УПРАВЛЕНИЕ ПЕРСОНАЛОМ
HUMAN RESOURCES MANAGEMENT

DOI: 10.18287/2542-0461-2020-11-4-83-89
УДК 330
Научная статья / Scientific article

Дата: поступления статьи / Submitted: 22.09.2020
после рецензирования / Revised: 18.10.2020
принятия статьи / Accepted: 27.11.2020

И.Н. Махмудова
Самарский национальный исследовательский университет имени академика С.П. Королева,
г. Самара, Российская Федерация
E-mail: Mahmudova.I@yandex.ru. ORCID: https://orcid.org/0000-0002-9943-3839

Влияние кадровых угроз на экономическую безопасность организации

Аннотация: Тема обеспечения безопасности компании является центральной в работе службы безопасности. В данной статье описаны факторы, создающие угрозу безопасности современной организации. Раскрыты возможные направления рисков, обусловленных действиями персонала организации, создающих кадровые угрозы. Определена роль кадровой безопасности и ликвидации кадровых угроз в системе обеспечения безопасности организации. В статье раскрывается понятие конкурентной (деловой) разведки, выявлены функции данной службы. Раскрыто понятие «промышленный шпионаж». В оперативной практике выясняется, что большое количество кадровых угроз представлено широким разнообразием. При этом для нейтрализации кадровых угроз, полномочий и компетентности работников службы безопасности организации явно недостаточно. В связи с этим в рамках данного исследования рассмотрен комплекс мероприятий, составляющих целостную систему безопасности. Центральное место в исследовании отведено вопросу устранения кадровых угроз. Поскольку кадровые угрозы создаются собственным персоналом организации, то обоснована необходимость взаимодействия всех служб по работе с персоналом в рамках единой системы обеспечения кадровой безопасности и безопасности организации в целом. Разграничены полномочия каждого из участников данного процесса в их взаимосвязи и взаимодействии. Определены меры противодействия кадровым угрозам и нейтрализации негативных последствий от несанкционированных действий в организации.

Ключевые слова: безопасность организации, кадровые риски, угрозы, кадровая безопасность, конкурентная (деловая) разведка, промышленный шпионаж, система безопасности, методы конкурентной борьбы.
Цитирование. Махмудова И.Н. Влияние кадровых угроз на экономическую безопасность организации // Вестник Самарского университета. Экономика и управление. 2020. Т. 11, № 4. С. 83–89. DOI: http://doi.org/10.18287/2542-0461-2020-11-4-83-89.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

I.N. Makhmudova
Samara National Research University, Samara, Russian Federation
E-mail: Mahmudova.I@yandex.ru. ORCID: https://orcid.org/0000-0002-9943-3839

The impact of personnel threats on the economic security of the organization

Abstract: The topic of company security is central to the work of the security service. This article describes the factors that pose a threat to the security of a modern organization. The author discloses possible directions of risks caused by the actions of the organization's personnel that create personnel threats. The article determines the role of personnel security and elimination of personnel threats in the organization's security system. The article reveals

the concept of competitive (business) intelligence, identifies the functions of this service. The concept of «industrial espionage» is disclosed. In operational practice, it turns out that a large number of personnel threats are represented by a wide variety. In operational practice, it turns out that a large number of personnel threats are represented by a wide variety. At the same time, in order to neutralize personnel threats, the powers and competence of the organization's security personnel are clearly not enough. In this regard, within the framework of this study, a set of measures that make up an integral security system is considered. The central place in the study is devoted to the issue of eliminating personnel threats. Since personnel threats are created by the organization's own personnel, the necessity of interaction of all personnel services within the framework of a single system for ensuring personnel safety and security of the organization as a whole is substantiated. The powers of each of the participants in this process in their relationship and interaction are delimited. The author defined measures to counter personnel threats and neutralize the negative consequences of unauthorized actions in the organization.

Key words: security of the organization, personnel risks, threats, personnel security, competitive (business) intelligence, industrial espionage, security system, methods of competition.

Citation. Makhmudova I.N. The impact of personnel threats on the economic security of the organization. *Vestnik Samarskogo universiteta. Ekonomika i upravlenie = Vestnik of Samara University. Economics and Management*, vol. 11, no. 4. pp. 83–89. DOI: http://doi.org/10.18287/2542-0461-2020-12-1-83-89. (In Russ.)

Information on the conflict of interest: author declares no conflict of interest.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHOR

© *Ирина Николаевна Махмудова* – доктор экономических наук, профессор кафедры управления человеческими ресурсами, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

© *Irina N. Makhmudova* – Doctor of Economics, professor of the Department of Human Resource Management, Samara National Research University, 34 Moskovskoye shosse, Samara, 443086, Russian Federation.

Введение

Вопрос устранения кадровых угроз для обеспечения безопасности компании является центральным в работе службы безопасности. Однако в оперативной практике выясняется, что большое количество кадровых угроз представлено широким разнообразием. При этом для нейтрализации кадровых угроз, полномочий и компетентности работников службы безопасности организации явно недостаточно. В связи с этим в рамках данного исследования будем рассматривать комплекс мероприятий, составляющих целостную систему безопасности. Более того, разграничим полномочия всех участников данного процесса в их взаимосвязи и взаимодействии.

Ход исследования

Прежде чем перейти к анализу рисков, приводящих к кадровым угрозам, необходимо уделить внимание тем факторам, которые способны дестабилизировать обстановку в компании, вызвать несанкционированные действия со стороны персонала.

