ОСНОВНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под информационной безопасностью понимается состояние защищенности информационной среды. Соответственно, защита информации понимается как действия по предотвращению возможного повреждения или уничтожения информации, а также несанкционированного доступа к ней (но вместе с тем — обеспечение беспрепятственного доступа к информации со стороны легитимных пользователей). Особо может рассматриваться информационная безопасность организации (как состояние защищенности информационной среды некоторой организации, например, образовательного учреждения), а также информационная безопасность государства (как состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере).

В современных условиях информационная безопасность общества и государства может рассматриваться как совокупность информационно-технической и информационно-психологической (психофизической) безопасности.

Меры по обеспечению информационной безопасности можно разделить на *технические* (различные аппаратные и программные средства и технологии защиты от вредоносных программ, внешних сетевых атак и пр.; к ним, в частности, относятся все ранее рассмотренные в данном курсе антивирусные программы) и *правовые*, под которыми понимается совокупность нормативных и правовых актов, регулирующих вопросы защиты информации.

Правовые основы информационной безопасности

Основным законом, касающимся вопросов использования и защиты информации, в нашей стране является *Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»*, принятый 27 июля 2006 г.

взамен ранее действовавшего Федерального закона № 24-ФЗ «Об информации, информатизации и защите информации» от 20 февраля 1995 г.

В частности, статья 1 Закона «Об информации, информационных технологиях и о защите информации» гласит, что данный закон «регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации».

Статья 3 формулирует понятия «безопасность» и «защита информации» в рамках принципов правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Причем в качестве одного из основных принципов постулируется «обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации».

А вот статья 10, носящая название «Распространение информации или предоставление информации», уже напрямую касается проблемы спам-рассылок:

- пункт 2: «Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица»;
- пункт 3: «При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации»;
- пункт 4: «Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией».

Следовательно, противозаконной является рассылка любой информации, в которой отсутствуют точные и достоверные сведения о ее распространителе, причем даже при наличии

таких сведений пользователь должен иметь возможность отказа от получения этой информации. Однако если вы сами где-либо подписались на электронную рассылку, то ее отправка вам становится законной в соответствии с любыми теми условиями, которые указаны в правилах этой рассылки или в соответствующем «публичном договоре». Поэтому прежде чем нажать кнопку «подписка» на каком-нибудь сайте, обязательно прочтите внимательно соответствующие правила!

Далее, статья 16 Закона «Об информации, информационных технологиях и о защите информации» рассматривает уже основные понятия и положения, касающиеся защиты информации:

- пункт 1: «Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
  1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации,
  2) соблюдение конфиденциальности информации ограниченного доступа,
  3) реализацию права на доступ к информации»;
- пункт 2: «Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации»;
- пункт 4: «Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:
  1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации,
  2) своевременное обнаружение фактов несанкционированного доступа к информации,

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации,
4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование,
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней,
6) постоянный контроль за обеспечением уровня защищенности информации».

Эти положения закона относятся, например, к администрации и техническим службам организаций, поддерживающих размещенные в Интернете базы данных, к владельцам серверов для размещения пользовательских сайтов и т. д.

Наконец, статья 17 рассматриваемого Закона определяет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации:

- пункт 1: «Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации».

То есть любые деяния, приводящие к повреждению или уничтожению информации, к ее намеренному искажению, равно как и стремление получить неправомерный доступ к чужой конфиденциальной информации, — то, чем, собственно, и занимаются авторы вирусов, «троянов» и других вредоносных программ, — являются ***преступлением***, со всеми вытекающими отсюда последствиями. О том, какими могут быть эти последствия, мы поговорим чуть позже.

