УДК 65.012.8
DOI 10.22213/2413-1172-2018-1-68-70

И. В. Пронина, кандидат экономических наук, доцент, Глазовский инженерно-экономический институт (филиал) ИжГТУ имени М. Т. Калашникова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИННОВАЦИОННОЙ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Одним из ключевых условий выхода экономики из кризиса является развитие инновационной сферы. Создание и внедрение принципиально новых технологий и продуктов способствует повышению экономического потенциала и конкурентоспособности российских товаропроизводителей, расширению рынков сбыта отечественных товаров. С учетом фактора глобализации можно сказать, что для российских предприятий важно стать активными игроками на мировом рынке инноваций.

Рынок инноваций – очень специфическая и мало изученная зона с высоким уровнем риска. Объектами купли-продажи на нем могут быть не только материальные товары или услуги (инновационные продукты), но и идеи. Не умаляя сложности продвижения инновационных продуктов, отметим угрозы, связанные с распространением инновационных идей.

Инновационная идея может быть зафиксирована и оформлена, например, в виде патента. Тогда акт ее купли-продажи мало чем отличается от обычной рыночной операции. Но если идея не зафиксирована, а сразу предназначена для внедрения в производство, т. е. существует в виде информации, она становится особым товаром. Спрос на него формируют не столько конечные потребители, сколько другие игроки на рынке, конкуренты, для которых инновация – средство увеличения прибыли или даже выживания. Конкуренция формирует спрос на инновации [1].

Другими словами, спрос на инновационные идеи и проекты возникает среди производителей, ведущих конкурентную борьбу на рынке. К сожалению, средства ведения конкурентной борьбы не всегда добросовестные. В связи с этим в инновационной деятельности возникает проблема обеспечения информационной безопасности.

Информационное поле инновационного проекта можно разделить на три зоны: технические данные, оперативные, коммерческие.

Техническая информация позволяет узнать все о продукте проекта и процессе его создания: какие материалы, комплектующие нужны для изготовления продукта, машины и оборудование, технологии и инструментарий, используемые в рабочем процессе.

Оперативные данные регламентируют работу персонала, регулируют производственный процесс на предприятии, позволяют контролировать ход и сроки выполнения работ по проекту, дают возможность координировать все процессы в рамках проекта и минимизировать затраты ресурсов.

К коммерческим данным относятся сведения о расходах на разработку и реализацию проекта, планах инвестиций, контрагентах, с которыми заключаются сделки по проекту, ценах, по которым продукт проекта будет предоставляться заказчику [2].

Любая из названных зон информационного поля проекта может иметь предпринимательскую ценность. Разглашение относящихся к ней сведений может нанести ущерб и усилить проектные риски.

Основными угрозами информационной среде инновационной деятельности можно считать:

– утечку информации (например, извлечение, копирование, подслушивание);

– нарушение целостности (например, подделка, уничтожение);

– блокирование (например, невозможность доступа) [3].

На крупных предприятиях для выявления, устранения и предупреждения вышеперечисленных угроз создаются специальные подразделения – службы информационной безопасности. В функции службы входит выявление возможных каналов утечки и способов нарушения целостности информации, формирование модели угроз, разработка политики безопасности информации, определение мероприятий, направленных на ее реализацию.

Для эффективной работы такие подразделения должны быть укомплектованы штатом ква-

лифицированных специалистов и обеспечены современными техническими средствами, что требует соответствующего финансирования. Далеко не каждое предприятие может себе позволить дополнительные расходы.

Альтернативой может стать составление перечня минимально необходимых функций по обеспечению информационной безопасности по каждому инновационному проекту и возложение ответственности за их исполнение на руководителя проекта.

Нам представляется, что необходимый минимум по защите информации инновационного проекта должен включать следующие моменты.

I. Идентификация угроз, а именно:

1. Определение перечня сведений, относящихся к разработке и реализации инновационного проекта, составляющих коммерческую тайну.

Для этого информацию по проекту следует разделить:

– на открытую для использования;

– ограниченную, доступную определенному кругу доверенных лиц и органам, чьи права прописаны в законе (например, следователи, прокуроры, налоговые инспекторы);

– конфиденциальную, доступную только разработчикам проекта и руководящему составу.

Ограниченная и конфиденциальная информация представляет сведения, составляющие коммерческую тайну.

