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 ПО, 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.)

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*

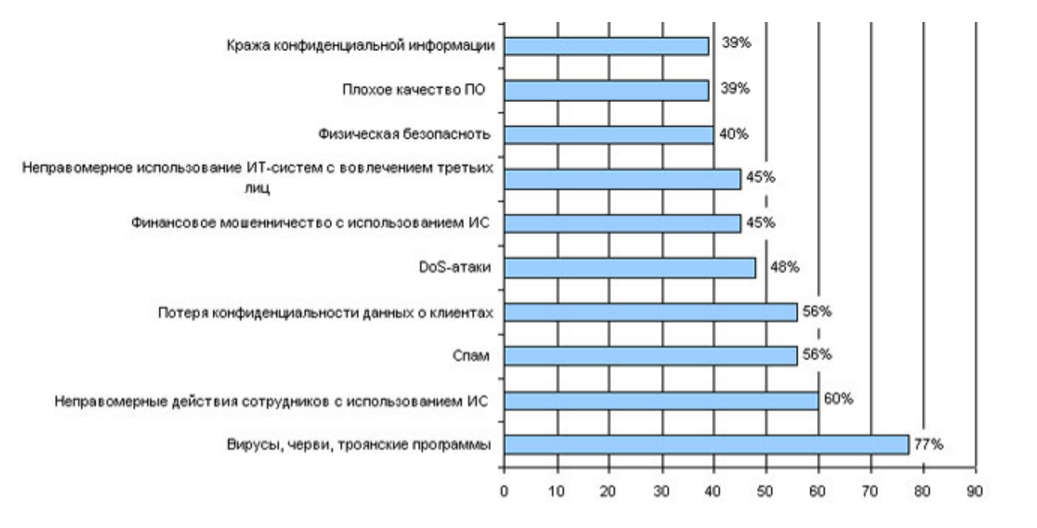
* **Контакты.** Пройтись по контактам в телефонах и удалить ненужные.
* **Сообщения.** Удалить все СМС и другие сообщения на смартфоне/планшете.
* **Документы.** Найти и удалить ненужные и забытые документы и книги на смартфоне/планшете.
* **Закладки в браузере.** Внимательно просмотреть и выявить все 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.

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, так и программными.

***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.

***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.

В зависимости от среды обитания основными типами компьютерных вирусов являются:

* Программные (поражают файлы с расширением .СОМ и .ЕХЕ) вирусы
* Загрузочные вирусы
* Макровирусы
* Сетевые вирусы

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 тобой 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. Тебе, буквально, 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 осуществляется 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 "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 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. 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. На протяжении девяностых дважды был осужден один из самых знаменитых хакеров двадцатого века — Кевин Митник, взломавший внутреннюю сеть компании DEC. 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. 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 ПО 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 массированные 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.

Подведем итог о том, что такое хакерство сегодня, и чего стоит ожидать в ближайшем будущем. 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.