Еще один законодательный акт — *Федеральный закон № 152-ФЗ «О персональных данных»*, вступивший в действие 27 июля 2006 г., определяет основные понятия и положения о защите персональной, т. е. личной информации каждого человека. Так, статья 3 гласит, что персональные данные — это «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому

лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация». А согласно пункту 1 статьи 6, обработка таких персональных данных может осуществляться оператором только с согласия субъектов этих персональных данных, за исключением лишь особо оговоренных пунктом 2 этой статьи случаев. Тем самым еще раз подчеркивается противозаконность действий, приводящих к несанкционированному доступу и хищению личной информации пользователей, даже если такое хищение не привело к непосредственному материальному ущербу.

Что же грозит тем, кто, несмотря на предупреждения двух рассмотренных выше законов (причем незнание закона, как известно, не освобождает от ответственности!), будет создавать вредоносные программы или производить какие-либо вредоносные действия либо пытаться получить несанкционированный доступ к чужой информации? В России соответствующие меры наказания определены в *Уголовном кодексе Российской Федерации* (*УК РФ*), носящем номер 63-ФЗ и вступившем в действие 13.06.1996 г. Преступления, связанные с компьютерной информацией, рассмотрены в нем в главе 28, где содержатся три следующие статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Приведем здесь полностью их текст.

Статья 272
Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло унич-

тожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается **штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.**

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается **штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.**

Статья 273
Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами — наказываются **лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.**
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются **лишением свободы на срок от трех до семи лет.**

Статья 274
Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, — наказывается **лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет**
2. То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается **лишением свободы на срок до четырех лет.**

Таким образом, создание вредоносных программ, несмотря на «виртуальный» характер, является реальным преступлением и карается реальными штрафами (чаще всего — с конфискацией соответствующего компьютерного оборудования), а в отдельных случаях — реальными тюремными сроками (и далеко не всегда условными).

Впрочем, в других странах наказание за информационные преступления бывают еще строже. Например, на Филиппинах в настоящее время принят закон, предусматривающий за разработку вирусов **смертную казнь**.

Заметим, кстати, что высокий уровень знаний принципов работы компьютера и операционных систем и программистских умений, которыми любят хвастаться хакеры, не спасает их от возмездия. Вот перечень фамилий целого ряда знаменитых хакеров, попавших, несмотря на все свои ухищрения, в руки правосудия:

- Кэвин Митник — был арестован 15 февраля 1995 г. в городе Рэлей (Северная Каролина), когда его сумел выследить компьютерный эксперт Цитому Шимомура. На суде Митник признал свою вину по большинству предъявленных обвинений и был приговорен к 46 месяцам реального и трем годам условного заключения, а также к выплате значительного штрафа (Митник вышел на свободу из тюрьмы 21 января 2000 г.);

- Пьер-Ги Лавуа, 22-летний канадский хакер, согласно канадским же законам, был приговорен к 12 месяцам общественных работ и к условному заключению на 12 месяцев за подбор паролей с целью проникновения в чужие компьютеры;
- наш соотечественник, 26-летний Василий Горшков из Челябинска, 10 октября 2001 г. был приговорен по 20 пунктам обвинения за многочисленные компьютерные преступления, совершенные против сети Speakeasy в Сиэтле (Вашингтон), банка Nara в Лос-Анджелесе (Калифорния), Центрального национального банка Вако в Техасе и онлайновой платежной компании PayPal из Пало-Альто (Калифорния);
- Олег Зезев, гражданин Казахстана, 1 июля 2003 г. был приговорен Манхэттенским федеральным судом к 51 месяцу заключения за компьютерное вымогательство.

Основы лицензионной политики в сфере распространения программ и данных

Итак, согласно закону, распространение, доступ и использование информации строго регламентируется, поэтому легальное (т. е. законное) распространение и использование любых программ, а также данных (например, информации в составе баз данных) должно осуществляться согласно определенным правилам. Набор таких правил, устанавливаемый (в рамках, допустимых законом) собственником программы — ее создателем или продавцом, называют *лицензией* (*пользовательской лицензией*). Соответственно, *лицензионная политика* рассматривается как комплексный механизм, определяющий всю совокупность условий предоставления той или иной программы пользователям, включая систему ценовых скидок и оговоренные в лицензии ограничения и специальные условия ее использования.