2. Определение участков сосредоточения сведений, составляющих коммерческую тайну, на каждом этапе разработки и внедрения инновационного проекта.

3. Определение круга лиц, имеющих доступ к сведениям, составляющим коммерческую тайну.

4. Определение уровня информационных рисков, т. е. вероятности порчи, потери или утечки проектной информации и связанный с этим ущерб.

Адекватная оценка уровня риска позволит правильно определить его значимость и расставить приоритеты в принятии мер по защите информации.

II. Меры по защите информации, например:

– разработка организационного регламента – положения о коммерческой тайне и конфиденциальной информации. В организации, занимающейся инновационной деятельностью, в положении должны быть прописаны в том числе и меры по защите проектной информации [4];

– документирование перечня сведений, составляющих коммерческую тайну. Наличие организационного регламента и утвержденного перечня сведений, составляющих коммерческую тайну, позволит в случае нанесения ущерба отстоять свои интересы в суде;

– включение мер по обеспечению информационной безопасности в график разработки и внедрения проекта;

– ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка работы с этой информацией и контроля над соблюдением такого порядка;

– учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

– нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации [5].

Как показывает практика, угроза информационной безопасности существенно повышается, если к разработке и реализации проекта привлекаются сторонние организации или специалисты. В этих случаях предпринимаются дополнительные меры защиты информации.

Например,

– при заключении договоров на проведение проектных, изыскательских и научно-исследовательских работ оговаривается недопустимость передачи сведений третьим лицам без согласия заказчика и обязанность обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов;

– при проведении экспертизы проектной документации законодательно установлены ограничения на проведение общественной экспертизы в отношении объектов, представляющих коммерческую тайну;

– при привлечении сторонних специалистов к выполнению работ по проекту с ними заключается соглашение о неразглашении коммерческой тайны.

Ответственность руководителей и специалистов, участвующих в проектной деятельности, соблюдение требований российского законодательства позволят предотвратить нанесение экономического ущерба, вызванного неправомерными или неквалифицированными действиями.

Своевременная постановка и решение задачи обеспечения информационной безопасности в инновационной проектной деятельности позволит принять превентивные меры по устране-

нию возможных угроз и потенциальных потерь и, как следствие, повышению инновационной активности предприятия.

Библиографические ссылки

1. *Светунков С.* Рынок инноваций. URL: http://sergey.svetunkov.ru/economics/innovation/inn6.phtml (дата обращения: 16.01.2018).

2. Рекомендации по охране конфиденциальности информации, составляющей коммерческую тайну в проектной организации. URL: http://files.stroyinf.ru/Data2/1/4293848/4293848225.htm (дата обращения: 02.02.2018).

3. *Герасимов П. А.* Проблемы экономической безопасности инновационной деятельности // Безопасность бизнеса. 2009. № 1. URL: http://www.center-bereg.ru/m2411.html (дата обращения: 02.02.2018).

4. О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014).

5. *Анашенко И. К.* Режим коммерческой тайны в организации // Молодой ученый. 2016. № 28. С. 617–619. URL: https://moluch.ru/archive/132/36323/ (дата обращения: 02.02.2018).

Получено 08.02.2018

References

1. Svetunkov S. (2018). *Rynok innovatsii* [The market of innovations], available at http://sergey.svetunkov.ru/economics/innovation/inn6.phtml (accessed January 16, 2018) (in Russ.).

2. *Rekomendatsii po okhrane konfidentsial'nosti informatsii, sostavlyayushhej kommercheskuyu tajnu v proektnoj organizatsii* [Recommendations for the protection of confidentiality of information constituting a commercial secret in the project organization], available at http://files.stroyinf.ru/Data2/1/4293848/4293848225.htm (accessed February 2, 2018) (in Russ.).

3. *GerasimovP. A.* (2009). *Bezopasnost' biznesa* [Business security], no. 1, available at http://www.center-bereg.ru/m2411.html (accessed February 2, 2018) (in Russ.).

4. *O kommercheskoj tajne: Federal'ny jzakon ot 29.07.2004 № 98-FZ* [On commercial secret: Federal law of 29.07.2004 no. 98-FZ] (in Russ.).

5. Anashenko I. K. (2016). *Molodoj uchenyj* [The Young scientist], no. 2, pp. 617-619, available at https://moluch.ru/archive/132/36323/ (accessed February 2, 2018) (in Russ.).