Горбачев А.Ю., Гулякин Д.В.

Риски, связанные с использованием нелицензионного программного обеспечения

*Кубанский государственный технологический университет
(Россия, Краснодар)*

doi: 10.18411/lj-01-2021-05

idsp: ljjournal-01-2021-05

Аннотация

Правоохранительные и государственные органы на сегодняшний день практически в каждой стране все в большей степени обращают внимание и стараются предотвратить нарушения в сфере пользования организациями нелицензионного программного обеспечения (ПО). В связи с этим, компании, использующие нелицензионное ПО рискуют столкнуться не только с техническими проблемами в работе, но и с юридическими.

Ключевые слова: технологии, лицензия, ПО, программное обеспечение, закон, риски, сложности.

Abstract

Today, law enforcement and government agencies in almost every country are increasingly paying attention to and trying to prevent violations in the use of unlicensed software by organizations. In this regard, companies using unlicensed software risk facing not only technical problems in their work, but also legal ones.

Keywords: technologies, license, software, law, risks, complications.

Программное обеспечение в том виде, в котором мы понимаем его сейчас, появилось еще в 20 веке. В наши дни невозможно представить работу какого-либо предприятия без определенного программного обеспечения. Однако, следует понимать, что программное обеспечение для пользования в коммерческих целях как правило является платным[1,2]. Безусловно, существует возможность избежать платы за пользование таким ПО, но в таком случае недобросовестный предприниматель может столкнуться с множеством рисков. Это следует четко понимать при планировании работы бизнеса.

В целом, можно выделить множество рисков, связанных с использованием нелицензионного программного обеспечения, давайте разберем самые главные из них.

1. Юридические риски

В настоящем законодательстве РФ предусмотрены наказания за использование нелицензионного ПО. Согласно действующему законодательству РФ, использование нелицензионного программного обеспечением является нарушением авторских и смежных прав и влечет за собой административную (ст. 7.12. КоАП РФ), уголовную (ст.146 УК РФ) и гражданско-правовую ответственность. Административная ответственность предусматривает наложение штрафа с конфискацией нелицензионного ПО и оборудования, используемого для их воспроизведения: для граждан в размере – от 1 500 до 2 000 рублей, для должностных лиц – от 10 тыс. руб. до 20 тыс. руб, для юридических лиц – от 30 тыс. руб, до 40 тыс. руб. Уголовная ответственность имеет место быть лишь в случаях, когда был причинен крупный ущерб автору или правообладателю ПО и влечет за собой наказания от штрафа, суммой до 200 000 рублей, до лишения свободы на срок до двух лет для физических лиц. Исходя из вышесказанного не трудно сделать вывод, что использование нелицензионного ПО может повлечь за собой значительные потери, которые, вероятно, перевесят выгоду.

2. Незащищенность ПО

Любое ПО является не только инструментом для функционирования компании и/или извлечения прибыли, но также и лазейкой для хакеров. В современной сети с

каждым днем появляется все больше вредоносного кода, который использует всяческие лазейки для проникновения в компьютеры и выполнения определенных действий, включающих дальнейшее распространение вредоносного ПО [3,4,5]. Статистика показывает, что количество уязвимостей растет год от года. Это в значительной степени связано с использованием нелегального программного обеспечения. Ведь как известно, нелегальное ПО в своем большинстве не имеет возможности получать официальные обновления от разработчиков, которые предусматривают постоянное повышение уровня безопасности ПО. Вряд ли перспектива полной или частичной остановки работы нелегального ПО, и, как следствие, резкое падение прибыли и продуктивности устроит его владельца.

3. Несовершенство ПО

При использовании нелегального программного обеспечения нужно понимать, что никто не сможет гарантировать правильность работы тех или иных компонентов этого ПО. Периодические сбои, помехи в работе ПО у владельцев нелегального ПО наблюдаются значительно чаще, чем у пользователей, купивших лицензию. Убытки от несовершенства ПО, в целом, сопоставимы с убытками от ее незащищенности, но могут быть и больше, в случаях, когда сбои в работе ПО открыто не выявляют себя, а, как вариант, выдают неверные вычисления. Подобные сбои в долгосрочной перспективе могут причинить значительный вред как единичному пользователю, так и компании в целом. Следует заметить, что пользователи нелегального ПО в отличие от владельцев лицензии не имеют возможности в полной мере получить поддержку от технической поддержки разработчиков ПО, что только усугубляет ситуацию.