Виды ПО

По принципам распространения и использования, согласно соответствующим лицензиям, программное обеспечение делится на следующие виды:

Коммерческое программное обеспечение (*commercial software*) — это программы и программные пакеты, распространяемые только путем продажи. Возможен также вариант, когда сама программа предоставляется бесплатно, а продаже подлежит, например, подписка на осуществляемые при помощи этой программы онлайн или иные услуги. Возможен и случай, когда плата взимается как за саму программу (однократно при ее покупке), так и в виде абонентской платы за некоторый период времени. Примером является «Антивирус Касперского»: купив саму программу, далее нужно оплачивать только подписку на услугу по регулярному обновлению антивирусных баз, что необходимо для полноценной работы антивируса.

Разновидностями коммерческого ПО являются также *пробные версии программ*. Как правило, это разновидности

соответствующей коммерческой программы, распространяемые бесплатно в рекламных целях, но ограниченные по функциям по сравнению с полноценной версией либо полнофункциональные, но работающие только в течение ограниченного периода времени (оговоренное количество дней либо количество запусков) после установки, после чего пробная программа либо перестает работать вовсе, либо переходит в режим с ограниченным функционалом. Примером такого вида ПО (или, точнее, способа распространения и рекламы соответствующих коммерческих программ) является все тот же «Антивирус Касперского»: можно скачать с сайта саму программу, получить к ней «пробный» ключ доступа к обновлениям вирусных баз на 1 месяц, а по завершении этого периода (если не оплатить подписку на дальнейшее обновление вирусных баз) программа перейдет в ограниченный режим: ее функции по проверке и лечению ранее известных программе вирусов сохранятся, но функции обновления вирусных баз будут отключены.

Условно-бесплатное ПО (*shareware*) — это программы (как правило, созданные индивидуальными программистами-любителями), которые можно получить и использовать бесплатно, но с определенными ограничениями, указанными в лицензии (например, разрешается бесплатное использование только в некоммерческих, личных целях или в образовательных учреждениях), либо имеется обращение к пользователю с просьбой о небольшом добровольном денежном пожертвовании в качестве вознаграждения автору в качестве стимула к дальнейшему совершенствованию программы, если она понравилась данному пользователю. Примером этого класса ПО является антивирус Avira AntiVir Personal-Edition Classic, который можно бесплатно использовать на личном компьютере или в школе.

Бесплатное ПО (*freeware*) — это программы, которые, согласно лицензии, вообще не требуют никаких денежных выплат автору (ограничиваются лишь возможные действия пользователя по отношению к этой программе, — например, допускается только ее личное использование «как есть», но не разрешено что-либо менять в исполняемом коде, переписывать программу другим лицам и т. д.). Как правило, это

программы, созданные отдельными энтузиастами «для себя и для друзей» либо написанные начинающими программистами, желающими «создать себе имя». В некоторых случаях бесплатное ПО также создают крупные фирмы, если этого требует какая-либо важная цель: например, «Лаборатория Касперского» предлагает посетителям своего сайта целый ряд бесплатных антивирусных утилит, нацеленных на борьбу с отдельными вредоносными программами, — ради того, чтобы как можно быстрее «погасить» ту или иную вирусную эпидемию.

Заметим, что все указанные программы относятся к категории *проприетарного*, или *«собственнического» программного обеспечения*, поскольку во всех описанных разновидностях предполагается, что программа (даже бесплатная, freeware) кому-то принадлежит: пользователь покупает или получает на иных условиях право использовать такую программу, но не имеет права что-либо менять в ней или копировать программу другим лицам.

Противоположностью проприетарного является *свободное* или *открытое программное обеспечение*. Как правило, оно тоже является бесплатным (а оплата может браться только за сборку комплекта дистрибутивов с учетом их тестирования на возможные взаимные конфликты, выполнения русификации программ и пр.). Сами категории свободного и открытого ПО в основном аналогичны и различаются небольшими нюансами.

Так, *свободное ПО* (*free software*) предполагает, что пользователю (согласно особой, свободной лицензии) предоставляются права («свободы») на неограниченные установку, запуск, свободное использование, изучение, распространение и изменение (совершенствование) таких программ.

В отличие от вышесказанного, сторонники *открытого ПО* (*open source software*) делают основной акцент на предоставлении вместе с исполняемой программой ее исходного программного кода (листинга), открытого для просмотра, изучения и внесения изменений. Поэтому открытой лицензией не запрещается ни дорабатывать открытую программу (вносить изменения и исправления в ее исходный код с последующей компиляцией в новую версию исполняемой програм-

мы), ни использовать фрагменты такого исходного кода для создания собственных программ (хотя при этом может ставиться условие, что программы, содержащие такой заимствованный исходный код, могут далее распространяться тоже только как открытые). А вот свободность и даже бесплатность открытых программ необязательны, хотя большинство открытых программ также одновременно являются и бесплатными. Обратным примером является, скажем, утилита UnRAR — распаковщик RAR-архивов: ее исходный код имеется в открытом доступе для распространения и изменения, но, согласно лицензии, его нельзя использовать для создания RAR-совместимых архиваторов, т. е. эта утилита не является полностью свободной.

Коммерческая лицензия

Рассмотрим типовые условия, указанные в лицензии (лицензионном соглашении) на коммерческую программу (на примере пользовательской лицензии на «Антивирус Касперского»[1]). Процитируем ее текст.

Лицензионное соглашение

Исключительные имущественные авторские права на ПО (программа, сигнатуры угроз, база сетевых атак, база антиспама) и Руководство пользователя в печатном и/или электронном виде принадлежат Правообладателю.

В случае если Вы приобрели ПО через Интернет, нажатие Вами кнопки «Согласен» означает Ваше безоговорочное согласие с условиями настоящего Соглашения. Если Вы не согласны с условиями настоящего Соглашения, Вы должны прекратить инсталляцию ПО.

С момента инсталляции ПО:

1. Вы имеете право использовать ПО для защиты объектов, указанных в настоящем Лицензионном Соглашении. Количество защищаемых объектов также указано в настоящем Лицензионном Соглашении.

---

[1] http://www.softkey.ru/catalog/license_view.php?l=p&p_id=28760&strlang=ru

2. С момента покупки ПО в течение срока, указанного в настоящем Лицензионном Соглашении, Вы имеете право получать от Правообладателя или его партнеров:
   - новые версии ПО, включая сигнатуры угроз (сигнатуры вирусов, образцов спама и сетевых атак), по мере их выхода (через Интернет);
   - техническую поддержку (по телефону и/или через Интернет);
   - новые версии сигнатур угроз для лечения обнаруженного Вами ранее неизвестного вируса. Изготовление обновления сигнатур угроз для лечения ранее неизвестного вируса выполняется в течение 48 часов после получения вируса Правообладателем;
   - дубликат ключевого файла.
3. Сервисы, описанные в п. 2 настоящего Соглашения, предоставляются при условии установки пользователем последнего обновления последней версии ПО.
4. Правообладатель не гарантирует Пользователю качественную защиту объектов, указанных в п. 1 настоящего Соглашения, в случае, если пользователь не осуществляет обновлений ПО и сигнатур угроз.
5. Правообладатель не гарантирует Пользователю защиту объектов, указанных в п. 1, по окончании срока, указанного в п. 2 настоящего Соглашения.
6. Пользователь может использовать в ПО расширенный набор антивирусных баз; в этом случае ПО обнаруживает не только вредоносные, но и потенциально опасные программные продукты, относящиеся к категориям Adware, Riskware, Pornware и т. п.
7. Правообладатель не несет ответственности за какой-либо ущерб, связанный с использованием расширенного набора антивирусных баз (например, ПО может привести к неработоспособности и/или удалению программных продуктов, относящихся к категориям Adware, Riskware, Pornware и т. п. Отнесение программных продуктов к перечисленным категориям осуществляется Правообладателем по классификации Правообладателя).

8. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Указанная в настоящем пункте копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.
9. Вы имеете право продать имеющийся у Вас экземпляр ПО лицу, согласному с условиями настоящего Соглашения, при этом Вы перестаете быть правомерным владельцем экземпляра ПО и обязаны уничтожить все оставшиеся у Вас копии ПО, включая архивную.
10. Запрещается производить декомпиляцию и/или модификацию ПО.
11. Запрещается сдавать ПО в аренду, прокат или во временное пользование.
12. Запрещается разделять ПО на составляющие части для использования их на разных компьютерах.
13. Запрещается использовать ПО с целью создания данных или кода, предназначенных для детектирования, блокирования или лечения вредоносных программ и данных (сигнатур и процедур детектирования вредоносных программ).
14. Правообладатель гарантирует работу ПО в соответствии с условиями, описанными в Руководстве пользователя.
15. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Руководстве пользователя, а также в случае нарушения Пользователем условий настоящего Лицензионного Соглашения.
16. Правообладатель и/или его партнеры не несут ответственности за какой-либо ущерб, связанный с использованием или невозможностью использования ПО. За нарушение авторских прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Таким образом, данная лицензия указывает следующее:

- поскольку исключительные имущественные права на все компоненты поставляемого программного пакета принадлежат Правообладателю (т. е. «Лаборатории Касперского»), покупка антивирусной программы не передает Пользователю никаких прав собственности на нее, а передает только перечисленные ниже в лицензии права на использование этой программы при соблюдении ряда оговоренных условий, а также права на получение обновлений и указанных в лицензии сервисных услуг;
- для юридической фиксации соглашения между Правообладателем и Пользователем достаточно, чтобы Пользователь выразил свое согласие, нажав на кнопку **Согласен** и продолжив установку программы (а не прервав этот процесс), — никаких подписей под тем или иным документом (как это обычно делается при заключении договоров) от обеих сторон соглашения не требуется;
- четко оговорено, что именно Пользователь может делать с программой (или с ее помощью) и какие еще услуги (и при каких условиях) он может получать от Правообладателя;
- определяется возможность для Пользователя изготавливать для себя «страховочную» (архивную) копию программы, а также полностью передавать свои права, оговоренные лицензией, другому Пользователю;
- указаны действия над программой, которые запрещено производить Пользователю;
- наконец, присутствует ряд указаний на ситуации, в случае которых Правообладатель (как изготовитель программы) снимает с себя ответственность за неправильную работу либо полную неработоспособность самой программы, а также за возможный прямой или косвенный ущерб от ее использования.

В других образцах текста лицензии также могут оговариваться условия использования программы в каких-либо конкретных ситуациях (например, только некоммерческое, только личное, только в образовательных учреждениях), количество компьютеров, на которые может быть установлена данная программа с одного приобретенного дистрибутива и т. д.

Кроме лицензии, в некоторых случаях для подтверждения лицензионных прав пользователя предусматривается *сертификат подлинности* (*лицензионный сертификат*), на котором указаны наименование программного продукта и *«ключ продукта»* (*Product Key*) в виде некоторого *серийного номера*.

Открытая лицензия GNU GPL

В отличие от коммерческой, *открытая лицензия* (*GNU General Public License*, *GNU GPL*) удостоверяет, что данное ПО является свободным для всех его пользователей, и гарантирует им свободу использовать и изменять это ПО. Она была создана в рамках проекта GNU в 1988 г., а позже были созданы вторая (в 1991 г.) и третья ее версия (в 2007 г.). Цель лицензии GNU GPL — предоставить пользователю следующие права («свободы»):

- свободу запуска программы с любой целью;
- свободу изучения исходного кода программы, принципов ее работы и ее улучшения (модификации);
- свободу распространения копий программы;
- свободу улучшений и доработок программы и выпуска новых ее версий в публичный доступ.

