УДК 331.1:338

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

[1]Кайгородцев А.А., [2]Кайгородцева Т.Ф.

[1]Восточно-Казахстанский государственный университет им. С. Аманжолова, Усть-Каменогорск, e-mail: kay-alex@mail.ru;

[2]Ярославский колледж индустрии питания, Ярославль, e-mail: tanya19651@mail.ru

В статье рассматривается актуальная проблема обеспечения сохранности коммерческой тайны, которая в условиях рыночной экономики является активом, позволяющим ее обладателю получать конкурентные преимущества и извлекать экономическую выгоду. Раскрыта сущность коммерческой тайны. Проведено подразделение информации на относящуюся и не относящуюся к коммерческой тайне. Выявлены основные угрозы, реализация которых может привести к утрате организацией коммерческой тайны. Определены законные и незаконные, тайные и открытые способы получения третьими лицами информации, составляющей коммерческую тайну. Дано авторское определение механизма обеспечения сохранности коммерческой тайны. Рассмотрен комплекс мероприятий по обеспечению сохранности коммерческой тайны. Показана возможность использования при проведении мониторинга соблюдения режима сохранности коммерческой тайны современных компьютерных систем. Предложена система показателей эффективности работы по обеспечению сохранности коммерческой тайны: попытки несанкционированного доступа к локальной сети организации со стороны конкурентов, криминальных структур или сотрудников организации; утечка информации на электронных и бумажных носителях; контакты сотрудников организации с представителями конкурентов или криминальных структур; разглашение, несанкционированное уничтожение или изменение информации; блокирование или разрушение технических средств, используемых для работы с информацией; неисправность приборов видеонаблюдения и мониторинга информационных ресурсов.

Ключевые слова: коммерческая тайна, механизм обеспечения коммерческой тайны, режимные мероприятия, система показателей, мониторинг

THE MECHANISM OF PRESERVATION OF TRADE SECRET

[1]Kaygorodtsev A.A., [2]Kaygorodtseva T.F.

[1]S. Amanzholov East Kazakhstan State University, Ust-Kamenogorsk, e-mail: kay-alex@mail.ru;

[2]Yaroslavl College of Food Industry, Yaroslavl, e-mail: tanya19651@mail.ru

The article deals with the actual problem of ensuring the safety of commercial secrets, which in a market economy is an asset that allows its owner to obtain competitive advantages and extract economic benefits. The essence of a trade secret is revealed. The division of information into related and non-related trade secrets was carried out. The main threats, the implementation of which may lead to the loss of commercial secrets by the organization, are identified. Legal and illegal, secret and open ways for third parties to obtain information constituting a trade secret are defined. The author's definition of the mechanism for ensuring the safety of trade secrets is given. A set of measures to ensure the safety of trade secrets is considered. The possibility of using modern computer systems for monitoring compliance with the commercial secret protection regime is shown. The proposed system of performance indicators to ensure the preservation of trade secrets: unauthorized access to local network by competitors, criminal organizations or employees of the organization; information leakage in electronic and paper form; contacts of employees of the organization with representatives of competitors or criminal structures; the disclosure, destruction or unauthorised changes to information; the blocking or destruction of the technical means of reception, transmission, processing and storage of information; failure of video surveillance devices and monitoring of information resources.

Keywords: trade secret, mechanism for ensuring trade secret, security measures, indicator system, monitoring

В условиях рыночной экономики соблюдение режима сохранности информации, составляющей коммерческую тайну, позволяет ее владельцу увеличивать свои доходы, избегать дополнительных расходов, обеспечивать конкурентоспособность или получать иную выгоду. И наоборот, разглашение коммерческой тайны может привести к существенному уменьшению рентабельности производства и увеличению доходов конкурирующих фирм. Это свидетельствует об актуальности темы настоящей статьи.

Целью статьи является исследование механизма обеспечения сохранности коммерческой тайны.

Материалы и методы исследования

Теоретической и методологической основой исследования послужили произведения российских ученых, специализирующихся в области охраны коммерческой тайны, а также законодательные и нормативно-правовые акты, регулирующие предпринимательскую деятельность в Российской Федерации. Исследование проводилось на основе системного подхода с использованием абстрактно-логического метода.

Результаты исследования и их обсуждение

Необходимо различать понятия «коммерческая информация» и «коммерческая

тайна». Коммерческая информация – это сведения финансового и делового характера, а коммерческая тайна – это специально установленный правовой режим, при правильном применении которого государство обеспечивает защиту конфиденциальной информации [1].

Под коммерческой тайной следует понимать сведения, которые не являются секретами государства, но связаны с функционированием организации, управлением ею.

К коммерческой тайне относится информация, обладающая реальной или потенциальной ценностью коммерческого характера вследствие ее неизвестности третьим лицам. К этой информации отсутствует свободный доступ, а ее обладатель принимает меры по обеспечению ее конфиденциальности [2].

К коммерческой тайне относится научно-техническая, производственная, управленческая, финансово-экономическая, маркетинговая и прочая информация о деятельности организации, разглашение которой может причинить ущерб ее интересам [3].

Указанные сведения нуждаются в защите со стороны предпринимателей, так как не представляют собой государственную тайну, не защищены авторским и патентным правом.

В то же время не всякая информация, соответствующая перечисленным критериям, может относиться к коммерческой тайне. Так, согласно ФЗ «О коммерческой тайне» [4] к коммерческой тайне не относятся:

а) учредительные документы и устав;

б) документы, предоставляющие право заниматься предпринимательской деятельностью (патенты, лицензии, регистрационные удостоверения);

в) сведения, которые необходимы для проверки правильности исчисления налогов;

г) документы об уплате налогов;

д) сведения о финансовом состоянии организации;

е) информация о численности и заработной плате работников компании;

ж) данные об участии должностных лиц организации в других компаниях.

Годовая финансовая отчетность организации открыта для заинтересованных пользователей: покупателей, кредиторов, инвесторов, банков, поставщиков и др., которые имеют право знакомиться с этой отчетностью [5].

Основными угрозами безопасности информационных ресурсов компании являются:

а) хищение документа или его части;

б) утрата документа, его чернового варианта, рабочих записей, а также чистого носителя, используемого при составлении документа;

в) несанкционированное уничтожение носителя либо самой информации; подмена документов;

г) несанкционированное копирование информации;

д) неправомерное изменение информации, содержащейся в документе, и т.п. [6].

Конфиденциальная информация может быть получена третьими лицами законным и незаконным способом:

а) в случае если информация получена от ее обладателя на основании договора или на любом другом законном основании (например, по запросу правоохранительных органов), то такая информация считается полученной законным способом;

б) информация считается полученной незаконно, если ее приобретение было сопряжено с умышленным преодолением мер по обеспечению ее конфиденциальности, а также если лицо, получающее информацию, знало или имело достаточные основания считать, что эта информация представляет собой коммерческую тайну, а у лица, передающего информацию, отсутствуют для этого законные основания.

Организации, заинтересованной в охране коммерческой тайны, необходимо обладать соответствующим механизмом, вопросы создания, функционирования и развития которого до сих пор не получили достаточного теоретического обоснования.

Механизм обеспечения сохранности коммерческой тайны представляет собой самоорганизующуюся систему лиц, заинтересованных в деятельности организации, форм и методов управления, рычагов и инструментов, правовых норм и организационно-экономических форм их использования.

Организации, стремящейся обеспечить охрану своей конфиденциальной коммерческой информации, необходимо разработать Положение о коммерческой тайне, представляющее собой локальный нормативно-правовой акт, регулирующий отношения, связанные с обеспечением сохранности защищаемой информации. Наличие такого документа дает возможность руководству организации привлечь к ответственности сотрудников, обнародовавших конфиденциальную информацию. Отсутствие в организации Положения о коммерческой тайне и перечня информации, составляющей коммерческую тайну, а также неознакомление с этими документами работников, имеющих доступ к коммерческой тайне, является основанием для восстановления судом на работе сотрудников, уволенных за разглашение подобной информации.

