Безопасность интеллектуальной собственности компании
Третьякова Ю. Д.

Третьякова Юлия Дмитриевна / Tretiyakova Yulia Dmitrievna – студент,
кафедра анализа рисков и экономической безопасности,
Финансовый университет при Правительстве Российской Федерации, г. Москва

Аннотация: *в статье анализируются проблемы безопасности интеллектуальной собственности в компаниях и рассматриваются меры осуществления безопасности интеллектуальной собственности, с учётом зарубежного опыта.*

Ключевые слова: *экономическая безопасность, интеллектуальная собственность, нематериальные активы, коммерческая тайна, конфиденциальная информация.*

Информация обладает первостепенным значением в современном обществе. Собственные технологии и ноу-хау - важное конкурентное преимущество на рынке для каждого предприятия в отдельности и для России в целом. Во времена кризисов конкуренция особенно часто приобретает незаконный характер. К ней можно отнести использование информации, составляющей чужую коммерческую тайну.

Особо остро стоит вопрос об обеспечении безопасности коммерческой тайны, а также конфиденциальной информации на предприятиях.

Коммерческая тайна - это любая информация, которая имеет действительную или же потенциальную коммерческую ценность в силу того, что она неизвестна третьим лицам, также к данной информации нет доступа на законном основании и обладатель данной информации, который принимает меры по защите её конфиденциальности [2].

Большинство предприятий не отличается существованием единой политики в области защиты интеллектуальной собственности и продвижении собственных интеллектуальных ресурсов на рынок.

Перед каждым руководителем должна стоять цель – создание комплексной системы обеспечения безопасности предприятия.

Согласно статистике Компания Zecurion 70% работников выносят информацию, составляющую коммерческую тайну, за пределы офисов. 30% признались, что умышленно крадут информацию для дополнительного заработка, надеясь предложить сведения конкурентам, оставить для самостоятельных разработок или унести в другую компанию, сменив место работы. Однако 37% инцидентов с потерей конфиденциальных данных происходит исключительно по вине либо недостаточно подготовленного персонала, либо попросту игнорирования элементарных правила безопасности. Из-за низкой мотивации сотрудники умышленно скрывают ценную для компании информацию и не видят смысла в разработке новых идей [1].

Сотрудники предприятия должны предупреждаться о том, что на предприятии существует режим коммерческой тайны. Обязательно должны быть разработаны приказы об организации рабочего процесса в соответствии с защитой коммерческой тайны, о компьютерной безопасности, также обязательство по неразглашению коммерческой тайны и конфиденциальной информации, перечень сведений, которые относятся к коммерческой тайне организации и инструкции по работе с документами и другими видами носителей информации, которая составляет коммерческую тайну предприятия. Затем данные документы необходимо утвердить и довести до всех сотрудников предприятия, желательно под роспись.

В целях защиты интеллектуальной собственности нужно применять организационно-профилактические и режимные меры, которые заключаются в создании перечня коммерческой тайны и конфиденциальной информации, организации системы разграничения для сотрудников доступа к информации, включённой в перечень, в контроле над доступом, хранением и передачей носителей информации, которая относится к перечню с коммерческой тайной или же конфиденциальной информацией.

На собраниях и при приёме на работу разъясняются требования юридических документов и ответственность, которая может наступить при их нарушении.

Ответственность, наступающую впоследствии разглашения коммерческой тайны, стоит прописывать отдельно в трудовом договоре, в целях профилактической и юридической защиты.

Руководством предприятия или работниками всем режимных мер необходимо вести постоянный гласный, а также негласный контроль.

На больших предприятиях рекомендуется отдельно назначать в каждое подразделение предприятия лиц, которые будут ответственны за соблюдение режима охраны коммерческой тайны в организации. В бюджет организации может быть включена расходная статья на проведение дополнительного обучения этих людей, помимо зарплаты должна быть денежное вознаграждение.

В момент увольнения сотрудника из организации ему предлагают написание расписки о

неразглашении сведений, которые составляют коммерческую тайну.

В расписке должно быть указано, что бывший работник обязуется в будущем не разглашать коммерческую тайну предприятия в соответствии с действующим законодательством и не проводить в отношении указанной организации нелегальной подрывной деятельности в будущем.

Профилактическая беседа проводится специальными сотрудниками с бывшим работником на предмет неразглашения им конфиденциальной информации на ближайшие 5 лет. Продуманная и слаженная система увольнения сотрудников позволяет весомо сократить риск разглашения секретной информации.

Специалисты информационной безопасности считают, что даже самые современные системы безопасности не могут гарантировать 100%-й защиты конфиденциальной информации, но их использование предприятиями способно уменьшить риски утечки информации. Такие системы безопасности, как DLP (Data Loss Prevention), что в переводе означает контроль утечки информации, мониторят и блокируют попытки выноса сотрудниками конфиденциальной информации за пределы предприятия почти по всем каналам. К таким каналам относится запись на флешки, печать на принтере, отправка по электронной почте и многие другие. Удобство данных систем заключается в том, что информация, которая не относится к перечню конфиденциальной информации и коммерческой тайны, может свободно передаваться сотрудниками по всем доступным электронным каналам. Уже на данный момент 40% компаний в России внедрили или находятся на стадии внедрения системы DLP, после учащения серьёзных инцидентов с утечкой информации.

Не секрет, что главный мотиватор для сотрудников – материальные блага, но существуют и другие решения.

В некоторых случаях сотрудникам даётся 15% от рабочего времени на деятельность по своему усмотрению, ориентированную на разработку новшеств, которые впоследствии могут быть отнесены к перечню с коммерческой тайной. Цель также может быть поставлена руководителем, но каким образом ее достичь работники решат сами.

Может предоставляться такая возможность, при которой сотрудники будут сами разрабатывать персональные проекты. При условии, что сотрудники для начала будут согласовывать порядок реализации проекта и ключевые его части с руководством. Может применяться и более формализованная система. Например, фиксированный процент от бюджета НИОКР организация будет выделять на проекты с высокой степенью риска, при этом любому исследователю возможно воспользоваться данным процентом бюджета.

Ежегодно в мире количество утечек информации на предприятиях возрастает в 1,5 раза. В 2016 году по исследованиям Symantec можно ожидать ещё более значительный скачок, особенно увеличатся кражи в банковской сфере, так как такая информация позволит злоумышленникам быстро монетизировать полученные сведения. Вопросы обеспечения безопасности коммерческой тайны, как важнейшей составляющей интеллектуальной собственности, влияют на уровень экономической безопасности предприятия и требуют комплексной и системной разработки.

Литература

1. Официальный сайт Zecurion. [Электронный ресурс]. Режим доступа. URL: http://www.zecurion.ru (дата обращения: 12.05.2016).
2. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне"