала.

### Криптографическая защита информации

Для обеспечения секретности информации применяется ее шифрование или криптография. Для шифрования используется алгоритм или устройство, которое реализует определенный алгоритм. Управление шифрованием осуществляется с помощью изменяющегося кода ключа.

Извлечь зашифрованную информацию можно только с помощью ключа. Криптография - это очень эффективный метод, который повышает безопасность передачи данных в компьютерных сетях и при обмене информацией между удаленными компьютерами.

### Электронная подпись

Для исключения возможности модификации исходного сообщения или подмены этого сообщения другим необходимо передавать сообщение вместе с электронной подписью. Электронная цифровая подпись - это последовательность символов, полученная в результате криптографического преобразования исходного сообщения с использованием закрытого ключа и позволяющая определять целостность сообщения и принадлежность его автору при помощи открытого ключа.

Другими словами, сообщение, зашифрованное с помощью закрытого ключа, называется электронной цифровой подписью. Отправитель передает незашифрованное сообщение в исходном виде вместе с цифровой подписью. Получатель с помощью открытого ключа расшифровывает набор символов сообщения из цифровой подписи и сравнивает их с набором символов незашифрованного сообщения.

При полном совпадении символов можно утверждать, что полученное сообщение не модифицировано и принадлежит его автору.

Целью применения систем цифровой подписи является аутентификация информации - защита участников информационного обмена от навязывания ложной информации, установление факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений. Система цифровой подписи предполагает, что каждый пользователь сети имеет свой секретный ключ, который используется для формирования подписи, а также соответствующий этому секретному ключу открытый ключ, известный некоторому кругу пользователей сети и предназначенный для проверки подписи. Цифровая подпись вычисляется на основе секретного ключа отправителя информации и собственно информационных бит документа (файла). Один из пользователей может быть избран в качестве "нотариуса" и заверять с помощью своего секретного ключа любые документы. Остальные пользователи могут провести верификацию его подписи, то есть убедиться в подлинности полученного документа. Способ вычисления цифровой подписи таков, что знание открытого ключа не может привести к подделке подписи. Проверить подпись может любой пользователь, имеющий открытый ключ, в том числе независимый арбитр, который уполномочен решать возможные споры об авторстве сообщения (документа).

### Защита информации от компьютерных вирусов

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных и распространяться по каналам связи.

Существует несколько классификаций компьютерных вирусов:

1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.
2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.
3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные.
4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

**Загрузочные вирусы** заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.

**Резидентные вирусы** загружается в память компьютера и постоянно там находится до выключения компьютера.

**Самомодифицирующиеся вирусы (мутанты)** изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

**Стелс-вирусы (невидимки)** перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

**Троянские вирусы** маскируют свои действия под видом выполнения обычных приложений.

Троянская программа — вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и её передачу злоумышленнику, её разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Существуют Password Trojans. Эти трояны находят на вашем компьютере пароли и отправляют их хозяину. Нет разницы, какой пароль, будь то интернет пароль, пароль от почтового ящика, этот троян найдет все эти пароли.

Keyloggers трояны очень просты в использовании. Они записывают все, что было набрано на клавиатуре (включая пароли) в файл и впоследствии отправляют это все по электронной почте хозяину. Keylogger-ы обычно занимают мало места, и могут маскироваться под другие полезные программы, из-за чего их бывает трудно обнаружить. Некоторые трояны этого типа могут выделять и расшифровывать пароли, найденные в специальных полях для ввода паролей. Обычно информация с паролями отсылается хозяину трояна по электронной почте.

Одним из самых эффективных методов защиты от кейлоггеров является использование виртуальной клавиатуры. Не стоит спешить прибегать к помощи виртуальной клавиатуры, встроенной в Windows. Эта программа не предназначена для защиты от кейлоггеров. Подобного рода виртуальные клавиатуры не защищены от считывания информации, набираемой на них. В данном случае нужна специально разработанная виртуальная клавиатура, наподобие той, что входит в состав продуктов Лаборатории Касперского. Наличие виртуальной клавиатуры в программах данной лаборатории подтверждает факт сложности обнаружения кейлоггеров. В настоящее время в большинстве серьезных банков используются виртуальные клавиатуры для защиты своих клиентов от кражи вводимой информации при доступе к интернет-банкинг системам. Новое бесплатное приложение Oxynger KeySheild позволяет защитить данные от передачи хакерам без ведома пользователя. Оно реализовано в форме виртуальной клавиатуры, помогающей безопасно вводить критически важную информацию и таким образом избегать необходимости использовать аппаратную клавиатуру, за которой, возможно, следят кейлоггеры.

Современные кейлоггеры умеют соотносить клавиатурный ввод с текущим окном и элементом ввода. Многие из них умеют отслеживать список работающих приложений, делают “фото” экрана по заданному расписанию или событию, шпионят за содержимым буфера обмена, скрытно следить за пользователем. Вся собранная информация сохраняется на диске, а затем записывается в Log-файл – что-то вроде журнала регистрации, данные могут быть переданы по электронной почте или http/ftp-протоколу. Как заявляет разработчик виртуальной клавиатуры Oxynger KeySheild, программа обезопасит пользователя от шпионского программного обеспечения и троянов за счет запрета регистрации, входа в личный кабинет и тому подобного ввода критически важных данных при помощи клавиатуры, мыши, буфера обмена и экранных действий. Специальная функция блокирования скриншотов дает возможность отменять экранные снимки на таких уязвимых для информации этапах. Еще один интересный факт об Oxynger KeySheild – возможность полностью осуществлять ввод данных без помощи мыши. Для каждой инсталляции своего экземпляра программа использует различные раскладки клавиатуры. Поскольку стандартная раскладка QWERTY давно уже не является серьезным барьером для киберпреступников, Oxynger предоставляет уникальную организацию клавиш для каждой отдельной копии программного обеспечения, что в итоге оборачивается большой головной болью для хакеров.

Разумеется, приложение Oxynger KeySheild не предназначено для ежедневного использования в рамках работы с большими объемами данных на клавиатуре. Программа нацелена на ситуации, когда пользователю требуется ввести какую-либо конфиденциальную информацию: номер карты или счета, к примеру.

Подобрать пароли от различных аккаунтов можно с помощью фишинга — это популярный способ получения информации от беспечных пользователей. Хакеры присылают письма, которые по внешнему виду очень похожи на настоящие ресурсы и просят пользователя якобы заново ввести логин и пароль к своей учетной записи. Еще один пример фишинговых писем — это маскировка "зловредов" под отправленные документы. Правда никаких документов на самом деле в письме нет, а вместо документов в письмо вложена GIF-картинка со ссылкой на сайт для выманивания паролей.

Открывает список необычных компьютерных вирусов червь P2PShared.U. Этот вредоносный код распространялся с помощью почтовых сообщений с темой: "McDonalds желает Вам счастливого Рождества!". В сообщении речь шла о купоне, дающем право на бесплатный обед в McDonald’s. Но именно купон и являлся носителем вредоносного кода.

BatGen.D, испанский шеф-повар. Этот вредоносный код – специалист в области приготовления вредоносных закусок на любой вкус. Он попадает на компьютеры в виде файла под названием “personalcake.bat”. На деле он представляет собой инструмент для создания вредоносного программного обеспечения, который затем спрашивает у пользователя, каким именем он бы хотел назвать творение.

На седьмом месте расположился вредоносный код Aidreden.A. После заражения компьютера на экран выводится сообщение: "Вы умрете в следующем месяце". Таким образом Aidreden.A пытается убедить пользователя в том, что его компьютер якобы заражен вирусами, после чего предлагает загрузить фальшивый антивирус. Представляет собой обыкновенное окошко с кнопкой ОК. Потом открывает страницу Microsoft Security Center и предлагает скачать антивирус.

Все современные вирусы не пишутся наобум, нужно написать такой, который хорошо прячется, модифицируется, еще лучше если дальше распространяется и умеет выполнять какую-то работу, а не просто спалить видеокарту.

Поэтому при ответе на вопрос, на каком языке написать вирус, правильным ответом будет: на том, котором знаете. Ведь что такое вирус? Это программа, которая работает с определенными тонкостями системы. На каком языке можно сделать программу - теоретически на любом. Есть тонкости: что-то на одном проще, что-то на другом, вот и вся разница. Не рекомендуется писать на Ассемблере, так как тяжело получить доступ к каким-либо API.

### DoS-атаки

DoS (от англ. Denial of Service — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа "отказ в обслуживании"). В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик. Последняя проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищённой крупной компании или правительственной организации. Особенностью данного вида компьютерного преступления является то, что злоумышленники не ставят своей целью незаконное проникновение в защищенную компьютерную систему с целью кражи или уничтожения информации. Цель данной атаки - парализовать работу атакуемого веб-узла.

