8. Компьютерная безопасность

В прошлом компьютерам угрожали преимущественно вирусы и черви. Основной целью этих программ было самораспространение. Некоторые программы также причиняли вред файлам и самим компьютерам. Такие вредоносные программы — типичные проявления кибервандализма.

Понятие «вредоносные программы» объединяет все программы, создаваемые и используемые для осуществления несанкционированных и зачастую вредоносных действий. Вирусы, программы, создаваемые для незаконного удаленного администрирования, клавиатурные шпионы, программы для кражи паролей и другие типы троянцев, макровирусы для Word и Excel, вирусы сектора загрузки, мошенническое ПО, шпионские и рекламные программы — это далеко неполный список того, что классифицируется как вредоносные программы.

8.1. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ УГРОЗ.

В чем разница между вирусом и червем?

Вирус — это саморазмножающаяся программа: она распространяется с файла на файл и с компьютера на компьютер. Кроме того, вирус может быть запрограммирован на уничтожение или повреждение данных.

Черви считаются подклассом вирусов, но обладают характерными особенностями. Червь размножается (воспроизводит себя), не заражая другие файлы. Он внедряется один раз на конкретный компьютер и ищет способы распространиться далее на другие компьютеры.

Троянская программа. По классическому определению, троянец — это программа, которая внешне выглядит как легальный программный продукт, но при запуске совершает вредоносные действия. Троянские программы не могут распространяться сами по себе и этим они отличаются от вирусов и червей.

Обычно троянцы скрытно устанавливаются на компьютер и выполняют вредоносные действия без ведома пользователя. Трояны разных видов составляют большую часть современных вредоносных программ; все они пишутся специально для выполнения конкретной зловредной функции. Чаще всего встречаются backdoor-троянцы (утилиты удаленного администрирования, часто включают в себя клавиатурные шпионы), троянцы-шпионы, троянцы для кражи паролей и троянцы, превращающие ваш компьютер в машину для рассылки спама.

Drive-by (попутная загрузка). При drive-by загрузке, компьютер заражается при посещении веб-сайта, содержащего вредоносный код. Кибермошенники ищут в Интернете веб-серверы, уязвимые для взлома, чтобы вписать вредоносный код на веб-страницы (часто в виде вредоносного скрипта). Если в операционной системе или на приложениях не установлены обновления безопасности, то при посещении зараженного веб-сайта вредоносный код загружается на ваш компьютер автоматически.

Фишинг – это особый вид кибермошенничества, направленный на то, чтобы обманным путем заставить вас раскрыть персональные данные, как правило, финансового характера. Мошенники создают поддельный веб-сайт, который выглядит как сайт банка (или как любой другой сайт, через который производятся финансовые операции, например eBay). Затем преступники пытаются завлечь вас на этот сайт, чтобы вы ввели на нем конфиденциальные данные, такие как логин, пароль или PIN-код. Часто для этого мошенники с помощью спама распространяют ссылку на этот сайт.

Клавиатурный шпион – это программа, отслеживающая нажатия кнопок на клавиатуре. При помощи нее злоумышленник может получить доступ к конфиденциальным данным (логины, пароли, номера кредитных карт, PIN-коды и т.п.). Клавиатурные шпионы часто входят в состав backdoor-троянцев

Ботнеты (бот-сети или так называемые зомби-сети) создаются троянцами или другими специальными вредоносными программами и централизованно управляются хозяином, который получает доступ к ресурсам всех зараженных компьютеров и использует их в своих интересах.

Шпионские программы. Как следует из названия, эти программы предназначены для сбора данных и отправки их третьей стороне без вашего ведома и согласия. Такие программы могут отслеживать нажатия клавиш (клавиатурные шпионы), собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.д.), отслеживать адреса электронной почты в почтовом ящике или особенности вашей работы в Интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера.

Рекламные системы (adware). Понятие “adware” включает в себя программы, запускающие рекламу (часто в виде всплывающих окон) или перенаправляющие поисковые запросы на рекламные веб-сайты. Рекламное ПО часто бывает встроено в бесплатные или условно-бесплатные программы и устанавливается на компьютер пользователя одновременно с основным приложением без ведома и согласия пользователя. В некоторых случаях рекламное ПО может тайно загрузить и установить на ваш компьютер троянская программа.

