электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

Анализ рисков лицензирования программного обеспечения и систем управления промышленным предприятием

 # 04, апрель 2011

авторы: Кузьминов А. С., Меняев М. Ф.

МГТУ им. Н.Э. Баумана
askuzminov@yandex.ru
2505mmf@mail.ru

Современный менеджмент активно использует преимущества виртуальных систем и технологий, что позволяет найти и эффективно использовать как новые технологии управления, так и новые источники добавления стоимости.

Инструментарий виртуальных (сетевых) технологий базируется на использовании интерактивных методов управления, которые реализуются с помощью информационных и телекоммуникационных систем. Такие технологии работают в сетевой среде с помощью программного обеспечения (ПО), серверного и телекоммуникационного оборудования (сетей).

Для реализации интерактивной технологии менеджер использует различное ПО, которое поддерживается лицензией, дающей право на его использование.

Современное законодательство многих стран охраняет программное обеспечение и его исходный код авторским правом, оставляя за авторами и правообладателем полномочия по изменению, распространению, способами использования и поведению ПО, даже если исходный код опубликован, при этом изучение или исправления кода со стороны преследуются уголовным правом.

Вид лицензирования ПО в значительной мере определяет права менеджера при организации своей работы в глобальных сетях.

Существует несколько видов лицензирования ПО: свободное, открытое, несвободное. Несвободное, в свою очередь, подразделяется на проприетарное и полусвободное.

Открытые и свободные лицензии не сохраняют права на копию ПО за издателем, в отличие от проприетарных, а передают их конечному пользователю.

В итоге менеджер получает ключевые права, которые обычно в авторском праве даются только владельцу копии, но все авторские права на ПО сохраняются за издателем.

Свободное ПО – это широкий диапазон программных продуктов, в которых права («свободы») пользователя по свободным лицензиям позволяют неограниченно устанавливать ПО, запускать его, свободно использовать, изучать, распространять, изменять и совершенствовать ПО.

Особенностью свободных лицензий в том, что они позволяют пользователю принимать или не принимать право работы с ПО, т.е. работать без лицензии. Однако, если, например, менеджеру требуется предоставление ПО через сети, то он обязан действовать в рамках лицензии.

Существует много типов свободных лицензий, в которых поддерживаются основные принципы, но несколько отличаются методы и характер защиты прав пользователя, а также различные виды продуктов интеллектуальной деятельности.

Свободное ПО легко коммерциализировать через бизнес-модели, которые исключают необходимость оплаты за ПО, например, когда предприниматель зарабатывает за счёт предоставления услуг технической поддержки.

В процессе унификации требований к работе менеджера в рамках свободного ПО было разработано представление о таком ПО, получившее обозначение GNU General Public License (Универсальная общедоступная лицензия GNU или просто GNU GPL) – лицензия на свободное ПО, созданная в рамках проекта GNU в 1988 г. GNU GPL предоставляет пользователю права копировать, изменять и распространять (в т.ч. на коммерческой основе) программы, что по умолчанию запрещено законом об авторских правах, а также гарантирует, что пользователи всех производных программ получат вышеперечисленные права. [1]

GNU GPL даёт получателям ПО права на свободу запуска программы, изучения работы ПО, модификацию и улучшения ПО при условии открытия доступа исходного кода, свободу распространения.

Применение GPL – лицензии накладывает на менеджера ряд обязанностей, одно из которых предусматривает необходимость делиться с общественностью измененными версиями программ. Даже если была переписана пара строк кода, требуется предоставить другим свободный доступ к программе и её исходному коду.

Открытое ПО (англ. open source software) – это программы, у которых открыт исходный код, доступный для изучения и изменения, и которые позволяют

использовать код для написания новых программ, корректировки ошибок. Нередко пользователи помогают дорабатывать такие открытые программы. Открытая лицензия не означает бесплатность. Учитывая последние тенденции государственной политики по национальной безопасности в сфере ИТ, использование открытого и свободного ПО в государственных и бюджетных организациях становится перспективным в России.