Схематически DDoS-атака выглядит примерно так: на выбранный в качестве жертвы сервер обрушивается огромное количество ложных запросов со множества компьютеров с разных концов света. В результате сервер тратит все свои ресурсы на обслуживание этих запросов и становится практически недоступным для обычных пользователей. Циничность ситуации заключается в том, что пользователи компьютеров, с которых направляются ложные запросы, могут даже не подозревать о том, что их машина используется хакерами. Программы, установленные злоумышленниками на этих компьютерах, принято называть "зомби". Известно множество путей "зомбирования" компьютеров: от проникновения в незащищенные сети, до использования программ-троянцев. Пожалуй, этот подготовительный этап является для злоумышленника наиболее трудоемким. Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую архитектуру, которую называют "кластер DDoS". Такая иерархическая структура содержит:

* управляющую консоль (их может быть несколько), т.е. именно тот компьютер, с которого злоумышленник подает сигнал о начале атаки;
* главные компьютеры. Это те машины, которые получают сигнал об атаке с управляющей консоли и передают его агентам-"зомби". На одну управляющую консоль в зависимости от масштабности атаки может приходиться до нескольких сотен главных компьютеров;
* агенты - непосредственно сами "зомбированные" компьютеры, своими запросами атакующие узел-мишень.

Другая опасность DDoS заключается в том, что злоумышленникам не нужно обладать какими-то специальными знаниями и ресурсами. Программы для проведения атак свободно распространяются в Сети. Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределённых бот-сетей.

### Защита от основных видов DoS-атак

В основном защита от DoS-атак строится на правильной настройке компьютера. Следующие меры защиты способны защитить лишь от слабых DoS-атак, либо они будут использоваться в качестве снижения её эффективности.

Также есть несколько универсальных советов, которые помогут подготовить систему к DoS-атаке:

* Все серверы, которые имеют доступ во внешнюю сеть, должны быть подготовлены к удаленной аварийной перезагрузке. Также желательно наличие второго сетевого интерфейса, через который по ssh-соединению можно быстро получить доступ к серверу.
* Программное обеспечение, которое установлено на сервере, должно быть в актуальном состоянии, а именно: должно быть установлено последнее ПО, касающееся обеспечения безопасности системы.
* Все сетевые сервисы должны быть защищены брандмауэром.

Полностью защититься от DDoS-атак на сегодняшний день невозможно, так как совершенно надёжных систем не существует. Здесь также большую роль играет человеческий фактор, потому что любая ошибка системного администратора, неправильно настроившего маршрутизатор, может привести к весьма плачевным последствиям. Однако, несмотря на всё это, на настоящий момент существует масса как аппаратно-программных средств защиты, так и организационных методов противостояния.

### Хакерство

Как ни крути, а информационная безопасность у многих прочно ассоциируется с хакерами. В наши дни под хакером понимается злоумышленник, который делает что-то нелегальное, взламывает какие-то системы с материальной выгодой для себя. Но это далеко не всегда было так.

Вернемся на полвека назад, в 1960-е годы, когда ЭВМ постепенно стали проникать в нашу жизнь. Хакерство началось еще тогда, с попыток использовать технику не по назначению. Например, чтобы запустить на ней нами же написанную игру. В те времена понятие "хакер" — это очень увлеченный человек, пытающийся сделать с системой что-то нестандартное. Доступ к компьютерам ведь был в основном у сотрудников университетов, причем процессорного времени каждому выделялось не так уж много. Позволялось поработать с вычислительной машиной всего несколько часов в неделю, по строгому расписанию. Но даже в таких условиях людям удавалось выкраивать время на эксперименты. Хакерам того времени было интересно не просто решить какую-то вычислительную задачу, они хотели понять, как устроена и работает машина. Культура хакерства вышла из очень увлеченных людей.