Ряд исследований, проводившихся среди российских компаний, дал возможность выявить некоторые тенденции в практике использования программного обеспечения. В основном, опрашиваемыми в порядке приоритета были названы следующие преимущества использования легального программного обеспечения:

1. Отсутствие юридических рисков
2. Стабильная работа ПО
3. Наличие технической поддержки
4. Наличие постоянных обновлений ПО
5. Положительное влияние на имидж компании

Тем не менее, несмотря на вышеперечисленные проблемы, с которыми могут столкнуться пользователи нелегального ПО, количество таких пользователей по-прежнему остается на высоком уровне. В заключении попытаемся разобраться в причинах использования компаниями нелегального ПО.

Исходя из результатов проведенных исследований, цена программного обеспечения – не является основным фактором, влияющим на приобретения того или иного программного обеспечения. Здесь большую роль играет удобство использования ПО и его функциональность, во всяком случае, для руководителей крупных предприятий. Но и эта причина не всегда является основной.

Зачастую в организации отсутствует политика автоматизации и использования информационных ресурсов. Не редки случаи, когда внутри организации, представители ИТ-службы и вовсе не знают, что установлено на компьютерах у персонала. Сами же сотрудники компании сами решают, какие программы им необходимы им для работы, а какие считают лишними.

Такой подход к использованию ПО следует брать под контроль руководителей, так как потенциальные убытки могут значительно превышать преимущества от использования нелегального программного обеспечения. Т.е. на оперативном уровне политика автоматизации имеет место быть, например, в должностных инструкциях сотрудников, где следует указать на недопустимость использования нелегального программного обеспечения. В специальной документации также

следует отразить четкую последовательность процедуры поступления программного обеспечения в компанию.

При выборе лицензионного программного обеспечения отдельное внимание следует обратить на выбор поставщиков. К сожалению, в наши дни, пользователь/компания, желающие приобрести лицензионное ПО, сталкиваются с недобросовестными поставщиками программного обеспечения. Именно поэтому, в организациях также должен быть зафиксирован перечень минимальных требований по отношению к поставщикам ПО. Это в свою очередь обезопасит организацию от рисков, связанных с использованием нелицензионной продукции.

Заключая все вышесказанное, можно сделать вывод, что, приобретая ПО у правообладателя или непосредственно у его автора, компания исключает довольно большое количество рисков и получает гарантии стабильности, защищенности и качества работы программного обеспечения.

Опыт компаний, которые прежде сталкивались с последствиями использования нелицензионного ПО, дает понимание, что совокупный ущерб может значительно превышать сэкономленные средства. Таким образом, использование лицензионного программного обеспечения – в первую очередь в интересах его пользователей.

1. Гулякин Д.В. Информационная деятельность в процессе формирования социально-информационной компетентности будущего специалиста // В мире научных открытий. 2010. № 2-2 (8). С. 19-21.
2. Kharchenko L., Panova I., Babaeva E., Magomedova R., Gulyakin D., Pashtaev B. Russian syndromes, impeding the development of the innovation processes in education // Life Sci J 2014;11(9s):184-187, USA, (ISSN:1097-8135). <http://www.lifesciencesite.com>. 35.
3. Гулякин Д. В. Роль информационно-коммуникационных технологий в формировании социально-информационной компетентности // Современные информационные технологии. – 2009. – №10. – с. 121-123.
4. Гулякин Д.В. Информационная культура и ее аспекты // В сборнике: ВУЗОВСКАЯ НАУКА - СЕВЕРО-КАВКАЗСКОМУ РЕГИОНУ. Материалы XIII научно-технической конференции. Главный редактор: Синельников Б.М., 2009. С. 181.
5. Гулякин Д.В. Социально-информационная компетентность в структуре деятельности личности // Научные проблемы гуманитарных исследований. 2009. № 12. С. 36-39.

Ермолаев К.А., Гудим С.Д.

**Зависимость величины выдвиг при циркуляции от основных характеристик
сухогрузных судов**

*Новосибирский государственный университет водного транспорта
(Россия, Новосибирск)*

doi: 10.18411/lj-01-2021-06

idsp: ljjournal-01-2021-06

Аннотация

В работе приведены исследования выдвиг грузовых судов при заходе на циркуляцию при различных углах перекадки руля. Был произведен расчет с последующим выводом аппроксимации и визуализирован в виде графического анализа.

Ключевые слова: судно; циркуляция; выдвиг; перекадка руля; аппроксимация; расчет; грузовое судно.

Abstract

The paper presents a study of the advancement of dry cargo ships when entering circulation at various angles of rudder shifting. A calculation was made with the subsequent derivation of the approximation and visualized in the form of graphical analysis.

Keywords: vessel; circulation; extension; rudder shift; approximation; calculation; dry cargo ship.