Большинство открытого ПО является одновременно свободным. Определения открытого и свободного ПО похожи, но не совпадают друг с другом. Многие лицензии являются сразу и открытыми, и свободными

Отличие между открытым и свободным ПО заключается в правилах использования программ и их исходных текстов. В открытом ПО делают упор на эффективность открытых исходных кодов, как способа разработки, модернизации и сопровождения программ. В свободном ПО приоритет за правами на свободное распространение, модификацию и изучение программ, как главным достоинством свободного открытого ПО.

Проприетарное, частное или собственническое ПО (англ. proprietary sofware) – ПО, являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободы ПО (речь именно о свободе, а не просто открытости ПО).

Правообладатель такого ПО владеет монополией по его использованию, копированию и модификации, как минимум в существенных моментах. Зачастую проприетарным считают любое несвободное ПО, в т.ч. полусвободное.

Не следует путать проприетарное ПО с коммерческим, которое может быть и свободным.

Основная характеристика проприетарных лицензий – издатель ПО остаётся правообладателем всех копий и в лицензии даёт разрешение использовать одну или несколько копий программы её получателю. Практически все права на ПО остаются у издателя, а пользователь имеет очень ограниченный набор строго очерченных прав. Причём конечный пользователь обязан принять лицензию, т.к. по закону владельцем ПО является не он, а издатель программы, и в случае отказа принять лицензию пользователь вообще не может работать с программой.

Компании производители проприетарного ПО обычно создают собственные лицензионные соглашения. Наиболее значимые ограничения проприетарного ПО следующие: ограничение на коммерческое использование, ограничение на распространение, ограничение на модификацию.

К полусвободному ПО относят несвободное и коммерческое ПО. Практически полусвободное ПО позволяет неограниченно использовать, распространять и изменять ПО в некоммерческих целях.

Коммерческое ПО (англ. commercial software) – ПО, созданное с целью получения прибыли от его использования другими, например, путем продажи экземпляров.

Ошибочно считают коммерческое и свободное противоположностями. Основные различия между ними невелики. Свободным ПО считается с того момента, когда автор предоставляет права на свободную модификацию, распространение и извлечение прибыли со своего продукта, поэтому свободные программы могут быть и коммерческими продуктами.

Противоположностью свободного ПО является собственническое ПО, которое также может быть как коммерческим, так и бесплатным.

Преимущества коммерческого ПО определяются значимой поддержкой крупных компаний, прямо заинтересованных в распространении своего продукта, малыми сроками модернизации программ, широким спектром выполняемых задач, возможность разработки программ «на заказ».

Большое значение в практике работы менеджера в виртуальной среде имеют вопросы легализации программного обеспечения.

Легализация ПО – это отказ от нелицензионного ПО и переход на использование ПО со всеми необходимыми лицензиями, разрешениями и правами, например покупка необходимых программ и лицензий, переход на использование бесплатного или условно-бесплатного ПО, демо-версий, самостоятельная или сторонняя разработка ПО.

В ряде случаев целесообразно заменять нелицензированное ПО на аналогичное ПО с недорогими или бесплатными лицензиями, аренда ПО, использование свободное ПО или ПО, приобретённое на льготных условиях, приобретение отдельных лицензий, легализующего нелицензионное ПО и т.д.

В странах СНГ, Восточной Европы, БРИК, Азии и других по разным причинам широко распространено массовое использование ПО без его приобретения.

В то же время не существует стран, где 100% ПО используется легально. Даже в благополучных странах, 20% программ используется незаконно, в ЕС около 33%. В странах БРИК на одну лицензионную программу приходится две нелицензионные. В среднем во всем мире количество программ, использующихся нелегальным способом, продолжает расти и составило в 2008 г. 41% – то есть почти половина программ во

всем мире нелицензионные. Проблема легализации ПО важна и актуальна во всех странах мира. [2]

В РФ в 2008 году 68% ПО, установленное на персональные компьютеры, было нелицензионным, а потери разработчиков ПО, превысили 4 млрд. долл. США. В последнее время в России существует тенденция к снижению уровня нелегального ПО. [3]

Практически важно не просто использования лицензионного ПО, а наличие у организации необходимых документов, подтверждающих законность приобретения и использования ПО.