Фальшивые антивирусные программы. Мошеннические схемы, в которых они задействованы, начинают работать со всплывающего сообщения на веб-сайте, из которого следует, что ваш компьютер заражен и вам необходимо загрузить бесплатную антивирусную программу для удаления якобы найденного вредоносного ПО. Но когда вы загружаете и запускаете предлагаемую программу, она сообщает, что для удаления с компьютера вредоносных программ необходима ее «полная» версия, за которую придется заплатить. В случае успеха мошенники оказываются в двойном выигрыше: они не только зарабатывают на фальшивом антивирусе, но и заполучают реквизиты вашей кредитной карты.

8.2. АНТИВИРУСНАЯ ЗАЩИТА

Антивирусная защита компьютера обеспечивает противодействие вредоносным программам, которые законно или незаконно проникли на Ваш компьютер. Основное правило борьбы с вирусами – никогда не запускайте программ, полученных из источников, доверять которым вы не можете. Здесь следует напомнить, что присланный файл от друзей или родственников, вполне может быть прислан от злоумышленника, подделавшего адрес отправителя.

Некоторые правила работы с антивирусными средствами:

1. Следите за обновлениями антивирусного обеспечения. Помните, что новые версии вирусов появляются каждую минуту. По этой причине следует выполнять обновления антивируса целью постоянной поддержки актуальности их баз.

2. Не выключайте антивирусный монитор. Даже при условии, что работа компьютера замедляется, знайте, что антивирусный монитор постоянно проводит поиск вирусов в памяти компьютера. В случае, если Вы его отключите, вирус, поразивший Ваш компьютер, будет обнаружен не на стадии активации, а задолго после заражения всего компьютера, когда вы начнете плановое сканирование жесткого диска.

3. При возникновении заражения одного или нескольких файлов, следует поместить их в карантинную зону (опциональная возможность антивируса), при условии, что их лечение невозможно.

4. Выполняйте сканирование всего вашего компьютера по расписанию. Это мероприятие позволит отслеживать вирусы и другие вредоносные программы до их активации в системе.

Помните, что антивирусное программное обеспечение позволяет избавиться от той головной боли, которую Вы можете получить, заразившись вирусом.

Популярные антивирусные продукты

Антивирус Касперского. ***Разработчик:*** «Лаборатория Касперского».

Цена 69 долл. (лицензия на 1 год). ***Web-сайт:*** http://www.kaspersky.ru/

Пожалуй, «Антивирус Касперского» — самый известный в России продукт этого типа, а фамилия «Касперский» стала синонимом борца с вредоносными кодами. Одноименная лаборатория не только постоянно выпускает новые версии своего защитного ПО, но и ведет просветительскую работу среди пользователей компьютеров. Он отличается простым и максимально прозрачным интерфейсом, объединяющим все необходимые утилиты в одном окне. Благодаря мастеру установки и интуитивно понятным пунктам меню, настроить этот продукт способен даже начинающий пользователь. С другой стороны, мощность используемых алгоритмов удовлетворит и профессионалов. С детальным описанием каждого из обнаруженных вирусов можно ознакомиться, вызвав соответствующую страницу в Интернете непосредственно из программы.

Тестирование: шесть зараженных объектов программа нашла за 15 минут. При этом в отчете не появилось ни одного сообщения о ложном срабатывании.

Dr.Web. ***Разработчик:*** «Лаборатория Данилова» и «ДиалогНаука».

Цена 50 долл. (лицензия на 1 год). ***Web-сайт:*** http://www.dialognauka.ru/, http://www.Dr.Web.ru/.

Еще один популярный российский антивирус, соперничающий по известности с “Антивирусом Касперского”,— Dr.Web. Его ознакомительная версия требует обязательной регистрации через Интернет. С одной стороны, это очень хорошо — сразу после регистрации производится обновление антивирусных баз и пользователь получает самые новые данные о

сигнатурах. С другой стороны, установить ознакомительную версию автономно невозможно, да и, как показал опыт, при неустойчивом соединении неизбежны проблемы.

Начинающим пользователям во время инсталляции лучше согласиться с установкой типичной конфигурации, иначе можно запутаться в терминах. После инсталляции в системной панели компьютера появится несколько "паучков". Это пиктограммы монитора, планировщика заданий Dr.Web и программы проверки электронной почты.

Тестирование: в процессе сканирования Dr.Web нашел все 7 зараженных объектов и даже выявил одну вредоносную процедуру, о существовании которой в системе никто не подозревал.

Panda Antivirus + Firewall 2007. ***Разработчик:*** Panda Software.

