**Десять непреложных законов безопасности**

В центре обеспечения безопасности корпорации Майкрософт ежегодно анализируются тысячи отчетов о нарушении безопасности. Иногда оказывается, что в отчете действительно описывается уязвимость системы безопасности, возникшая как следствие изъяна в одном из продуктов корпорации Майкрософт. В этих случаях специалисты корпорации Майкрософт как можно скорее разрабатывают исправление, устраняющее эту ошибку (см. раздел A Tour of the Microsoft Security Response Center [«Общие сведения о центре обеспечения безопасности корпорации Майкрософт»]). Бывает также, что описываемая проблема является следствием ошибки при использовании продукта. Однако многие отчеты не попадают ни в одну из этих категорий — хотя в них описываются настоящие проблемы с системой безопасности, однако эти проблемы не являются следствием изъянов в продуктах. За годы работы сотрудники центра создали список подобных проблем, назвав его «Десять непреложных законов безопасности».

Не ждите, затаив дыхание, что выйдет новое исправление, которое защитит вас от описанных ниже проблем — ни корпорация Майкрософт, ни любой другой разработчик программного обеспечения не сможет «устранить» эти проблемы, поскольку они обусловлены особенностями работы компьютеров. Однако не теряйте надежду — научитесь правильно оценивать ситуацию, не забывайте об этих проблемах, выполняя те или иные действия на компьютере, и ваши системы будут защищены значительно лучше.

Закон №1. Если вы запустили на своем компьютере приложение злоумышленника, это больше не ваш компьютер

Печально, но факт: когда приложение запускается на компьютере, оно всегда выполняет те задачи, для решения которых создавалось, даже если это абсолютно противозаконно. Запуская приложение, пользователь передает ему управление компьютером — оно может делать все, что может делать на компьютере сам пользователь. Например, оно может «запоминать», какие клавиши нажимает пользователь, и отправлять эти сведения в Интернет, открывать любые документы на компьютере и произвольным образом изменять их содержимое, отправлять друзьям и знакомым пользователя оскорбительные сообщения по электронной почте и даже форматировать жесткий диск компьютера. Да, вот еще: вредоносное приложение может установить вирус или программу, которая позволит кому угодно удаленно управлять компьютером через Интернет, подключившись к нему с помощью обычного модема где-нибудь в Катманду.

Поэтому очень важно никогда не запускать и даже не загружать приложения из источников, которым вы не доверяете, — причем под «источником» подразумевается не тот человек, от которого вы получили это приложение, а тот, который его создал. Кстати, существует хорошая аналогия между приложением и бутербродом. Если незнакомый человек предложит вам бутерброд, станете ли вы его есть? Вероятно, нет. А если бутерброд предложит ваш хороший друг? Может, станете, а может, и нет — в зависимости от того, сделал ли человек этот бутерброд сам или нашел на улице. Используйте для приложений те же критерии, что и для бутербродов, и вы защитите себя от большинства опасностей.

Закон №2. Если злоумышленник внес изменения в операционную систему вашего компьютера, это больше не ваш компьютер

Фактически, операционная система — это всего лишь набор нулей и единиц, которые интерпретируются процессором и «заставляют» компьютер выполнять определенные действия. Стоит изменить эти нули и единицы, и компьютер начнет делать что-то совершенно другое. Где же хранятся эти нули и единицы? На компьютере — там же, где и все остальное! Они представляют собой обыкновенные файлы, и если другие люди, которые используют этот компьютер, смогут изменять их — все пропало.

Это легко понять, если вспомнить, что файлы операционной системы входят в число наиболее доверенных файлов и, как правило, выполняются с правами системного уровня. Иначе говоря, содержащиеся в этих файлах программы могут выполнять любые действия. Кроме того, они имеют право управления учетными записями пользователей, изменения паролей и установки прав использования компьютера. Если злоумышленник сможет заменить эти файлы, содержащиеся в них приложения будут исполнять его команды, и он сможет сделать все, что захочет — похитить пароли, предоставить себе права администратора или же добавить в операционную систему новые функции. Чтобы предотвратить подобные атаки, обеспечьте надежную защиту системных файлов и реестра (для получения дополнительных сведений см. [контрольные списки требований по безопасности](https://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/iisbook/z02b_security_checklists.asp) на веб-узле [Microsoft Security](https://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/iisbook/z02b_security_checklists.asp%22%20%5Ct%20%22_blank) ).