Действия, связанные с завладением информацией, проходят тайно, посредством их покупки, сбора, хищения либо выдачи [7].

Кроме этого, возможны подмена, искажение, уничтожение конфиденциальной информации, блокирование или разрушение технических средств получения, обработки, хранения и передачи секретной информации. Это делается для того, чтобы не позволить владельцу информации использовать ее для получения экономической выгоды.

Несанкционированный доступ к конфиденциальной информации осуществляется умышленно. Совершая данное правонарушение, злоумышленник осознает, что неправомерно вторгается в информационную систему компании, предвидит возможность наступления вследствие этого отрицательных последствий для организации, сознательно допускает их наступление, или относится к ним безразлично. Цели данного правонарушения могут быть различными: корыстный интерес; стремление причинить вред владельцу информации; желание проверить свои профессиональные способности и т.п. [8].

Нарушителем режима сохранности коммерческой тайны является лицо, которое по ошибке, незнанию или осознанно пытается осуществить запрещенные действия и использует для этого различные способы и средства. Нарушители бывают внутренние и внешние.

Внутренние нарушители – это легитимные сотрудники организации, имеющие доступ к ее информационным ресурсам. Причинами нарушений режима коммерческой тайны внутри организации могут быть ошибки либо умышленные действия работников компании.

Учитывая важность обеспечения сохранности коммерческой тайны для эффективной работы организации, предприниматели стремятся предотвратить ее разглашение неограниченному кругу третьих лиц, указывая в хозяйственных договорах, что содержащаяся в них информация является конфиденциальной. Однако простого указания (в договоре или ином документе) на то, что определенная информация относится к коммерческой тайне, недостаточно [9].

В настоящее время основными методами защиты конфиденциальной информации выступают режимные, то есть специальные меры, направленные на предотвращение утечки охраняемых сведений [10]. Чем больший интерес к таким сведениям может проявляться или фиксировался в прошлом, тем более оперативно должны приниматься меры, противодействующие его удовлетворению.

Для защиты своей конфиденциальной информации предприниматели должны:

а) определить перечень информации, которая составляет коммерческую тайну, и ознакомить с ним под роспись работников организации;

б) нанести на документы, содержащие подлежащую защите информацию, гриф «Коммерческая тайна», поскольку отсутствие такого грифа является основанием для суда восстановить работника, уволенного за нарушение режима коммерческой тайны;

в) ограничить доступ к секретной информации, установив порядок обращения с ней и обеспечив контроль над соблюдением этого порядка;

г) отразить в должностных инструкциях работников, обладающих доступом к коммерческой тайне, обязанности по обеспечению режима ее охраны;

д) создать условия для соблюдения сохранности коммерческой тайны, обеспечив работников необходимыми материальными ресурсами и техническими возможностями (хранение документов и материальных носителей информации в сейфе, металлическом запираемом шкафу, в специально оборудованном помещении и т.п.; ограничение доступа к электронным ресурсам путем: кодирования сообщений, передаваемых по каналам электронной связи; установки устройств, препятствующих снятию информации в процессе ее прохождения по каналам связи; шифрования сведений, установки паролей; использования специальных аппаратов для уничтожения документов);

е) осуществлять учет лиц, имеющих доступ к секретной информации, а также лиц, которым такая информация была предоставлена;

ж) обеспечить регулирование отношений с работниками компании по использованию конфиденциальной информации на основе трудовых договоров, а с контрагентами – на основе гражданско-правовых договоров [11–13].

Наряду с перечисленными мерами, целесообразно использовать «метод паззлов», который предусматривает дробление информации, составляющей коммерческую тайну на фрагменты, каждый из которых должен находиться в различных условиях хранения и использования. Отдельные фрагменты такой информации официально оформляются в качестве коммерческой тайны, другие защищаются патентами, о третьих целесообразно умалчивать, четвертые можно взять из другой технологии и т.п. Такой способ защиты коммерческой тайны затрудняет ее целостное восприятие как собственными сотрудниками компании, так и потенциальными приобретателями. Это является дополнительным инструментом противодействия утечке конфиденциальной информации [10].

Необходимо осуществлять мониторинг системы обеспечения сохранности коммерческой тайны, основной целью которого является предотвращение возможной утечки критически важной информации посредством осуществления постоянного контроля над компьютерами корпоративной сети.

Современные системы компьютерного мониторинга позволяют фиксировать в цифровом формате большинство действий, осуществляемых на компьютере, и представлять для анализа следующую информацию:

а) осуществление входа в информационную систему организации и выхода из нее;

б) нажатие клавиш на клавиатуре компьютера;

в) посещение сотрудниками организации интернет-ресурсов;

г) содержание email-переписки;

д) операции с файлами и папками;

е) запуск приложений и процессов;

ж) подключение USB-устройств;

з) чаты и разговоры в программах мгновенного обмена сообщениями [14].

Анализ перечисленной информации позволяет специалистам службы безопасности организации предотвращать утечку информации, составляющей коммерческую тайну.

Служба безопасности, а в крупных организациях отдел информационной безопасности выполняет следующие функции по обеспечению сохранности коммерческой тайны:

а) защита информации, составляющей коммерческую тайну, а также других жизненно важных для функционирования компании информационных массивов:

б) разработка и осуществление режимных мероприятий, обеспечивающих сохранность коммерческих секретов;

в) противодействие техническим разведкам конкурентов и криминальных структур;

г) реализация комплекса мероприятий по обеспечению безопасности локальных компьютерных сетей;

д) обеспечение безопасной работы в сети Интернет;

е) обеспечение безопасности каналов связи.

При этом служба безопасности должна тесно взаимодействовать с другими структурными звеньями организации, например, с отделом кадров, который должен ознакомить сотрудников с перечнем сведений, содержащих коммерческую тайну, а также включить в должностные инструкции и трудовые договоры сотрудников, допущенных к использованию секретной информации, обязанность по ее неразглашению; с юридическим отделом, осуществляющим административно-правовое сопровождение мероприятий по обеспечению сохранности коммерческой тайны и т.п.

Для оценки эффективности работы по обеспечению сохранности коммерческой тайны можно использовать следующую систему показателей:

– попытки несанкционированного доступа к локальной сети организации со стороны конкурентов или криминальных структур;

– попытки несанкционированного доступа к локальным сетям со стороны сотрудников, не имеющих допуска;

– утечка информации на электронных и бумажных носителях в результате нарушения сотрудниками инструкций по обеспечению информационной безопасности организации;

– контакты сотрудников организации с представителями конкурентов или криминальных структур;

– разглашение сотрудниками конфиденциальной информации;

– несанкционированное уничтожение или изменение информации;

– блокирование или разрушение технических средств, используемых для работы с информацией;

– неисправность приборов круглосуточного видеонаблюдения и мониторинга всех информационных ресурсов.

Каждую из перечисленных выше угроз сохранности коммерческой тайны можно охарактеризовать количеством выявленных случаев. При этом оценка эффективности работы подразделения, отвечающего за охрану коммерческой тайны, не должна способствовать сокрытию выявленных случаев утечки конфиденциальной информации.

При разработке и реализации мероприятий по обеспечению сохранности коммерческой тайны необходимо руководствоваться принципом экономичности, согласно которому сумма средств, расходуемых при проведении мероприятий, обеспечивающих защиту коммерчески ценных сведений, не должны превышать ценности охраняемой информации, а затраты на защиту такой информации не должны превышать ущерб, который может быть получен в результате ее разглашения [15]. Поэтому при проведении дальнейших исследований необходимо разработать методику оптимизации затрат на функционирование системы защиты конфиденциальной информации.