Цена 39,95 долл. ***Web-сайт:*** http://www.pandasoftware.com/

Комплексное решение в области компьютерной безопасности — пакет Panda Antivirus+Firewall 2007 — включает в себя помимо антивирусной программы брандмауэр, отслеживающий сетевую активность. Интерфейс основного окна программы решен в «природных» зеленых тонах, но, несмотря на внешнюю привлекательность, система переходов по меню выстроена неудобно и начинающий пользователь вполне может запутаться в настройках.

Тестирование: к сожалению, применение новых технологий не помогло программе Panda найти все опасные объекты: в ее активе оказались лишь шесть классических «троянов». Кроме того, утилита половину из них вылечила «без спроса» а остальные переименовала. Найти в настройках отключение такого самоуправства не удалось.

Norton Antivirus 2005. ***Разработчик:*** Компания Symantec.

Цена 89,95 евро. ***Web-сайт:*** http://www.symantec.ru/

Основное впечатление от продукта знаменитой компании Symantec — антивирусного комплекса Norton Antivirus 2005 — его ориентация на мощные вычислительные системы. Реакция интерфейса Norton Antivirus 2005 на действия пользователя ощутимо запаздывает. Кроме того, при инсталляции она предъявляет достаточно жесткие требования к версиям операционной системы и Internet Explorer. В отличие от Dr.Web,Norton Antivirus не требует обязательного обновления вирусных баз при установке, но о том, что они устарели,будет напоминать в течение всего времени работы.

Тестирование: все 7 тестовых вирусов были обнаружены менее чем за 15 минут. Никаких ложных срабатываний зафиксировано не было.

NOD32. ***Разработчик:*** Компания ESET.

Цена от 1690 руб в год. ***Web-сайт:*** www.esetnod32.ru

Известный, не очень популярный в России, но прославившийся за рубежом пакет NOD32, является лидером регулярно проводимого международного тестирования Virus Bulletin 100%. По заявлениям разработчиков, в рамках этой процедуры NOD32 — единственный продукт,не пропустивший ни одного вредоносного объекта. Интерфейс NOD32,общий для модулей сканирования и мониторинга, поддерживает русский язык и может загружаться в двух вариантах: классическом Windows и так называемом Eset. Последний выглядит довольно привлекательно и прост в пользовании, однако требует некоторого привыкания, так как содержит массу англоязычных аббревиатур.

Тестирование: за 5 минут нашел шесть зараженных файлов, а седьмой (с вредоносным червем) лишь «заподозрил» в наличии вирусной опасности.

Avira AntiVir Personal Edition Classic. ***Разработчик:*** Компания Avira GmbH.

Цена от 20 евро в год. ***Web-сайт:*** www.avira.com

Avira AntiVir — продукт новый. Имеет невысокую требовательность к ресурсам, функциональность и простоту интерфейса. Все функции Avira AntiVir логично объединены несколькими вкладками в главном окне программы. В нем же можно посмотреть отчет о работе сканера и карантин, в который помещаются зараженные или подозрительные объекты. Недостаток — англоязычный интерфейс.

Тестирование: программа показала хорошие результаты, определив все 7 вредоносных объектов за 9 минут. При этом не было зафиксировано ни одного ложного срабатывания.

avast! ***Разработчик:*** Компания ALWIL Software.

Цена от 900 руб/год. ***Web-сайт:*** www.avsoft.ru

Бесплатный (для домашнего пользователя) пакет avast! состоит из нескольких утилит, в числе которых: сканер сигнатур avast! antivirus и сканер (монитор) доступа avast!. Последний включает в себя 7 резидентных модулей, называемых в данном случае провайдерами, контролирующих в реальном времени деятельность компьютера — от сетевых подключений до обмена мгновенными сообщениями. Сканер avast! antivirus выделяется из числа аналогичных продуктов чрезвычайно оригинальным интерфейсом. Внешне он напоминает скорее медиаплеер, чем утилиту обеспечения безопасности. Удобные кнопки-пиктограммы, выдвигающиеся панели и информационное табло позволяют быстро настроить параметры сканирования.

Тестирование: на поиск шести зараженных файлов avast! antivirus затратил менее 9 минут, однако в отчете присутствовало много предупреждений о поврежденных и защищенных файлах, которые программа проверить не смогла.

Стоимость антивирусной защиты

Вопрос необходимости приобретения коммерческой версии антивирусной программы рано или поздно встает перед каждым пользователем. С одной стороны, в Интернете достаточно бесплатных антивирусных утилит, а с другой, понятно, что только на основе коммерческих пакетов с гарантированным регулярным обновлением можно выстроить серьезную систему безопасности. Как определить оптимальную сумму расходов на приобретение антивируса? Нужно лишь трезво оценить стоимость содержащейся на винчестере компьютера информации, причем не только с позиции возможных злоумышленников, но и с точки зрения затрат на ее восстановление. К этому нужно добавить приблизительную стоимость рабочего времени пользователя или стороннего специалиста, которое может понадобиться на восстановление работоспособности компьютера и приложений. Сравнение полученной величины с ценой антивирусного ПО даст мгновенный ответ на поставленный вопрос.