В 70-е хакерство окончательно сформировалось как попытка "поиграть" с информационной системой, обходя ее ограничения. Интернета тогда еще не было, но уже была телефония. Поэтому появилось такое явление как фрикинг (сленговое выражение, обозначающее взлом телефонных автоматов, телефонных сетей и сетей мобильной связи, с использованием скрытых от пользователя или недокументированных функций. Обычно фрикинг осуществляетс для бесплатных звонков, пополнения личного мобильного счета.). Отцом фрикинга считается Джон Дрейпер, известный под ником "Капитан Кранч". Однажды он нашел в пачке кукурузных хлопьев "Captain Crunch" подарок — свисток. Телефонные линии в то время были аналоговыми и телефонные аппараты общались друг с другом посредством обмена тоновыми сигналами. Оказалось, что тональность обнаруженного Дрейпером свистка совпадает с тоном, используемым телефонным оборудованием для передачи команд. Фрикеры стали при помощи свистков эмулировать систему команд и бесплатно дозванивались из уличных телефонов в соседние города и штаты. Следующим шагом стало создание Стивеном Возняком и Стивом Джобсом "blue box" — аппарата, эмулировавшего все те же тоновые команды. Он позволял не только дозваниваться до нужных номеров, но и пользоваться секретными служебными линиями. Подав сигнал на частоте 2600 Гц можно было перевести телефонные системы в административный режим и дозвониться на недоступные обычному человеку номера, например, в Белый Дом. Развлечение продолжалось до конца 80-х, когда в популярной газете была опубликована большая статься о "blue box", которая привлекла к фрикерам внимание полиции. Многие фрикеры, в том числе и сам Дрейпер, были арестованы. Позже все же удалось разобраться, что делали они это все не ради денег, а скорее из спортивного интереса и баловства. В то время в уголовном кодексе просто не существовало никаких статей, относящихся к мошенничеству с информационными системами, так что вскоре все фрикеры были отпущены на свободу.

В 80-е годы слово "хакер" впервые получило негативный оттенок. В сознании людей уже стал формироваться образ хакера как человека, который может делать что-то незаконное для получения прибыли.

##### Кевин Митник

Как и его предшественники, Кевин Митник начал заниматься хакерством, вторгаясь в телефонные линии. В 1981 году семнадцатилетний Кевин со своим другом взломал телефонную станцию Computer System for Mainframe Operations (COSMOS), принадлежащую компании Pacific Bell в Лос-Анджелесе. Вторгшись в систему, он переключал телефонные линии и перехватывал все звонки, идущие через эту станцию. Абоненты вскоре начали жаловаться, списывая это на ошибки и розыгрыши операторов. Кевин Митник, разумеется, отвечал на звонки сам, иногда при этом отмачивая бестактные шутки.

Но Митник на этом не остановился: он продолжал влезать в систему компании Pacific Bell и её COSMOS. Хакер сумел войти в базу данных компании и украсть информацию о нескольких абонентах. Он с лёгкостью получил доступ к телефонным счетам, паролям, комбинациям шлюзов и даже к системному руководству. Митник даже использовал переключение телефонных линий для своих личных нужд. В конце концов, один из сотрудников Pacific Bell обнаружил нарушения в системе COSMOS. Было начато расследование, которое быстро привело к телефонной будке, используемой Кевином Митником для звонков и доступа к сети; оставалось только дождаться, когда появится преступник и поймать его с поличным. Приговор суда был мягким: Митника обвинили в порче данных и краже и приговорили к трём месяцам отбывания наказания в исправительном учреждении и дали один год испытательного срока.

Самый большой успех пришёл к Кевину Митнику в 1983 году, когда он совершил поистине впечатляющее деяние. В то время он был студентом южнокалифорнийского университета. Используя один из университетских компьютеров, возможно, TRS-80 с 1,77-МГц процессором Zilog, Митник проник в глобальную сеть ARPANet, являющуюся предшественницей Internet, которая в то время была предназначена для военных целей и объединяла крупные корпорации и университеты. Проникнув в эту сеть, Митник добрался до самых защищённых компьютеров того времени, до компьютеров Пентагона. Он получил доступ ко всем файлам Министерства обороны США. В то время не было никаких следов кражи информации или порчи: Митник действовал просто из любопытства и проверял свои способности. Но один из системных администраторов обнаружил акт вторжения и поднял тревогу. Расследование выявило автора атаки, и Кевина Митника арестовали прямо на территории университета. Он был осуждён и отбыл своё первое настоящее наказание за незаконное вторжение в компьютерную систему, проведя полгода в исправительном центре для молодёжи.

В 1987 году Митник оставил свою незаконную деятельность. Кевин находился на испытательном сроке, в соответствии с последним приговором суда, поэтому он не мог позволить себе никаких правонарушений. Однако вскоре Митник снова был замешан в тёмных делах.

Однажды вечером вместе со своим другом Ленни ДиСикко Митник вторгся во внутреннюю сеть исследовательской лаборатории американской компьютерной компании Digital Equipment Corporation (DEC). Для Митника сделать это было несложно, так как ДиСикко являлся сотрудником данной лаборатории и одновременно был соучастником взлома. EasyNet - внутренняя сеть DEC - не выдержала хакерской атаки, и вскоре сообщники получили доступ ко всей системе.