Выводы

В условиях рыночной экономики коммерческая тайна является активом, позволя-

ющим ее обладателю получать конкурентные преимущества и извлекать экономическую выгоду. Это обусловливает необходимость обеспечения защиты данного актива от неправомерного завладения третьими лицами. Основными методами защиты коммерческой тайны являются режимные меры, направленные на предотвращение конфиденциальной информации. Организациям необходимо осуществлять мониторинг эффективности функционирования системы обеспечения сохранности коммерческой тайны с использованием для этого современных средств программного обеспечения и предлагаемой авторами системы оценочных показателей.

Список литературы

1. Жижерина Ю. Устанавливаем режим коммерческой тайны // Кадровая служба и управление персоналом предприятия. 2014. № 11. [Электронный ресурс]. URL:https://wiseeconomist.ru/poleznoe/89260-ustanavlivaem-rezhim-kommercheskoj-tajny (дата обращения: 21.07.2020).

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (с последними изменениями, внесенными ФЗ от 16.12.2019 № 430-ФЗ). [Электронный ресурс]. URL:http://logos-pravo.ru/grazhdanskiy-kodeks-gk-rf-chast-1 (дата обращения: 22.07.2020).

3. Раздина Е.А. Коммерческая информация и экономическая безопасность предприятия // Бизнес-информ. 2017. № 24. С. 63–65.

4. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне». [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 22.07.2020).

5. Приказ Минфина России от 29.07.1998 № 34н (ред. от 11.04.2018) «Об утверждении Положения по ведению бухгалтерского учета и бухгалтерской отчетности в Российской Федерации» (Зарегистрировано в Минюсте России 27.08.1998 № 1598). [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_20081 (дата обращения: 22.07.2020).

6. Обеспечение информационной безопасности бизнеса / Под ред. А.П. Курило. М.: БЦД-пресс, 2011. 392 с.

7. Исамидинов А.Н. Защита коммерческой тайны в сфере трудовых отношений. М.: Ленанд, 2014. 120 с.

8. Деменченок О.Г., Баранов С.А., Позанова И.А., Полянский И.С. Информационная безопасность. Иркутск: Восточно-Сибирский институт МВД РФ, 2010. 112 с.

9. Сидоров С.С. Регулирование и поддержка экономической безопасности предприятий в ЕС и России // Финансы. 2015. № 1. С. 88–98.

10. Галифанов Р.Г., Карлиев Р.А., Галифанов Г.Г. О секретных изобретениях и коммерческой тайне // Интеллектуальная собственность. Промышленная собственность. 2018. № 7. С. 15–30.

11. Ситникова Е.Г., Сенаторова Н.В. Оформление трудовых отношений: образцы документов, комментарии и разъяснения. М.: Редакция «Российской газеты», 2016. 108 с.

12. Валова Е.А., Кузнецов Ф.В. Незаконные получение и разглашение сведений, составляющих коммерческую тайну // Законность. 2018. № 4. С. 43–46.

13. Казанок Е. Установление режима коммерческой тайны в компании: пошаговая инструкция. [Электронный ресурс]. URL: https://regforum.ru/posts/2392_kak_zaschitit_kommercheskuyu_taynu_na_predpriyatii_9_shagov_dlya._rabotodatelya (дата обращения: 22.07.2020).

14. Обеспечение информационной безопасности. Официальный сайт компании «Атом безопасность». [Электронный ресурс]. URL: https://www.staffcop.ru/information-security (дата обращения: 22.07.2020).

15. Грунтовский И.И. Правовая среда общества как основа безопасности бизнеса // Безопасность бизнеса. 2017. № 3. С. 20–25.