8.3. УЯЗВИМОСТИ, ОСНОВАННЫЕ НА ОСОБЕННОСТЯХ РЕАЛИЗАЦИИ INTERNET EXPLORER

Уязвимости данной категории не являются таковыми в прямом смысле этого слова — скорее это конструктивные недоработки, которые могут в том или ином виде использоваться в неблаговидных целях.

Хранение настроек в реестре

Все настройки Internet Explorer хранятся в системном реестре и могут модифицироваться из диалогового окна настройки IE или путем непосредственной правки реестра, а Internet

Explorer никак не контролирует целостность этих настроек и не проводит их защиту. По данной причине злоумышленниками было создано множество вредоносных программ, модифицирующих те или иные настройки Internet Explorer (существуют тысячи таких программ, причем довольно часто запуск подобной троянской программы производится за счет той или иной уязвимости Internet Explorer).

Обычно вредоносные программы модифицируют следующие настройки:

• домашняя страница,настройки поиска;

• параметры безопасности для одной или нескольких зон, причем возможно добавление одного или нескольких серверов в список надежных узлов;

• настройки подключения для реализации обмена через прокси-сервер злоумышленников.

Файлы Cookies.

Файлы Cookies у Internet Explorer хранятся в виде отдельных текстовых файлов с именами типа “zaitsev@yandex[1].txt” в папке Documents and Settings\<имя пользователя>\ Cookies. Эта папка имеет атрибут «Системный» и не видна в проводнике,но никакой иной защиты Cookies не предусмотрено. Следовательно,троянская программа может произвести анализ Cookies с целью поиска паролей или иной хранимой в них информации. Кроме того, при использовании чужого компьютера (например, в Интернет-кафе) следует помнить, что Cookies остаются и могут быть использованы злоумышленниками.

Меры против несанкционированных действий заключаются в ограничении прав доступа к папке Cookies и в отключении приема Cookies для определенных сайтов. В случае использования чужого компьютера нужно удалить файлы Cookies после завершения сеанса работы.

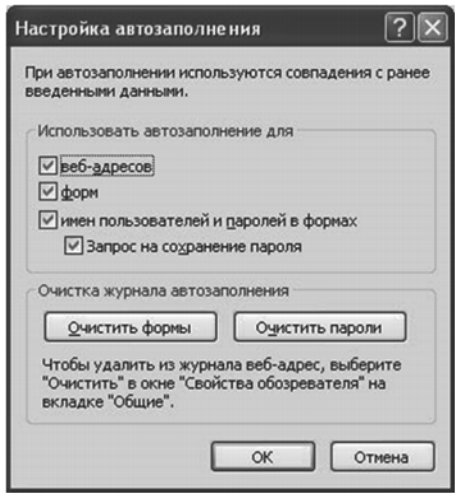
Журнал посещенных сайтов.

Internet Explorer ведет журнал, в котором фиксируются посещенные пользователем сайты. Особой опасности это не представляет, однако такой журнал не защищен и потому может быть проанализирован троянской программой. Чтобы предотвратить атаки, рекомендуем очистку журнала и настройку времени его хранения в параметрах Internet Explorer.

