Смирнова А.Д., Гулякин Д.В.

Риски, связанные с использованием нелицензионного программного обеспечения

*Кубанский государственный технологический университет
(Россия, Краснодар)*

doi: 10.18411/trnio-10-2021-47

Аннотация

Лицензия на программное обеспечение - это правовой инструмент, определяющий использование и распространение программного обеспечения, защищённого авторским правом. Обычно лицензия на программное обеспечение разрешает получателю использовать одну или несколько копий программы, причём без лицензии такое использование рассматривалось бы в рамках закона как нарушение авторских прав издателя. В статье рассмотрены виды рисков и ответственности юридических и физических лиц за использование нелицензионного программного обеспечения.

Ключевые слова: нелицензированное программное обеспечение, уголовная и административная ответственность, кибербезопасность, нарушение авторских прав.

Abstract

A software license is a legal instrument that determines the use and distribution of copyrighted software. Usually, a software license allows the recipient to use one or more copies of the program, and without a license, such use would be considered by law as a violation of the publisher's copyright. The article considers the types of risks and responsibilities of legal entities and individuals for the use of unlicensed software.

Keywords: unlicensed software, criminal and administrative liability, cybersecurity, copyright infringement.

При пользовании любым программным обеспечением (ПО) юридические и физические лица должны соблюдать авторское право разработчика. Установленное любое нелицензионное ПО и пользование базами данных автоматически делает пользователя ответственным перед законом об авторском праве. Покупатели нелегального программного обеспечения несут административную, уголовную, а также гражданско-правовую ответственность в соответствии с законодательством РФ.

По оценкам ассоциации Business Software Alliance, на нелицензионный софт в России приходится около 64% всех установок ПО.

В настоящий момент существует три способа присоединения к лицензионному соглашению:

- при покупке компьютера на нем может быть предустановлено программное обеспечение. Это так называемые OEM-версии. Подтверждением заключения лицензионного соглашения в данном случае служат специальные наклейки на корпусе компьютера и документация на сам компьютер с указанием, какие программы на нем были установлены;
- приобретение программного обеспечения на информационном носителе в магазине. Так называемые «коробочные версии». К таким программам может прилагаться соответствующая наклейка, она может быть прикреплена к самой коробке, в этом случае ее также необходимо сохранить. Кроме того, доказательствами заключения лицензионного договора в данном случае служат чеки, сопроводительная документация, прикладываемая к информационному носителю;
- «корпоративное лицензирование». В этом случае организация осуществляет контакт с официальным представителем правообладателя и заключает лицензионное соглашение с ним. В данном соглашении определяется

наименование и количество программ, количество рабочих станций (компьютеров) на которых они могут использоваться. Как правило, в этом случае также выдаются наклейки-сертификаты. Кроме того, подтверждением служит подписанный текст лицензионного соглашения, а также документы, подтверждающие оплату [2].

Существует ряд международных и российских стандартов как по информационной безопасности в целом так и управлению информационными рисками в частности, которые описывают информационные риски как со стороны информационных технологий так и со стороны менеджмента.

Главный международных стандартов управления информационной безопасностью – стандарт BS 7799. Этот документ является практическим руководством по управлению информационной организации. В нем описано 10 областей и 127 механизмов контроля, необходимых для построения систем безопасностью, определенных на основе лучших примеров из мировой практики.

Контролем деятельности компании занимается Министерство по борьбе с экономическими преступлениями. Основанием для проверки фирмы являются свидетельства того, что фирма занимается незаконной деятельностью. К примеру, это может быть жалоба от правообладателя или агентства по защите авторских прав, распространителя ПО.

Поводом для возбуждения административных/уголовных дел по фактам использования пиратского ПО может являться (ст. 28.1 КоАП РФ и ст. 140 УПК РФ):

- обнаружение нарушения непосредственно сотрудником правоохранительных органов;
- заявление правообладателя;
- сообщение о нарушении/преступлении, полученное из СМИ и иных источников [1].

Обновления программ - такие же объекты интеллектуальной собственности, как и само программное обеспечение. Помимо правовой и юридической защиты, могут использоваться и технологические, программные способы защиты обновлений. Незаконное обновление программ чревато судимостью, и такие прецеденты уже есть. В зависимости от способа обхода защиты, и распространителю, и исполнителю, и пользователю могут вменить как ст. 272 УК РФ, так и 273 УК РФ (максимальное наказание по ним - лишение свободы на срок до 5 лет) [1].