Закон №3. Если у злоумышленника есть неограниченный физический доступ к вашему компьютеру, это больше не ваш компьютер

Вам интересно, что злоумышленник может сделать с компьютером, если сможет до него дотянуться? Что ж, вариантов масса — начиная от методов каменного века и заканчивая утонченными приемами эпохи освоения космоса.

* Устроить высокоэффективную низкотехнологическую атаку типа «отказ в обслуживании», от души врезав по компьютеру кувалдой.
* Отсоединить компьютер от всех кабелей, вынести его из здания, а потом потребовать за него выкуп.
* Загрузить компьютер с дискеты и отформатировать жесткий диск. Вы рассчитываете, что этому помешает установленный в BIOS пароль на загрузку? Не надейтесь — если злоумышленник сможет открыть корпус компьютера, он просто заменит микросхему BIOS (на самом деле, есть еще более простые способы обойти этот пароль).
* Извлечь из компьютера жесткий диск, подключить его к другому компьютеру и считать все данные.
* Сделать копию данных с жесткого диска и забрать с собой. Тогда у злоумышленника будет сколько угодно времени, чтобы подобрать пароли для входа в систему, а с помощью специальных программ, автоматизирующих данный процесс, он почти наверняка сможет это сделать. Когда это случится, вступят в действие указанные выше законы №1 и №2.
* Заменить вашу клавиатуру клавиатурой с радиопередатчиком, который позволит следить за всеми нажатиями клавиш, включая ввод паролей.

Всегда обеспечивайте физическую защиту компьютера, соответствующую его ценности. Помните, что ценность компьютера определяется не только стоимостью самого оборудования, но и ценностью хранящихся на компьютере данных *и*размером убытков, которые может повлечь за собой доступ злоумышленника к сети компании. Как минимум, необходимо, чтобы все важные компьютеры (такие как контроллеры доменов, серверы баз данных, файловые серверы и серверы печати) находились в отдельной запертой комнате, в которую могли бы заходить только сотрудники, уполномоченные выполнять задачи по администрированию и обслуживанию. Однако можно защитить и остальные компьютеры организации, а также предпринять дополнительные меры безопасности.

Пользователи, которые берут в поездки переносные компьютеры, обязаны позаботиться об их защите. Все те особенности переносного компьютера, которые делают его таким удобным в поездках — маленький размер, небольшой вес и так далее, — облегчают и его кражу. Существует целый ряд замков и сигнализаций для переносных компьютеров, а некоторые модели позволяют извлекать из компьютера жесткий диск и носить с собой. Кроме того, существуют дополнительные возможности, такие как шифрующая файловая система (EFS) в Microsoft Windows® 2000, уменьшающие ущерб, даже если переносной компьютер будет похищен. Однако единственный способ, гарантирующий, что данные находятся в безопасности, а компьютер не испорчен — это всегда носить его с собой.

Закон №4. Если злоумышленник смог загрузить приложения на ваш веб-узел, это больше не ваш веб-узел

Фактически, этот закон является зеркальным отражением закона №1. В первом случае злоумышленник заставляет пользователя загрузить вредоносное приложение на свой компьютер и выполнить его, а во втором — злоумышленник загружает вредоносное приложение на компьютер пользователя и выполняет его самостоятельно. Хотя эта опасность возникает каждый раз, когда к компьютеру подключаются посторонние лица, подавляющее большинство подобных случаев происходит с веб-узлами. Многие люди, которые управляют веб-узлами, слишком беспечны и позволяют посетителям загружать на веб-узел приложения и выполнять их. Как было показано выше, запуск на компьютере приложения злоумышленника может привести к крайне нежелательным последствиям.

Поэтому администраторам веб-узлов необходимо ограничивать права посетителей и разрешать выполнение на веб-узле только приложений, созданных доверенными разработчиками или лично администратором. Однако этого может оказаться недостаточно. Администраторы, веб-узлы которых размещаются на одном сервере с веб-узлами других пользователей, должны соблюдать особую осторожность. Если злоумышленник сможет преодолеть систему безопасности одного из веб-узлов этого сервера, возможно, ему удастся получить контроль над сервером в целом и, как следствие, — над всеми веб-узлами данного сервера. Поэтому при размещении веб-узла на общем сервере необходимо изучить политику администратора сервера (кроме того, прежде чем предоставлять доступ к своему веб-узлу всем пользователям Интернета, убедитесь, что выполняются рекомендации [контрольных списков требований по безопасности](https://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/iisbook/z02b_security_checklists.asp) для IIS 4.0 и IIS 5.0).