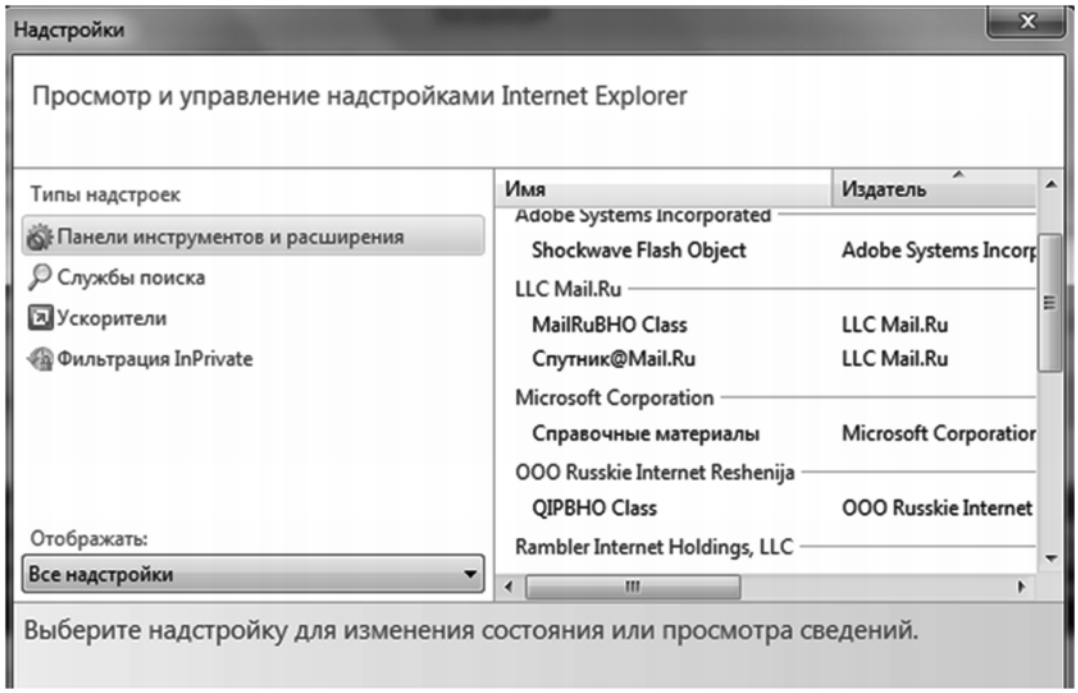
Недостаточная защита паролей доступа к веб-сайтам и к данным системы автозаполнения форм.

Когда пользователю приходится авторизоваться на некотором веб-сайте,Internet Explorer предлагает сохранить пароли. Это очень удобная функция, за одним исключением — защита сохраненных паролей доступа находится на низком уровне. Существуют программы (например, Advanced Internet Explorer Password Recovery), предназначенные для отображения сохраненных паролей и позволяющих просмотреть сохраненные пароли к веб-сайтам и данные системы автоматического заполнения форм.

Поэтому советуем не использовать сохранение паролей и автозаполнение веб-форм, причем это особенно важно при работе на компьютере, к которому имеется публичный доступ. Окно настройки автоматического заполнения форм, показанное на рисунке, позволяет выполнить два вида операций: настроить автозаполнение и произвести очистку журналов автозаполнения.



Следует отметить, что в последних версиях Internet Explorer появилась возможность просматривать подключенные надстройки и модули расширения (меню Сервис\Свойства обозревателя, в окне свойств — закладка «Программы», кнопка «Надстройки»). В данном окне можно не только просмотреть установленные надстройки и расширения IE, но и отключить любую из надстроек.



Как проверить, уязвим ли ваш Internet Explorer

Провести комплексную проверку и дать однозначные ответы крайне трудно, но проверка наличия десятка наиболее популярных уязвимостей доступна любому пользователю. Проще всего выполнить проверку при помощи онлайновых ресурсов (например, http://

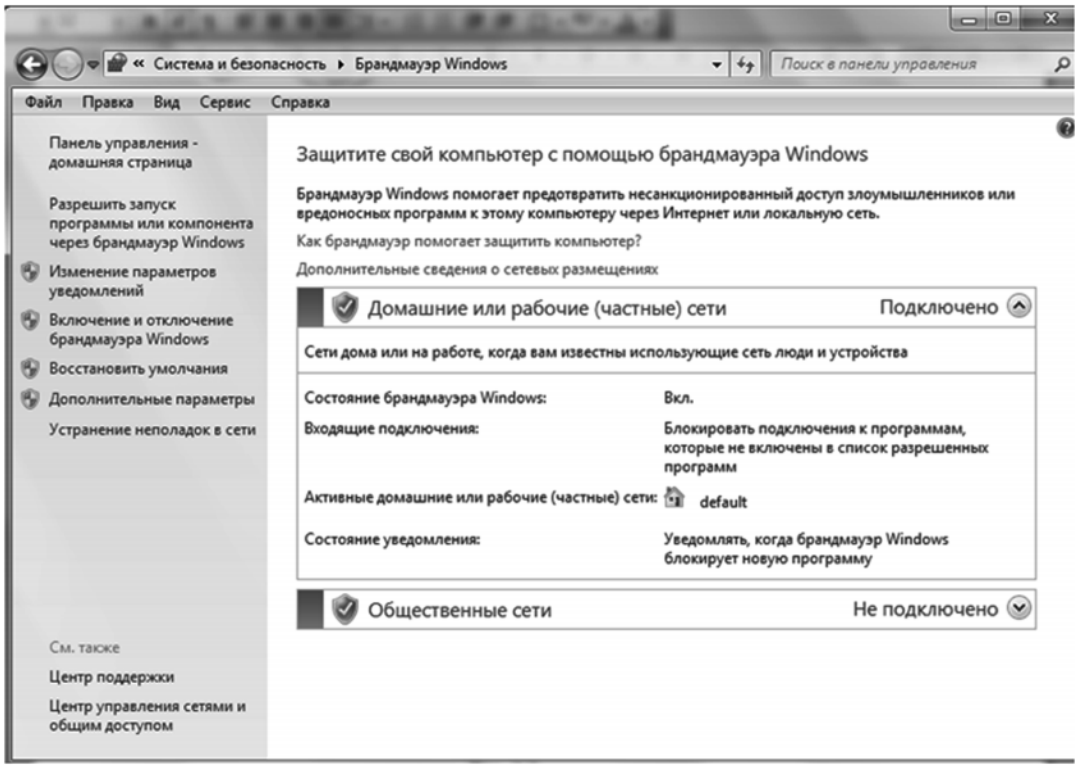
bcheck.scanit.be/bcheck/). Идея подобных тестов весьма проста: после начала теста против браузера поочередно применяется несколько эксплоитов, а пользователь при этом может наблюдать за реакцией браузера на каждый из них. Затем формируется отчет, в котором указано, сколько эксплоитов успешно сработало, с описанием соответствующих им уязвимостей и методов их устранения.

***Эксплойт**, (англ. exploit, эксплуатировать) — это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий) так и нарушение ее функционирования.*

Бранмауэр (firewall) Windows 7 представляет собой программный или аппаратный комплекс, проверяющий данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.

Брандмауэр поможет предотвратить проникновение хакеров или вредоносного программного обеспечения в ваш компьютер через сеть или Интернет. Брандмауэр также помогает предотвратить отправку вредоносных программ на другие компьютеры.

Доступ к настройкам брандмауэра Windows 7 можно получить при помощи Пуск — Панель управления — Система и безопасность - брандмауэр Windows. Пример окна с настройками брандмауэра показан на рисунке.



В этом окне можно включить или выключить брандмауэр для всех соединений с сетью. Нормальное состояние для брандмауэра — «Включить». Не следует выключать брандмауэр даже на короткое время без согласования с администратором сети, т.к. при этом Вы рискуете подвергнуться сетевой атаке.

8.4. МЕТОДИКА ПРОТИВОДЕЙСТВИЯ УЯЗВИМОСТЯМ

1. Своевременная установка обновлений. Как ни банален этот совет, своевременная установка обновлений является одной из самых эффективных мер борьбы с уязвимостями.

2. Применение антивирусных мониторов.

Целью многих эксплоитов является загрузка и запуск троянской программы. Монитор может обнаружить эту программу в момент ее загрузки или запуска. Некоторые антивирусные мониторы могут проверять скрипты перед их выполнением (такую проверку, в частности, выполняет монитор антивируса Касперского).

3. Работа с Internet Explorer из-под учетной записи пользователя, причем в идеале пользователь должен обладать минимальными правами. От уязвимости это не спасет, но нанесенный системе ущерб будет несравненно ниже. Кроме того, можно запустить Internet Explorer с пониженными правами — при помощи запуска от имени пользователя с ограниченными правами.

4. Применение брандмауэров. Некоторые брандмауэры могут обнаруживать и блокировать эксплоиты по сигнатурам, и практически любой брандмауэр окажется полезным в случае проникновения на компьютер вредоносной программы, так как он заблокирует ее попытки обмена с Интернетом.

5. Тщательная настройка безопасности, особенно для Интернет-зоны. Настройки безопасности Internet Explorer необходимо периодически проверять, поскольку они могут быть несанкционированно изменены вредоносными программами. Повышенная осторожность при открытии ссылок, особенно в письмах, полученных по электронной почте.

8.4.1. ОБЩИЕ ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ INTERNET

1. Не устанавливайте и не сохраняйте подозрительные файлы,полученные из ненадежных источников, скачанные с неизвестных веб-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять. В случае необходимости загрузки файла, убедитесь, что он проверен антивирусом.

2. Никому не передавайте свои регистрационные данные (имена пользователей и пароли) и храните их в защищенном месте,доступном только для Вас.

3. По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.), периодически их меняйте.