Кроме того, лицензия GNU GPL гарантирует, что пользователи всех программ, созданных на основе упомянутого исходного кода, тоже получат все вышеперечисленные права. Например, запрещается создавать на основе свободной программы с лицензией GPL какое-либо другое ПО, в комплекте которого не будет предоставлен открытый исходный листинг.

Более подробно текст открытой лицензии GNU GPL мы здесь рассматривать не будем. Интересующиеся могут ознакомиться с ним, например, на сайтах:

- http://www.gnu.org/copyleft/gpl.html — исходный английский текст;
- http://www.citforum.ru/operating_systems/articles/gpl_rus.shtml — неофициальный русский перевод.

Угрозы при использовании нелицензионного ПО

Нелицензионным (*пиратским*) называют программное обеспечение, полученное и/или используемое незаконным способом, т. е. в нарушение правил пользовательской лицензии (как правило, от третьих лиц или через третьих лиц[1], не имеющих прав на распространение такой программы).

Что же грозит вам и вашему компьютеру при использовании нелицензионного программного обеспечения?

Во-первых, распространение и использование нелицензионного ПО является нарушением *Закона об охране авторских прав*, за что виновный несет гражданскую, административную или уголовную ответственность. Подробно этот аспект мы рассматривать не будем; желающие могут обратиться к тексту Закона РФ «Об авторском праве и смежных правах».

Во-вторых, практически любая современная программа, распространяемая на коммерческой основе, содержит встроенные средства контроля нелицензионного использования (защита от несанкционированного копирования): это может быть индивидуальный серийный номер либо специальная *процедура «активации»*, специальный ключевой файл, аппаратный ключ, вставляемый в один из портов компьютера, и т. д. Конечно, абсолютной защиты, которую невозможно было бы «взломать», практически не существует, — однако, «взламывая» подобную защиту, хакер может по незнанию повредить остальной программный код. В этом случае работа «взломанной» программы становится нестабильной, она может время от времени аварийно прекращать работу, в ней могут не работать некоторые функции[2] либо даже такая

---

[1] В юридических документах «третьим лицом» называют кого-либо, кто не является одним из участников заключенного договора, документа и т. д. (т. е. кто-то посторонний). Если нелицензионное ПО было переписано из Интернета, то это означает, что существует кто-то, кто в нарушение Закона об охране авторских прав разместил эту программу в Интернете (на сайте, в файловой коллекции, сети файлообмена и пр.). Поэтому и в этом случае речь идет о незаконном получении программы от третьих лиц.

[2] Например, при нелицензионном использовании антивирусной программы становится невозможным своевременное автоматическое обновление ее вирусных баз, из-за чего программа теряет существенную часть своей эффективности.

программа может портить информацию, имеющуюся на диске. Более того, хакеры нередко используют «взломанные» программы в качестве своеобразной «приманки», встраивая в них «троянские программы» для своих преступных целей. Разумеется, ни в том, ни в другом случае изготовитель программы не несет никакой ответственности за нанесенный ею ущерб.

Наконец, в-третьих, сайты (а нередко — и диски), посредством которых распространяются «взломанные» программы либо различные средства для их «взлома» пользователями (серийные номера, программы — «генераторы серийных номеров», утилиты[1] для отключения средств контроля нелицензионного использования и т. п.), нередко бывают заражены вредоносными программами различных видов: опять-таки возможность бесплатно заполучить дорогостоящую программу используется как «приманка».

Таким образом, пользуясь нелицензионным программным обеспечением, вы подвергаете опасности данные, которые хранятся на вашем компьютере. А в результате вам в лучшем случае потребуется заново переустанавливать операционную систему и все прикладное ПО, а в худшем это может привести к невосстановимой потере результатов вашей работы за длительный период времени либо даже к тому, что ваша конфиденциальная информация (а может быть, даже и деньги) окажется в руках злоумышленников. Подобный ущерб может оказаться существенно большим, чем стоимость полноценной коммерческой версии программы.

---

[1] *Утилита* — компьютерная программа, расширяющая стандартные возможности оборудования и операционных систем, выполняющая узкий круг специфических задач.