До недавнего времени легализация ПО не было самостоятельной формой распространения ПО. После того, как некоторые производители, предложили услуги легализации ПО для лицензирования нелегальной программы без её переустановки, ситуация стала улучшаться.

Процесс легализации как услуги в современном мире сформировал специфический вид услуг. Компания, желающая легализовать ПО, обращается к ИТ-консультантам. В процессе легализации выполняют комплексную процедуру, позволяющую перейти к полноценному применению в компании методологии управления лицензиями на ПО как активами SAM (Software Asset Management).

Для поддержки процесса легализации используют специализированное ПО, позволяющее автоматизировать процессы проведения инвентаризации лицензий и программного обеспечения, установленного на компьютерах менеджеров компании.

В Российской Федерации защита авторских прав на программы для ЭВМ обеспечивается статьями 146, 183, 272 и 273 Уголовного кодекса РФ. Ответственность за использование нелегального ПО рассмотрена в таблице: [4]

Стоимость незаконно установленного ПО	Ответственность за использование нелегального ПО по ст. 146 УК РФ
до 50 тыс. руб.	Штраф: - Физ. лицо 1,5 тыс. руб. - Должностное лицо от 10 до 20 тыс. руб. - Юр. лицо от 30 до 40 тыс. руб.
50-250 тыс. руб.	Лишение свободы: до 2 лет Обязательные работы: от 180 до 240 часов Штраф: до 200 тыс. руб. или в объёме оплаты труда или иного дохода осуждённого за период до 18 месяцев
свыше 250 тыс. руб.	Лишение свободы: до 6 лет Штраф: до 500 тыс. руб. или в объёме оплаты труда или иного дохода осуждённого за период до 3 лет

Помимо штрафов, организация обязана в качестве компенсации ущерба уплатить стоимость всех обнаруженных нелицензионных программ.

По закону сотрудники милиции, в т.ч. ОБЭПа могут изъять подозрительную технику для экспертизы даже без постановления суда. Для проведения проверок привлекают понятых и экспертов. Эксперты на месте могут оценить необходимость изъятия техники, в случае сотрудничества организации и предоставления полного доступа к технике. Если сотрудничество не обеспечивается, сотрудники ОБЭП описывают технику, оформляют протокол и забирают её для экспертизы. Благодаря «стараниям» конкурентов организации, технику могут изъять до 30 дней для «оперативно-розыскных мероприятий».

Работники ОБЭП осматривают всю технику на территории предприятия в не зависимости от того личный это компьютер или нет и при любых подозрениях описывают и изымают её. Если на компьютере обнаруживают нелицензированный софт и этот компьютер не находится на балансе предприятия, то ответственность несёт владелец компьютера, при условии если компьютер не связан с деятельностью предприятия, иначе ответственность будет нести предприятие и его руководство, что добавит проблем в зависимости от количества найденного нелицензионного ПО в компьютере. Поэтому на многих предприятиях используется жёсткая корпоративная политика, запрещающая использование личной аппаратуры, установку ПО пользователями и декларирующая определённый фиксированный набор разрешённого ПО.

Небольшие предприятия представляют особый интерес для проверки, т.к. такие организации хуже контролируют используемое ПО, не имеют собственных юридических отделов и покровительства в разных органах власти. Ведь даже у предприятий с качественным контролем используемого ПО, могут обнаружить нелицензированные программы. Для предприятия это грозит штрафом до 40 тыс. руб. и уплатой полной стоимости нелицензионного ПО, найденного в ходе проверки. Помимо прямых расходов на штрафы и возмещение ущерба, следует учесть потери, которые возникнут из-за простоя, что критично для ряда служб, например бухгалтерии, т.к. технику могут изъять на срок 30 и более дней.

Бывают случаи, превышения должностных полномочий сотрудников ОБЭП, которые после проверки и изъятия удерживают технику как можно дольше, вынуждая таким образом руководство или владельцев организации учитывать личные интересы проверяющих. Как показывает современная практика, ОБЭП проводит проверки даже в

организациях, существующие менее 3 лет, и на которые нет заявлений, и отсутствуют какие-либо правонарушения.