4. Используйте антивирусную программу для проверки жесткого диска. В случае обнаружения вирусов, выполняйте полную проверку всех разделов.

5. Очень часто злоумышленник выдает себя за администратора или представителя регулирующего государственного органа. Объясняя какие-либо технические детали, может утверждать о том, что, например, база данных с регистрационными данными повреждена, может пытаться выведать у Вас имя пользователя и пароль к Вашему личному счету и пр.

8.4.2. РОДИТЕЛЬСКИЙ КОНТРОЛЬ В ИНТЕРНЕТЕ

http://www.ixbt.com/soft/parentalcontrol.shtml

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно,ему еще рано знать и видеть. Одна из основных задач приложений — создание фильтра веб-сайтов. Все очень просто: на одни страницы заходить можно, на другие — нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

Довольно часто применяется более жесткий способ контроля — создание белого списка. Ребенок может посещать только те веб-сайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребенок даже не в курсе, о чем вообще сверстники ведут разговор, Интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на веб-странице, то она не открывается. Родителям, возможно, придется

отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к веб-сайтам. Есть еще одна, если так можно выразиться, группа риска — это программы обмена мгновенными сообщениями. Ребенок наивен, он можно нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками,невзначай задают каверзные вопросы. Напрашивается и вторая опасность — собеседники ребенка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьезных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

В вашей семье один ребенок или несколько детей, есть компьютер, подключенный к Интернету. Как обезопасить младшее поколение от негативных последствий пребывания в Сети? Первое, что сразу напрашивается — компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь родителей сможет постоянно следить за тем, чем занимается ребенок. В противном случае, он запрется в комнате, и вы даже, возможно,не догадаетесь, что чадом скачано несколько фильмов эротического содержания, а в местном чате ему рассказали,как самому делать петарды.

Ребенку надо показать Интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя. Нельзя соглашаться на встречи с незнакомыми людьми, нельзя сообщать личные данные, нельзя самостоятельно совершать покупки в сетевых магазинах. Ну а вместо нравоучений сыну «не смотри на голых женщин», уместней воспользоваться специальными программными продуктами, которые закроют ему доступ к взрослым ресурсам.

Вот примеры подобных программ:

- Crawler Parental Control 1.1
- KidsControl 2.02
- ParentalControl Bar 5.22
- Spector Pro 6.0
- КиберМама

8.4.3. ОНЛАЙН-ИГРЫ.

По мнению психологов,непреодолимая тяга к онлайн-играм сегодня стоит в одном ряду с такими патологическими расстройствами, как шопингомания или клептомания. Как правило, Интернет-зависимый индивид является обладателем каких-либо недостатков или проблем, затрудняющих социальные контакты. Самые распространенные из них: социофобия,дефекты внешности, лишний вес, дефекты речи, сексуальные проблемы, трудности в общении, а также недостаток самоуважения, со всеми ними связанный. Человеку может не хватать внимания или одобрения со стороны близких,самостоятельности, веры в себя. Потребность в компенсации этих недостатков толкает индивида в виртуальную реальность, которая предоставляет убежище от реальности настоящей. Личность перестает жить в реальном мире и начинает грезить наяву. Однако все может закончиться трагически — бездыханным телом, распростертым у монитора.

Взрослым, пристрастившимся к онлайн-играм, гораздо проще. Они могут расставить приоритеты, сказать себе в какой-то момент, что убийство нарисованного дракона не стоит

семейных проблем. Они могут отделить виртуальную безнаказанность от реалий жизни. У них — определенного рода иммунитет против всего того,что вкладывают в подсознание такие онлайн-игры. Иммунитет, в основе которого лежит жизненный опыт. Правда, не всегда и не у всех этот иммунитет срабатывает, но это уже другая история. Детям приходится тяжелее. У них нет жизненного опыта, они не сталкивались со многими жизненными реалиями. У них не возникает семейных проблем из-за пристрастия к онлайн-играм. Максимум — проблемы с учебой, но и тут не всякий родитель способен увидеть взаимосвязь, а спишет неуспеваемость на сложную школьную программу, в крайнем случае — на тупость собственного ребенка.

Детям сложнее остановиться. И с каждым днем они все больше втягиваются в виртуальный мир, обрастая там друзьями и знакомыми,отворачиваясь от реальной жизни. Тем более,что в виртуальном мире так просто стать лидером. И весь негатив онлайн-игр выплескивается на их неподготовленное сознание. И приживается там. Последствия уже известны. Не одна и не две истории об убийствах и избиениях, совершенных детьми, любителями различных онлайн-игр. Что неудивительно. Уже неоднократно было сказано: травмы в игре не болят,а если даже и убили, то легкое нажатие клавиши — и игрок воскрешен,готов к новым подвигам. Когда смешиваются в сознании виртуал и реал,то со стиранием этой грани стирается и многое другое. И виртуальная безнаказанность приводит к беспределу в реальной жизни.