Закон №5. Ненадежные пароли делают бесполезной любую систему безопасности

Процесс входа в систему нужен для идентификации пользователя. Получив эти сведения, операционная система разрешает или запрещает доступ к соответствующим системным ресурсам. Если злоумышленник узнает пароль пользователя, он сможет входить в систему под именем этого пользователя. Фактически, операционная система будет считать, что **он и есть** этот пользователь. и, соответственно, позволит ему делать все, что может делать тот. Возможно, злоумышленник захочет ознакомиться с содержимым электронной почты и другими хранящимися на компьютере важными сведениями или выполнит какие-либо операции в сети, которые в другой ситуации были бы ему недоступны. А может, он просто попытается навредить и свалить вину на того пользователя, под именем которого он зашел в систему. В любом случае, чтобы избежать подобных последствий, необходимо защищать свои учетные данные.

Всегда используйте пароль (вы не поверите, узнав, сколько учетных записей имеют пустые пароли!), причем придумывайте что-нибудь посложнее. Не используйте в качестве пароля имя своей собаки, дату рождения или название любимой футбольной команды. И не вводите в качестве пароля слово «пароль»! Выбирайте пароли, содержащие строчные и заглавные буквы, цифры, знаки препинания и т. п. Используйте пароли максимальной длины и меняйте их как можно чаще. Выбрав надежный пароль, обращайтесь с ним надлежащим образом. Никогда не записывайте пароль. Если же записать пароль все-таки необходимо, спрячьте его в сейф или запирающийся шкаф — злоумышленники, пытающиеся узнать чужие пароли, первым делом изучают содержимое верхнего ящика стола и надписи на желтых наклейках, прилепленных к верхней части монитора. Никому не сообщайте свой пароль. Помните слова Бенджамина Франклина: «Два человека могут хранить тайну, только если один из них мертв».

И последнее — чтобы идентифицировать себя в системе, используйте более надежные средства, чем пароль. Например, Windows 2000 поддерживает применение смарт-карт, значительно повышающих надежность выполняемой системой проверки подлинности. Можно также использовать проверку отпечатков пальцев или сетчатки глаза и другие биометрические процедуры.

Закон №6. Безопасность компьютера напрямую зависит от надежности администратора

У каждого компьютера должен быть администратор — человек, который может устанавливать программное обеспечение, настраивать операционную систему, добавлять учетные записи пользователей и управлять ими, создавать политики безопасности и выполнять все остальные задачи по управлению компьютером, необходимые для поддержания его работоспособности. Для выполнения этих задач требуется полный контроль над компьютером — а это предоставляет администратору беспрецедентные возможности. Ненадежность администратора сделает бесполезными все остальные меры безопасности — он может изменить права доступа к компьютеру и политику безопасности системы, установить вредоносные приложения, добавить фиктивных пользователей, выполнить десятки других действий и обойти практически все защитные механизмы операционной системы, поскольку он ею полностью управляет. Хуже всего то, что он может уничтожить следы своих действий. Компания, в которой работает ненадежный администратор, абсолютно не защищена.

Принимая на работу системного администратора, помните о том, насколько ответственной является эта должность, и выбирайте того, кто заслуживает доверия. Проверьте его рекомендации и расспросите его о предыдущем месте работы, особенно если известно, что у его предыдущих работодателей возникали проблемы с безопасностью. Если возможно, поступите так, как поступают банки и другие компании, уделяющие повышенное внимание мерам безопасности, — потребуйте, чтобы при приеме на работу нового администратора была произведена полная проверка его анкетных данных, и регулярно выполняйте такую проверку в дальнейшем. Выбрав критерии, применяйте их ко всем без исключения — не предоставляйте никому (включая временных сотрудников и подрядчиков) административных полномочий в сети, пока соответствующий сотрудник не будет тщательно проверен.

Позаботьтесь, чтобы честные люди такими и оставались. Используйте книгу учета, чтобы регистрировать всех, кто заходит в серверную комнату (если в организации нет серверной комнаты с запирающейся дверью, перечитайте еще раз закон №3). Внедрите правило «двух ответственных» при установке и обновлении программного обеспечения. Разграничьте функции администраторов таким образом, чтобы уменьшить полномочия, предоставляемые каждому из них. Не используйте учетную запись «Администратор» — вместо этого создайте для каждого администратора собственную учетную запись с административными правами. Это позволит определять, кто из администраторов выполнял те или иные действия. И, наконец, обязательно предпринимайте меры, которые затруднили бы администратору-злоумышленнику сокрытие следов своих действий. Например, храните данные аудита на носителе, поддерживающем только однократную запись, или разместите журналы аудита системы А в системе Б, выбрав ее таким образом, чтобы у систем А и Б были разные администраторы. Чем полнее контроль за деятельностью администратора, тем меньше вероятность возникновения проблем.