Как и в случае с предыдущими атаками, вторжение в лабораторию было быстро обнаружено, но на этот раз Митник это предвидел и подготовился. Он зашифровал источник вызовов, сделав бесполезными все попытки выследить его. И на этот раз Митник взломал систему не из простого любопытства или для проверки своих способностей: у него было другая цель. Хакер хотел завладеть исходным кодом операционной системы VMS, разработанной компанией DEC для компьютеров VAX.

Митник предпринял все меры предосторожности, но не учёл одного - своего собственного друга. Кевин любил игры и розыгрыши, поэтому как-то раз он позвонил работодателю своего друга Ленни ДиСикко, притворившись представителем государственной власти. Он сказал, будто у одного из его служащих (ДиСикко) проблемы с налогами. ДиСикко не оценил такую шутку и решил отомстить по-своему.

ДиСикко предал Митника, сообщив своему работодателю о вторжении Митника в сеть компании. Затем он связался с ФБР и сказал, что может сдать хакера, который регулярно проникал в сеть лаборатории. Во время встречи Митника с ДиСикко хакер попал в ловушку, расставленную его собственным другом, который пришёл в сопровождении двух агентов ФБР. Митник был арестован.

Судебное дело длилось недолго: компания DEC обвинила хакера в краже информации и запросила за нанесённый ущерб более $200 000. Митника приговорили к одному году тюремного заключения, кроме того, он должен был посещать шестимесячные курсы для излечения от компьютерной зависимости.

В 1994 году Кевин Митник вернулся к своей незаконной деятельности, его разыскивало ФБР. За свои "подвиги" Митник уже прославился на весь мир. Федералы разослали повсюду его фотографии, чтобы узнавшие его люди могли позвонить властям. В течение этого и следующего года на Кевина Митника была объявлена облава, самая впечатляющая за всю историю поимки хакеров.

Митник решил атаковать другого хакера и эксперта по компьютерной безопасности - Тсутому Шимомуру (Tsutomu Shimomura). Он хорошо подготовил свою атаку и, чтобы убедиться, что никто ему не помешает, запустил её в Рождество, 25 декабря 1994 года. Митник взломал личный компьютер Шимомуры, используя неизвестную в то время методику - подмену IP-адреса, то есть разновидность вторжения, при котором взломщик пытается замаскироваться под другую систему, используя её IP-адрес.

Однако Митника подвёл брандмауэр Шимомуры, который записывал все действия, происходящие на целевой машине. На следующий же день, 26 декабря, Шимомуре позвонил один из его коллег и сообщил, что его компьютер стал жертвой вторжения. Шимомура быстро вычислил Митника и решил помочь ФБР в поимке хакера, используя свои же хакерские умения.

Для поимки Митника ФБР предоставило Шимомуре полную свободу действий, в том числе разрешило использовать хакерство. Облава превратилась в виртуальную охоту. Однажды Шимомура сообщил, например, что он застал Митника врасплох 17 января 1995 года, когда тот влез в сеть, принадлежащую Motorola, чтобы украсть секретное программное обеспечение компании.

Преследование усиливалось, и спецслужбы начали приближаться к киберпреступнику, отступающему в г. Роли, штат Северная Каролина. Чтобы засечь сотовый телефон, с которого Митник совершал свои атаки, Шимомура в течение двух дней бродил по улицам Роли с детектором связи. 15 февраля 1995 года в 2 часа ночи агенты ФБР вместе с Шимомурой ворвались в квартиру Митника. Когда знаменитый хакер увидел своего соперника, он воскликнул: "Hi, Тсутому! Мои поздравления!". После почти двухлетнего преследования Митника приговорили к пяти годам тюремного заключения. На то время это было самое суровое наказание для хакера. Ныне является консультантом по компьютерной безопасности.

##### Роберт Таппан Моррис

Роберт Таппан Моррис (Robert Tappan Morris), который сейчас является штатным профессором в Массачусетском технологическом институте (МТИ) в лаборатории компьютерных наук и искусственного интеллекта, создал первого "интернет-червя".

И опять же, к созданию "червя" Морриса побудило любопытство. По его словам, основной целью его программы было оценить истинные размеры сети Интернет, т.е. определить количество подключённых к ней компьютеров. В то время к Интернету было подключено не так много машин, но вопреки расчётам Морриса, его "червь" причинил гораздо больше вреда, чем ожидалось.