Даже если предположить, что есть «свой человек» в проверяющей структуре, следует оценить насколько оправдано постоянно платить существенные суммы за покровительство, не имея при этом никаких гарантий, т.к. этот же сотрудник первым сдаст организацию ради повышения.

Одна копия ПО часто позволяет использовать её только на одном компьютере, и установка её на множество машин будет считаться нелицензионным использованием копии ПО. Все эти нелицензионные копий будут посчитаны при учёте штрафа и их стоимость будет добавлена к сумме ущерба.

Даже несмотря на наличие только бесплатного открытого ПО, к приходу проверяющих необходимо подготавливаться. В соответствии с законодательством проверяются не столько лицензии, сколько документы на приобретение ПО, которых может и не быть в случае бесплатной программы.

В качестве выхода из такой ситуации многие компании предлагают за символическую сумму приобрести «лицензионный сертификат», в результате чего у организации появляется товарная накладная с наименованием и проверяющим органам этого достаточно.

Альтернативным решением может стать использование такого ПО как результат тестовой эксплуатации, опытного производства или научно исследовательских разработок, в случае, если лицензия на ПО позволяет модификация исходного кода. Более того, тестовая эксплуатация позволит вывести часть прибыли в НИОКР и уменьшить налогооблагаемую базу.

Доказать сотруднику проверяющих органов без соответствующей квалификации, что ПО бесплатное затруднительно, т.к. у него чёткие инструкции: каждый компьютер, должен быть снабжён документами на ПО, а если они отсутствуют, то следует описать компьютер и отправить на экспертизу.

Так же рекомендуется распечатать официальный текст GPL и других лицензий на русском языке, используемых в ПО организации. Этот текст подписывает директор и заверяется печатью.

Лицензионные наклейки или упаковка ПО говорит от правомерном использовании, но они не определяют, кому принадлежат данные права использования. Организация ещё должна иметь документы на покупку программного обеспечения, чтобы считаться лицензиатом, т.е. лицом получившее право использования ПО.

При обнаружении нарушения отвечать будет не только программист, администратор, менеджер по техническим вопросам, но и обязательно организация. Если сумма причинённого ущерба меньше 50 тыс. руб., то организация будет оштрафована до 40 тыс. руб. Иногда руководство организации договаривается с сотрудниками, чтобы они подписали документ, указывающий, что всё ПО на компьютере установлено с их ведома лично, что позволит снизить сумму штрафа до 10 – 20 тыс. руб., но организация всё равно будет нести ответственность, т.к. компьютер на рабочем месте, находящийся в собственности организации, используется в производственном процессе. Следствие и суд зачастую не учитывают такие «документы», считая их фиктивными. В любой ситуации организация должна уплатить штраф вместе с суммой ущерба. При обнаружении ущерба в крупных размерах по ст. 146 УК РФ и другим статьям ответственность будут нести одно или несколько должностных лиц, в зависимости от степени вины по заключению экспертов. Уголовная ответственность распределяется между всеми должностными лицами, которые ответственны за приобретение, установку и использование ПО.

Пытаясь обмануть следователей, организации ограничивают доступ к системе, например, установив пароль. Но все эти меры легко и быстро устраняются при наличии непосредственного доступа к системе. Использование программ на внешних носителях, может сократить риски обнаружения, однако в системе остаётся множество следов и записей от деятельности программ, поэтому у проверяющих будет повод для изъятия.

Так же не поможет удаление программ до или в момент проведения проверки, т.к. особенности жёстких дисков позволяют восстановить данные даже после нескольких перезаписей. Однако если программы были удалены, то, как показывает следственная практика, обвинения не предъявляются.

Многие предприятия используют технологии шифрования, чтобы предотвратить утечки коммерческих и не коммерческих тайн, в т.ч. и об используемом ПО. Но данные инструменты могут снизить производительность и повысить риск утраты информации. Качественное шифрование предполагает наличие специалистов и организационной схемы, которая будет учитывать, что сотрудники под давлением следствия могут выдать пароль и стать свидетелями, что создаст дополнительную ответственность за использование криптографии в преступных целях.