Закон №7. Безопасность зашифрованных данных напрямую зависит от того, насколько защищен ключ расшифровки

Предположим, кто-то установил на свою входную дверь самый большой и надежный замок в мире, но при этом кладет ключ под коврик у порога. Важно ли при этом, насколько хорош сам замок? Самым слабым местом в этом случае будет являться ненадежная защита ключа, поскольку, если злоумышленник его обнаружит, у него будет все необходимое, чтобы открыть дверь. Шифрование данных работает таким же образом — независимо от того, насколько надежен алгоритм шифрования, данные не могут быть защищены надежнее, чем защищен ключ для их расшифровки.

Многие операционные системы и программные продукты для шифрования позволяют хранить ключ шифрования на компьютере. Преимуществом такого метода является его удобство — не надо заботиться о том, куда определить ключ, — однако за это приходится расплачиваться снижением безопасности. Как правило, при этом используются специальные методы сокрытия ключа (то есть ключ прячется на компьютере), некоторые из них достаточно эффективны. И все же, независимо от того, насколько хорошо спрятан ключ, — если он находится на компьютере, его можно найти. Действительно, раз его находит приложение шифрования, то, при большом желании, найдет и злоумышленник. Поэтому, если возможно, всегда используйте ключи, которые хранятся отдельно. Если ключом служит фраза или слово, запомните их. В противном случае экспортируйте ключ на дискету, сделайте ее резервную копию и храните обе копии в разных, хорошо защищенных местах (администраторам, использующим средство [Syskey](http://support.microsoft.com/default.aspx?scid=kb;en-us;143475&sd=tech" \t "_blank) в режиме локального хранилища, нужно сию минуту приступать к переконфигурации сервера).

Закон №8. Устаревшее антивирусное приложение лишь немногим лучше, чем его отсутствие

Антивирусное программное обеспечение сравнивает хранящиеся на компьютере данные с набором «сигнатур» вирусов. Каждая сигнатура соответствует отдельному вирусу, и если антивирусная программа обнаруживает эту сигнатуру в файле, сообщении электронной почте или где-либо еще, она решает, что обнаружила вирус. Однако антивирусные программы могут обнаруживать лишь известные им вирусы, а поскольку новые вирусы появляются ежедневно, необходимо всегда использовать последние версии файлов сигнатур.

Фактически, проблема несколько шире, чем описано выше. Как правило, наибольший ущерб новые вирусы причиняют на начальных этапах своего распространения, поскольку в это время их может обнаружить лишь небольшое число людей. Как только сведения о новом вирусе получают широкое распространение, пользователи обновляют сигнатуры вирусов, и темпы распространения вируса многократно снижаются. Поэтому очень важно, чтобы на момент вирусной атаки на компьютере использовались обновленные файлы сигнатур.

Практически все разработчики антивирусного программного обеспечения позволяют бесплатно загружать последние версии файлов сигнатур со своих веб-узлов. Более того, у многих из них существуют службы оповещения, уведомляющие пользователей о выпуске новых сигнатур. Пользуйтесь услугами этих служб. Помните, что необходимо обновлять не только сигнатуры, но и само антивирусное приложение, поскольку авторы вирусов регулярно разрабатывают новые технологии, требующие изменения методов работы антивирусных средств.

Закон №9. Абсолютная анонимность недостижима ни в жизни, ни в Интернете

Общаясь, люди каждый раз обмениваются сведениями. Если кто-то соберет достаточно сведений, он сможет узнать, кем является другой человек. Подумайте, сколько сведений узнают собеседники друг о друге даже в коротком разговоре! С первого взгляда они могут оценить рост, вес и приблизительный возраст партнера по коммуникации. В дальнейшем собеседник может сообщить, из какой он страны, и даже из какого региона. Если говорить с человеком о чем-то, кроме погоды, возможно, он расскажет о своей семье, увлечениях, месте жительства и работе. Итак, не составляет никакого труда собрать достаточно сведений о другом человеке. Чтобы сохранить полную анонимность, лучше всего жить в пещере и прекратить все контакты с другими людьми.