"Червь" Морриса, отправленный с компьютеров МТИ, был запрограммирован на то, чтобы проверить компьютер и скопировать себя в систему, если машина ещё не была инфицирована. Проблемы начались, когда Моррису пришла в голову мысль, что некоторые системные администраторы могут придумать уловку с поддельными копиями, чтобы обмануть "червя" и заставить его думать, что компьютер уже заражён. Тогда он модифицировал код программы, чтобы "червь" оставлял свои копии каждый раз, независимо от того, инфицирован компьютер или нет.

"Червь" Морриса распространился, как пожар, заразив несколько тысяч компьютеров всего за несколько часов. Приблизительно подсчитали, что восстановление каждой инфицированной системы будет стоить от $200 до $53 000, в зависимости от компьютера. Чтобы остановить "червя", были мобилизованы различные команды программистов, для нейтрализации атаки понадобилось несколько дней.

Роберт Таппан Моррис был признан виновным в компьютерном мошенничестве и был приговорён к трём годам условно, 400 часам общественных работ и $10 050 штрафа.

##### Кевин Поулсен

Кевин Поулсен - это ещё одно имя, которое вошло в анналы ФБР в 80-е гг. Впервые его арестовали в 1989 году, когда ему было 24 года. Тогда его обвинили в нескольких взломах телефонных сетей и компьютерных серверов, против него были собраны разные уличающие доказательства. Но когда пришло время предстать перед судом, Поулсен решил скрыться, агенты ФБР 17 месяцев выслеживали его. Именно в это время он совершил своё самое знаменитое хакерское деяние. В прямом эфире на лос-анджелесской радиостанции KIIS-FM проходила викторина-розыгрыш. Слушателям предлагалось позвонить на радиостанцию и попытаться выиграть автомобиль Porsche 944 S2. Приз должен был достаться 102-му дозвонившемуся радиослушателю. Кевин Поулсен начал действовать: он так заблокировал телефонную сеть, что на радио никто не мог дозвониться, кроме него самого. Следовательно, Кевин стал 102-м дозвонившимся и выиграл приз. Поулсен "утёр нос" ФБР, заставив власти вновь приступить к его поиску, потому что после этого он исчез.

В апреле 1991 года ФБР, наконец, удалось арестовать Поулсена. Поимке поспособствовал анонимный донос: кто-то сообщил властям, что Поулсен делает покупки в супермаркете на окраине Лос-Анджелеса. В 1994 году ему предъявили обвинение и в результате приговорили к четырём годам тюремного заключения. В то время это был самый суровый приговор, назначенный судом за хакерство.

В 1983 году на обложке Newsweek появился один из основателей хакерской группы "414s", ставшей известной благодаря серии взломов серьезных компьютерных систем. У хакеров появляются и собственные журналы, и другие способы обмена информации. В эти же годы власти западных стран начинают формировать законы, связанные с компьютерной безопасностью. Впрочем, масштаб, конечно, не идет ни в какое сравнение с сегодняшним днем. Так, много шума случилось вокруг дела Кевина Поулсена, который, благодаря своим фрикерским навыкам, первым дозвонился в эфир радиостанции KIIS-FM, что позволило ему выиграть автомобиль Porsche в рамках проходящего конкурса. По сравнению с современными атаками, которые позволяют уводить со счетов миллионы долларов — это просто мелочь, но тогда эта история вызвала очень большой резонанс.

Девяностые – это эра активного развития интернета, в это же время за хакерством окончательно закрепляется криминальный оттенок. Персональные компьютеры уже стали относительно доступны простым людям, при этом о безопасности никто особенно не задумывался. Появлялось огромное количество готовых программ, с помощью которых можно было взламывать пользовательские компьютеры, не имея каких-то серьезных технических навыков и способностей. Чего стоит только известная программа winnuke, которая позволяла отправить Windows 95/98 в "синий экран" путем отправки одного-единственного IP-пакета.

##### Владимир Левин

Люди занимаются хакерством не только из любопытства и азарта, иногда в дело замешаны деньги. Самый яркий пример - ограбление банка с целью получения денег, иногда удавалось украсть миллионы. Так, Владимир Левин (Vladimir Levin) завоевал дурную славу тем, что украл несколько миллионов долларов при странных обстоятельствах.

В 1994 году Левин проник во внутреннюю сеть американского банка Citibank, взломав аналоговое модемное подключение банка и получив доступ к нескольким счетам. Он сумел перевести 10,7 миллиона долларов на счета в США, Финляндию, Германию, Израиль и Нидерланды. Левину помогали трое сообщников, которые должны были вернуть украденные деньги.

