УДК 34.096

ПРОБЛЕМЫ И ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ПРАВАМИ НА ПРОГРАММЫ ДЛЯ ЭВМ В КОРПОРАТИВНОМ СЕКТОРЕ

Петрова А.А. (Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»),

Научный руководитель – к.и.н. Тарасов А.С.

(Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный морской технический университет»)

Аннотация: В работе представлен анализ основных рисков в международных и отечественных подходах к управлению программой для ЭВМ как нематериальным активом компании. По итогам исследования был сформулирован алгоритм защиты технологии с момента формирования технического задания до достижения уровня широкого внедрения кода в качестве составляющего продукта.

Введение. Эксперты в области корпоративного управления интеллектуальной собственностью отмечают, что программы для ЭВМ могут быть основным нематериальным активом компании в совокупности с базой данных и иными компонентами «продукта». Тем не менее, на сегодняшний день имеются существенные риски по его утрате или обесцениванию по техническим причинам, либо вследствие ненадлежащего управления на каком-либо этапе жизненного цикла.

Актуальность проблемы обусловлена также повышением востребованности российского программного обеспечения. Об этом свидетельствует утверждение Правительством Российской Федерации плана мероприятий «Создание дополнительных условий для развития отрасли информационных технологий» на 2021-2022 год. Анализ статистики IPO, согласно которому за 2021 год к стадии IPO подошли такие компании, имеющие российское происхождение, как ClickHouse, Revolut, Arrival и иные. Все они специализируются на разработке ПО, системам управления базами данных или используют в основе принципа работы программный код.

Основная часть. Проведенное исследование позволяет выделить следующие ключевые риск-ориентированные направления управления программой ЭВМ как нематериальным активом компании в РФ:

1. Правовое направление. Действующее законодательство предусматривает достаточное количество правил и требований, своевременное несоблюдение или игнорирование которых влечет значительный ущерб для компании. К таковым можно отнести:

Во-первых, риски по организации управления внутри компании (оценка возможности регистрации, в том числе в качестве иного объекта интеллектуальной собственности, учет, уплата пошлин и вознаграждений сотрудникам, распределение прав между авторами и фактическими правообладателями, в том числе с учетом внедрения искусственного интеллекта в качестве создателя кода).

Во-вторых, существуют риски, возникающие при реализации программы для ЭВМ в качестве составного компонента продукта для контрагентов и третьих лиц. В данном случае, большое внимание уделяется составлению документации, в которой отражаются допустимые пределы использования программы, цели, иные существенные условия, подлежащие включению в зависимости от квалификации договора.

В-третьих, имеют место риски, возникающие при осуществлении модификации, проведении работ по улучшению программы, в том числе с использованием внешних источников (открытого кода). Это выражается в том, что действующее законодательство допускает различные варианты «open source» лицензий: разрешительные, копилефтные. От

варианта использованной лицензии зависит дальнейшая судьба программы. В частности, в случае использования копилефтной лицензии возникает корреспондирующая обязанность по распространению ПО на условиях open source лицензии, в то время как при разрешительной лицензии – производные ПО могут быть проприетарным.

2. Техническое направление. В данном случае речь идет о рисках, которые могут возникнут вследствие отсутствия надлежащей технической защиты кода. К таковым могут относится неправомерные действия с кодом: модификация, адаптация, переработка, компилирование, совершение иных запрещенных действий, связанных с кодом, в том числе реверс-инженеринг. Как показывает судебная практика, наиболее часто это встречается в случаях, когда сами сотрудники компании будучи авторами программы для ЭВМ «забирают» ее с собой и воспроизводят для других компаний.

В целях повышения эффективности управления программами для ЭВМ и снижения рисков на различных этапах зрелости технологии предлагается алгоритм действий по его защите.

1. Первый этап – постановка цели, определение задач, подготовка технического задания.
2. Второй этап – определение автора и последующего правообладателя программы.
3. Третий этап – разработка правовой документации по оформлению отношений между правообладателем, автором, разработчиком, выбор формы договора (авторского заказа, подряда или иного), определение существенных условий договора.
4. Четвертый этап – разработка кода с учетом применения технических мер для его защиты от третьих лиц (например, обфускация (шифрование), установление датчиков и исполнительных механизмов в защищенном исполнении). В случае использования открытого кода следует осуществить следующие действия:

- составить перечень компонентов программы для ЭВМ;
- определить лицензии, применимые к каждому компоненту;
- проверить совместимость лицензий;
- удостовериться в соблюдении условий лицензии, в соответствии перечню одобренных лицензий;
- проверить приобретаемый код.

5. Пятый этап – регистрация программы, постановка программы для ЭВМ на бухгалтерский баланс в качестве нематериального актива.
6. Шестой этап – разработкой внутренних регламентов компании по защите кода.
7. Седьмой этап – разработка документов для работы с контрагентами, в частности лицензионных договоров.
8. Восьмой этап – ведение бизнес-процессов по управлению программой, в частности: осуществление учета, формирование реестра лиц, имеющих доступ к коду, заключение с ними соглашений о неразглашении конфиденциальной информации, учет данных документов; формирование реестра лицензионных договоров, договоров о переходе прав и иных документов, имеющих юридическое значение.

Выводы: по итогам проведенного исследования были выявлены проблемы и риски в управлении программами как нематериальными активами компании, был разработан алгоритм, применение которого будет способствовать обеспечению безопасности компании в указанном управлении деятельности.

Петрова А.А. (автор)

Тарасов А.С. (научный руководитель)