Существуют следующие риски [2-5].

1. Риски, связанные с безопасностью - пытаясь обойти закон и сэкономить, пользователь от лица своей компании может стать не только преступником, но и жертвой. Ведь использование пиратского софта ставит под угрозу сохранность критически важных для бизнеса данных. Однако скачивание и установка ПО из неизвестных источников может повлечь взлом или утечку критически важных бизнес-данных.
2. Репутационные - они наиболее очевидны. Любая компания на рынке стремиться позиционировать себя как надежного партнера, который никогда не оставляет обязательства незакрытыми. А вот использование пиратского ПО может нанести ее репутации непоправимый ущерб. Отношение к уличенным в таком преступлении компаниям также намного хуже. Контрафактные программы зачастую могут содержать ошибки, которые приводят к неточностям в работе. И это тоже сказывается на репутации компании. При использовании нелегального ПО на стадии проектирования, неправильные расчеты, некорректная аналитика и ошибки в разработке устройства могут быть весьма критичными.
3. Технические - нелегальное ПО нередко не дает пользователю возможности своевременно получать обновления, направленные на исправления ошибок в коде, ведущих к сбоям, сложности в скачивании

обновлений. И само по себе вмешательство в код программных продуктов распространителями пиратского ПО может служить причиной некорректной или нестабильной работы.

4. Финансовые - включают в себя несоблюдение правил лицензирования (некоторые продукты могут быть бесплатными только для некоммерческого использования, поэтому предприниматель должен знать, что, устанавливая такие продукты для работы, он нарушает условия лицензионного соглашения, а следовательно, и закон) и отсутствие необходимой экспертизы (покупка одной лицензии не всегда дает права установить ее на любые устройства, а тем более сразу на несколько устройств).
5. Юридические - административная ответственность за нарушение авторских прав наступает в соответствии со ст. 7.12 КоАП РФ «Нарушение авторских и смежных прав, изобретательских и патентных прав», уголовная ответственность (в соответствии с п. 2 ст. 146 УК РФ «незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, наказываются») и гражданско-правовая ответственность.

Как видно, использование нелегального программного обеспечения невыгодно не только его разработчикам, но и пользователям. Приобретая продукты у правообладателя или его официального представителя, компания исключает большое количество рисков и помимо спокойствия получает гарантии качества и стабильности работы.

Весь спектр программных обеспечений просто неиссякаем. На сегодняшний день рынок ПО растет, появляются новые программы. Какие-то из них останутся неизвестными, какие-то получают мировое признание. Создание программного обеспечения для персональных компьютеров за какой-то десяток лет превратилось из занятия программистов-одиночек в важную и мощную сферу промышленности. Помимо этого, создание новых программ влечет за собой развитие новых комплектующих, способных полностью покрыть все требования программы, необходимые для нормального её функционирования. Многочисленные разновидности лицензионных соглашений предоставляют правообладателю широкий набор инструментов для эффективной реализации и защиты своих прав на программное обеспечение. Конечные пользователи, приобретающие программное обеспечение, должны знать о юридических рисках использования нелегальных программных продуктов.

1. Нелегальные программы: ответственность за использование [<https://buh.ru/articles/documents/82643/>], Дата обращения (11.09.2021 г.)
2. Нелегальное программное обеспечение: риски и ответственность// Россол Сергей [<http://delo-press.ru/articles.php?n=5013>], (Дата обращения 11.09.2021 г.)
3. Нелегальное программное обеспечение и риски для кибербезопасности // Павел Сопер, Джон Ф. Грантц.[http://globalstudy.bsa.org/2013/Malware/study_malware_ru.pdf], Дата обращения (12.09.2021 г.)
4. Gulyakin D, Babaeva E., Magomedova R., Panova I. и др. Transgression of culturological approach in the practise of the Russian higher education. // Life Sci J 2014;11(9s):188-191, USA, (ISSN:1097-8135). <http://www.lifesciencesite.com>. 36.
5. Гулякин Д.В. Современный вуз как среда, реплицирующая культуру общества // Научное обозрение. Серия 2: Гуманитарные науки. – 2012. – № 6. – С. 91-95.