Однако его сообщников арестовали, когда они пытались стащить украденные деньги. Их допрос вывел на след Левина, который работал программистом в Санкт-Петербурге. Российского хакера арестовали в марте 1995 года в лондонском аэропорту Хитроу. Судебное разбирательство против него началось только в сентябре 1997 года и закончились в феврале следующего года. Левина приговорили к трём годам лишения свободы.

Вообще, девяностые считаются золотыми годами темных хакеров: возможностей для мошенничества полно, компьютерные системы соединены через интернет, а серьезных механизмов безопасности в массовых ОС в эти годы еще нет.  Еще одна отличительная особенность девяностых — огромное количество голливудских фильмов про хакеров как иллюстрация того факта, что взлом компьютерных систем постепенно становится "обыденной диковинкой" для широких масс. Ведь почти в каждом таком фильме обязательно фигурировал какой-нибудь вирус, который взрывал мониторы. Может быть, именно из-за киноиндустрии у пользователей в голове сложился стереотип "безопасность — это вирусы", что, конечно, помогло многим антивирусным компаниям сделать свое состояние.

В 2002 году Билл Гейтс написал своим сотрудникам в компании Microsoft письмо о том, что ситуацию нужно исправлять, и пора начинать разрабатывать программное обеспечение с оглядкой на безопасность. Данная инициатива получила название "Trustworthy computing", и развивается она до сих пор. Начиная с Windows Vista, эта идея начала воплощаться в жизнь. Количество уязвимостей в ОС от Microsoft заметно снизилось, эксплойты (компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему) под них все реже появляются в публичном доступе. Как ни удивительно это звучит, но с точки зрения подхода к безопасности последние версии Windows гораздо надежнее других распространенных операционных систем. Так, в OS X только в последнее время стали появляться механизмы, которые затрудняют эксплуатацию уязвимостей.

Нулевые годы нашего века. Цифровой криминал выходит на новый уровень. Каналы связи стали толще, стало проще совершать мощные DoS-атаки. Никто уже не занимается взломом компьютерных систем просто ради удовольствия, это многомиллиардный бизнес. Расцветают ботнеты: огромные системы, состоящие из миллионов зараженных компьютеров. Другой характерной особенностью последнего десятилетия является тот факт, что фокус атакующего сместился на пользователя, на его персональный компьютер. Системы становятся сложнее, современный браузер — это уже не просто программа, которая умеет рендерить HTML, показывать текст и картинки. Это очень сложный механизм, полноценное окно в интернет. Почти никто уже не пользуется отдельными мессенджерами и почтовыми клиентами, все взаимодействие с интернетом происходит именно через браузер. Неудивительно, что один из основных методов заражения пользователей в наш дни — drive-by-downloads — происходит как раз при помощи браузера. Конечно, в современных браузерах стали появляться механизмы борьбы с этим, пользователей стараются предупреждать, что посещаемый сайт может быть опасен. Но браузер по-прежнему остается одним из основных посредников при заражении пользовательских машин. Еще один большой канал распространения вредоносных программ — мобильные устройства. Если в официальных магазинах приложений программы хоть как-то проверяют на вредоносность, то из неофициальных источников можно занести на свой девайс практически все, что угодно. Да и вообще безопасность мобильных устройств сейчас — довольно молодая и немного сумбурная отрасль, что связано с той скоростью, с которой современные мобильные платформы ворвались в нашу жизнь.

##### Андриан Ламо

Адриан Ламо, безусловно, свёл с ума самое большое количество сетевых администраторов. От его деятельности пострадали такие крупные корпорации, как Microsoft, New York Times, AOL, Sun Microsystems, Yahoo!, MacDonald's и Cingular. Ему приписывают все виды атак и нарушений защиты корпоративных систем безопасности. Ламо обходил защитные системы с обескураживающей простотой. Так, во время эфира ночных новостей телекомпании NBC журналист предложил Адриану доказать свой талант прямо перед объективом камеры, и тогда хакер менее чем за пять минут проник во внутреннюю сеть самой телекомпании. В настоящее время Ламо является специалистом по безопасности и наслаждается полной свободой передвижения после того, как многие годы был под наблюдением властей США.