Так что родителям рекомендуется внимательно наблюдать — а что именно увлекает ребенка, в какую игру он играет, закрывшись в своей комнате наедине с компьютером. Желательно еще и немного поиграть самому,чтобы точно знать — какие именно опасности подстерегают неокрепшую психику и неразвитую мораль ребенка на виртуальных дорогах.

И если выяснится, что данная игра является для ребенка потенциально опасной, то нужно... Нет, не запретить. Запреты — самый худший выход из положения. Запретный плод сладок. Но — предложить альтернативу. Настоящие приключения. Хотя бы поход в лес с палатками — дешево и сердито. Настоящую рыбалку — она куда увлекательнее ловли нарисованной рыбы. Настоящих друзей.

В конце концов, виртуальный пряник совсем не сладкий. Просто потому, что он — нарисованный. И как только ребенок это поймет — опасность миновала.

8.4.4. ПАРОЛИ

К сожалению,чем больше пользователи сообщают о себе в сети, тем выше риск кражи их личных данных киберпреступниками, которые в дальнейшем мошенническим путем приобретают товары и услуги от имени пользователей и даже крадут деньги непосредственно с банковских счетов своих жертв.

Поскольку пароли защищают конфиденциальную информацию, их важность трудно переоценить. Все ваши учетные записи в Интернете должны быть защищены паролями. Но выбирать пароль нужно осмотрительно.

Пароль защищает ваши персональные данные от кражи, в том числе не позволяет злоумышленникам получить доступ к банковскому счету или другим электронным учетным записям и украсть ваши деньги.

Выбор надежного пароля

Выбирайте пароли,которые вам будет легко запомнить и не придется записывать (в том числе вносить в файл на вашем компьютере). Такой файл может быть стерт,поврежден или украден киберпреступниками.

1. Не используйте в качестве пароля реальные слова,которые киберпреступники могут найти в словаре.

2. Используйте буквы как нижнего, так и верхнего регистра, а также цифры и другие символы — например, знаки препинания (хотя использование последних не всегда разрешено).

3. Не прибегайте к «ротации» паролей, когда «пароль1», «пароль2», «пароль3» и т.д. используются попеременно для разных учетных записей.

4. Если возможно, используйте в качестве пароля словосочетание, а не отдельное слово.

5. Не используйте один и тот же пароль для разных учетных записей. В противном случае, подобрав только один пароль, злоумышленники получат доступ ко всем вашим онлайн-аккаунтам.

6. Не используйте для защиты своих данных очевидные пароли, которые легко угадать: имя вашего супруга, ребенка, домашнего животного, регистрационный номер машины, почтовый индекс и т.п.

7. Не сообщайте никому свой пароль. Если с вами связался (например, по телефону) представитель некой организации и попросил сообщить ваш пароль, не раскрывайте свои личные данные: вы не знаете, кто на самом деле находится на другом конце провода.

8. Если онлайн-магазин или веб-сайт прислал вам по электронной почте сообщение с подтверждением регистрационной информации и новым паролем, как можно скорее зайдите на соответствующий сайт и смените пароль.

9. Убедитесь в том, что установленное на вашем компьютере программное обеспечение для защиты от Интернет-угроз блокирует попытки перехвата или кражи.

Итак, выбирая пароль:

- Делайте его запоминающимся;
- Храните его в секрете;
- Не позволяйте с виду легальным организациям выманить его у вас обманным путем;
- Используйте одновременно буквы нижнего и верхнего регистра, цифры и другие символы;
- Не используйте один пароль для нескольких учетных записей;
- Не ротируйте пароли между разными учетными записями.

8.4.5. ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Не запускайте программы, полученные по электронной почте. Это действительно опасно, даже если письмо прислал хорошо известный Вам человек. Если есть подозрение, что это вирус или, так называемый «троян», просто удалите письмо.

2. Никому не доверяйте Ваш пароль! Если Вам пришло письмо с требованием сообщить все данные о себе, включая пароль для вашей почты, не отдавайте пароль, даже если это письмо пришло с адреса webmaster или support. Не доверяйте доводам вроде «устранения технических проблем с Вашим ящиком» и не бойтесь угроз Ваш ящик закрыть.