И не смотря на обилие проблем, компании пытаются использовать нелицензионное ПО, ошибочно или умышленно, с подачи правообладателей, называемого «пиратским» (пиратство – это грабёж кораблей в море). И главная

причина в этом – попытка сэкономить бюджет предприятия, помимо не очевидных факторов: невозможность приобретения нужного ПО, отсутствие ответственности со стороны разработчика за свой программный продукт, низкое качество ПО и поддержки региональных дилеров, идеологические соображения и т.д.

Но помимо проблем с законом, существует множество мифов о том, что нелицензионное ПО содержит вирусы, отправляет конфиденциальную информацию в сеть, работает гораздо медленнее, не стабильнее, сложно обновлять и т.д.

На практике лицензионный софт от нелицензионного отличается исключительно наличием документов, позволяющих законно использовать его. С технической точки зрения используются одинаковые дистрибутивы.

Нередко когда нелицензионные сборки ПО выложенные в сеть «для ознакомления» превосходят в стабильности и доработанности версии от производителей этого ПО, особенно если производитель прекратил поддержку. Другое дело, что основной риск идёт от специализированных программ, таких как изменённые файлы программ, генераторы ключей, патчеры, которые во многих случаев определяются как вредоносное ПО, т.к. используют сходные с вирусами принципы работы. Они изменяют оригинальный код программы, что бы отключить проверку на наличие лицензии и тем самым позволяют использовать ПО бесплатно. Многие антивирусы определяют такие программы взломщики, по договорённости с крупными производителями ПО.

Но так как в случае нелицензионного ПО, никто ответственности не несёт, то есть риск получить не рабочую программу или вредоносную. Здесь поможет только квалификация человека, занимающегося администрированием компьютеров.

Что же касается официальной поддержки, то зачастую это информация, находящаяся в свободном доступе в Интернете или документации. Хотя в ряде случаев именно качественная поддержка от производителя может стать причиной выбора ПО.

Подводя итоги, можно сказать, что выбор между легализацией и контрафакцией представляет собой весы, где на одной чаше затраченные средства, юридическая чистота и стабильность, а на другой экономия средств на начальном этапе, штрафы и компенсации, а так же административная и уголовная ответственность.

Для выбора нужной «чаши», необходимо представить эти обе ситуации:

$$k = \frac{(S + P + C + D + L + V) \times x + N}{S + M},$$

где: k – коэффициент эффективности легализации,

S – стоимость ПО;

P – штраф;

C – судебные издержки;

D – упущенная выгода из-за изъятия оборудования;

L – потеря средств вложенных в сотрудника, попавшего по уголовную ответственность;

V – риски в связи со сбоями ПО из-за некорректного взлома и как следствие утраты данных;

N – «покровительство» местных органов проверки;

M – платная поддержка производителя (опционально);

x – вероятность проверки ($0 \le x \le 1$), на практике $x \to 1$ для юридических лиц.

При $k > 1$ экономически целесообразно использовать легальное ПО. При $k < 1$ экономически не целесообразно использовать легальное ПО. При $k = 1$ экономической разницы нет, но для юридической чистоты следует отдать предпочтение легальному ПО.

Здесь не рассматриваются такие моменты, как затраты на установку, содержание, налоги и т.д., т.к. эти затраты будут в любом случае и их можно внести в стоимость ПО S.

Не смотря на то, что нелицензионное ПО подкупает, в первую очередь, именно экономией средств, необходимо учитывать все юридические и финансовые риски и затраты, которые может повлечь данный путь, учитывать что вероятность проверок k для организация всегда стремится к 1, что практически всегда приводит к гораздо большим потерям, чем если бы все ПО было лицензионным. А значит, если предприятие хочет стабильности, перспектив развития и экономию средств в долгосрочном периоде, то единственный правильный выбор – это соблюдение законов и использование только легального ПО.

Литература:

1. GNU, http://www.gnu.org/licenses/
2. BSA, http://www.bsa.org/country/News%20and%20Events/News%20Archives/global/05122009-idc-globalstudy.aspx
3. BSA, http://portal.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf
4. Статья (ст.) 127 УК РФ «Незаконное лишение свободы»