12 февраля 2004 года был самый обычный день, но в компании Microsoft было объявлено чрезвычайное положение. Кто-то украл исходный код операционной системы Windows 2000, которой до сих пор пользуется большое количество пользователей. И что ещё хуже, неизвестный хакер выложил этот код в Wild. Кража была масштабна: 600 миллионов байт данных, 30 195 файлов и 13,5 миллиона строк кода. Утечка информации коснулась операционной системы Windows 2000 и её "старшей сестры" Windows NT4. Все сотрудники "софтового" гиганта пытались выяснить, что произошло, но никто не мог дать ответ. Данные были украдены прямо из сети Microsoft. Неизвестный хакер вошёл во внутреннюю сеть компании, взломав пароль одного из компьютеров. Исходный код быстро распространился по Интернету, особенно по P2P-сетям. К счастью, несмотря на то, что все опасались худшего, последствия этой грандиозной кражи оказались довольно мягкими.

### Ответственность

На сегодняшний день за "хакерство" можно получить наказания по статьям 212 (Хищение путем использования компьютерной техники), 354 (Разработка, использование либо распространение вредоносных программ).

#### Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, - наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в крупном размере, - наказываются лишением свободы на срок от трех до десяти лет с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, - наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

#### Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

За всю историю самое жестокое наказание за хакерство было в 1998-1999 годах в Китае, когда два брата подверглись смертной казни за взлом компьютерной системы государственного банка с целью кражи денег. Один из братьев получил отсрочку исполнения приговора за согласие дать свидетельские показания.

Не всегда же хакерство носит негативный оттенок. Известны случаи, когда можно законно зарабатывать, будучи хакером. Ведь некоторые из них помогают защитить наши компьютеры и гаджеты от кражи информации и взломов. Весной 2015 года особо отличился хакер Джун Хун Ли из Южной Кореи. Участвовал в конкурсе Pwn2Own, который спонсирует корпорация Google. В ходе этого мероприятия хакеры со всего мира демонстрируют конкурсному жюри обнаруженные ими баги, уязвимости и эксплойты в различных приложениях и операционных системах. Разумеется, за каждый обнаруженный баг хакер получает награду от организаторов. Джун Хун Ли выявлял одну уязвимость за другой. Сначала он сломал браузер Chrome. Затем продемонстрировал, как с помощью этого же браузера можно организовать широкомасштабную атаку на операционную систему. Потом взломал браузер Apple. Заработав в общей сложности 225 000 долларов за два дня конкурса, Джун Хун Ли наконец расслабился и перевёл дыхание.

Подведем итог о том, что такое хакерство сегодня, и чего стоит ожидать в ближайшем будущем. Хакерство возникло в 70-е гг. прошлого века, но некоторые из многочисленных группировок, сформировавшихся вокруг этого движения, существуют и по сей день. Всё больше и больше людей получают возможность пользоваться Интернетом, а хакеров и так называемых "script kiddies" (компьютерных хулиганов-подростков) сейчас больше, чем когда-либо. Однако мы не наблюдаем бурного роста крупномасштабных атак против компьютерных систем, который был бы соразмерен увеличению числа хакеров. Движение пошло немного по другому направлению, по сравнению с периодом расцвета хакерства. Некоторые атаки по-прежнему производят фурор, и системным администраторам приходится за это расплачиваться. Кевины Митники и Джоны Дрейперы, которые вошли в историю, уже успокоились и остепенились, а нынешние специалисты по безопасности компьютерных систем сталкиваются с менее опасной, но гораздо более массовой угрозой. В начале двухтысячных, если обнаруживалась какая-нибудь уязвимость в Windows, практически сразу в свободном доступе появлялся эксплойт, который позволял получить контроль над пользовательским компьютером. Тогда над извлечением прибыли от уязвимостей практически не задумывались. Конечно, были программы, которые воровали данные пользователей, уводили компьютеры в ботнеты, но сами уязвимости, приводящие к компрометации компьютера, было относительно просто эксплуатировать, а значит, написать эксплоит. Примерно последние пять лет найти в публичном доступе рабочий эксплоит для недавно обнаруженной уязвимости стало очень непросто. Теперь это огромный бизнес. Ведь написать эксплоит для уязвимости в системе, в которой внедрены механизмы вроде DEP и ASLR, значительно сложнее. Последние годы также показывают, что всех нас ждут проблемы безопасности так называемого "интернета вещей". Компьютеры с доступом в интернет сейчас все чаще в том или ином виде присутствуют в самых разнообразных бытовых и медицинских приборах, а также автомобилях. И уязвимости в них точно такие же, как в обычных компьютерах. Исследования по взлому привычных нам вещей становятся популярной темой на ведущих мировых конференциях по безопасности. Ведь если злоумышленники начнут пользоваться такими уязвимостями, это будет представлять серьезную опасность для здоровья и жизни пользователей. Тем важнее становится роль специалиста по безопасности.