То же самое можно сказать про Интернет. Владельцы посещаемых пользователем веб-узлов при необходимости смогут узнать, кто он такой — ведь единицы и нули, формирующие содержимое веб-узла, находят путь к своему месту назначения, которым является компьютер данного пользователя. Существует множество способов, позволяющих скрыть место назначения этих битов, и чем больше таких способов будет использоваться, тем труднее будет определить подлинное место назначения. Например, можно скрыть свой фактический IP-адрес с помощью преобразования сетевых адресов, воспользоваться службами обеспечения анонимности, передающими эти биты из одного конца Интернета в другой, применять для обращения к разным веб-узлам учетные записи различных поставщиков услуг Интернета, обращаться к веб-узлам только из интернет-кафе и т. п. Все эти методы затрудняют обнаружение пользователя, обращающегося к веб-узлу, но не исключают его полностью. Например, может оказаться, что службами обеспечения анонимности управляет тот же человек, что и веб-узлом, к которому обращался пользователь. А владелец веб-узла, предложивший бесплатно отправить пользователю по почте купон на скидку в 10 долларов, может поделиться сведениями об этом пользователе с владельцами других веб-узлов. В результате кто-то, сопоставив сведения, полученные с разных веб-узлов, сможет определить личность пользователя.

Означает ли это, что попытки соблюдения конфиденциальности в Интернете — лишь пустая трата времени? Ни в коем случае. Это означает, что в Интернете, как и в обычной жизни, наилучший способ сохранить конфиденциальность — вести себя надлежащим образом. Изучайте заявления о конфиденциальности посещаемых веб-узлов и используйте только те узлы, с правилами которых вы согласны. Если считаете нужным, отключите использование файлов cookie. А самое важное правило — избегайте беспорядочного блуждания по веб-узлам; помните, что в Интернете, как и во всех городах, есть неблагополучные места, в которые лучше не заходить. Однако, если вы хотите сохранить полную анонимность, лучше начните поиски подходящей пещеры.

Закон №10. Технология не является панацеей

Технология может творить поразительные вещи. Мы видим, как в последние несколько лет появляется все более мощное и дешевое оборудование и программное обеспечение, использующее это оборудование и открывающее пользователям компьютеров новые возможности, а также способствующее прогрессу в криптографии и других науках. И хочется верить, что в конце концов новые технологии избавят мир от опасностей. К сожалению, это невозможно.

Для создания идеальной системы безопасности требуется уровень развития технологий, который недостижим на сегодняшний день и вряд ли будет достигнут когда-либо в будущем. Это утверждение в равной степени относится как к программному обеспечению, так и почти ко всем областям человеческой деятельности. Разработка программного обеспечения — несовершенная наука, и во всех программных продуктах есть ошибки, некоторые из которых приводят к возникновению уязвимостей в системе безопасности. Это — реальность нашей жизни. Однако, даже если удастся создать идеальное приложение, это не решит проблему в целом — большинство атак в той или иной степени использует особенности человеческого характера (как правило, подобные методы атак называют социальной инженерией). Повышение сложности и трудоемкости преодоления технологических компонентов системы безопасности приводит к тому, что основными объектами атак злоумышленников становятся сотрудники, работающие за компьютерами. Поэтому необходимо, чтобы каждый сотрудник понимал свою роль в поддержании общей безопасности. В противном случае он может стать тем слабым звеном, из-за которого рухнет защищаемая им же система.

Чтобы решить эту проблему, необходимо знать следующие правила. Во-первых, система безопасности включает как технологические компоненты, так и политику — то есть она объединяет технологии и методы их применения, и именно это сочетание определяет уровень защиты системы. Во-вторых, обеспечение безопасности — это непрерывный процесс, а не конечная цель. Это не проблема, которую можно однажды «решить» и забыть о ней навсегда, а постоянная борьба между злоумышленниками и теми, кто осуществляет защиту. Руководители компании должны быть уверены в том, что сотрудники хорошо осведомлены о возможных проблемах безопасности и умеют правильно оценивать ситуацию. Существуют различные ресурсы, которые могут помочь в решении этой задачи. Например, веб-узел Microsoft Security содержит сотни документов, рекомендаций, контрольных списков и программных средств, а сотрудники корпорации Майкрософт постоянно работают над созданием новых продуктов. Используйте современные технологии и не забывайте о необходимости рационального подхода к проблеме — тогда ваши системы будут надежно защищены.