Цифровая экономика внесла свои коррективы в деятельность современных предприятий. Сложились новые конкурентные отношения в бизнес-среде за рынки сбыта, финансы, кадровые и материальные ресурсы. Выживание бизнеса подвергается риску со стороны неконтролируемых воздействий внешней среды. Они определяются прежде всего тем, что:

– область конкурентных отношений становится крайне обостренной в силу внедрения новых цифровых технологий в деятельность современных предприятий, а следовательно, и более рискованной;

– многие рыночные механизмы в области обеспечения экономической безопасности предприятий не срабатывают, поскольку на предприятиях не сформирована целостная система мер безопасности либо она действует фрагментарно;

– рынок деловой информации для обеспечения экономической и кадровой безопасности в организациях в силу конфиденциальности информации сформирован не в достаточном объеме. Ни одно предприятие не готово делиться секретами организации собственной службы безопасности, чтобы не подвергаться риску негативного воздействия извне.

Вместе с тем немалую долю в профиле рискогенных факторов любой организации составляют кадровые риски. Именно поэтому, прежде чем говорить об экономической безопасности, следует тщательно выстроить систему кадровой безопасности в организации.

Само понятие «кадровая безопасность» двоякое по своему содержанию. С одной стороны, она нацелена на защиту прав персонала от неправомерных действий работодателя, которые причиняют им серьезный вред. Все еще имеют место такие нарушения со стороны работодателя, как:

– задержки выплаты заработной платы;

– подмена трудовых договоров на гражданско-правовые при трудоустройстве граждан;

– нарушение режима труда и отдыха сотрудников (например, непредоставление заслуженного отпуска или, напротив, отправка работника в вынужденный (неоплачиваемый) отпуск);

– незаконное увольнение и многое другое.

С другой стороны, кадровая безопасность включает защиту самой организации от несанкционированных действий или бездействий ее персонала. К их числу можно отнести:

– воровство,

– приписки,

– сговор с конкурирующими сторонами,

– подлог,

– порчу имущества работодателя,

– хищения,

– разглашение конфиденциальной информации и многое другое.

Однако поскольку каждой организации важно занять свое достойное место в конкурентной среде по отношению к другим организациям, то одним из самых дорогих и сложно обеспечиваемых преимуществ организации является ее интеллектуальный капитал, а также охрана интеллектуальной собственности. Интеллектуальный капитал способен многократно увеличивать рыночную стоимость самой организации, а потому организация становится достаточно привлекательной для инвесторов. Кроме того, интеллектуальный капитал организации является потенциальным объектом в привлечении внимания как со стороны конкурентной разведки, так и со стороны промышленного шпионажа и прочих недобросовестных методов конкурентной борьбы. Известны случаи хищения запатентованного продукта и использования его в личных целях для наживы. О таком примере рассказал Александр Костанянц, профессор кафедры управления фирмой Высшей школы корпоративного управления РАНХиГС: в российскую компанию пригласили менеджера для развития запатентованного продукта. Он похитил компьютерные коды компании, выехал в США, где зарегистрировал свою фирму, после чего начал продвигать видоизмененный продукт на российском рынке. В итоге его осудили по статье 147 УК РФ за незаконное использование патентного права [1].

Функции службы конкурентной (деловой) разведки

Чтобы обеспечить экономическое благополучие организации, необходимо своевременно выявлять и адекватно реагировать на выявленные кадровые угрозы. Для этого должна быть организована в структуре компании самостоятельная информационно-аналитическая служба обеспечения безопасности или служба конкурентной (деловой) разведки. В ее задачи входят сбор и обеспечение руководителей соответствующих структур полноценной и актуальной деловой информацией. Благодаря наличию такой информации принимаемые управленческие решения будут своевременными и оптимальными. К задачам службы можно отнести:

– сбор, анализ и систематизацию данных бизнес-среды и кадровых угроз внутри компании, то есть выявление внешних и внутренних угроз функционирования организации;

– обнаружение рисков и подготовку рекомендаций по вопросам правовой защиты от противоправных кадровых угроз;

– работу с финансовыми документами в инвестиционной сфере в России и за рубежом;

– применение методов конкурентной разведки в сборе информации по конкурирующим фирмам (анализ процессов и тенденций их развития, а также составление психологического портрета их руководителей-лидеров);

– разработку концепции экономической безопасности организации, подготовку стратегического плана развития организации;

– разработку и реализацию отдельных организационно-управленческих и финансовых проектов и технологий.

Система обеспечения кадровой безопасности в организации

Кадровые угрозы безопасности организации способны формироваться по всем направлениям деятельности персонала. Именно поэтому службе конкурентной разведки необходимо в первую очередь наладить тесный контакт со службой управления персоналом в лице ее директора (не отдела кадров!). Следует отдельно оговориться, что работой с персоналом занимается именно директор по персоналу (отдел по работе с персоналом). Отдел кадров к оперативной работе с персоналом не имеет никакого отношения. Он ведет документальное оформление работы с персоналом, фиксирует итоги работы каждого сотрудника в личных делах (т. е. это работа с документами). И структурно отдел кадров подчиняется директору по персоналу наравне с отделом организации труда и мотивации (заработной платы – ООТиЗ), учебным центром (или отделом развития персонала), отделом оценки и аттестации персонала и социальной службы. Отдел по подбору персонала в структуре организации может находиться в качестве самостоятельного элемента, но также это может быть служба в структуре отдела кадров. Как видно, практически все участки работы персонала представлены отдельными структурными подразделениями или службами. Производственный персонал подконтролен линейным руководителям и их вышестоящим руководителям.

В связи с этим система безопасности организации не должна работать автономно от всех названных служб, если она хочет быть эффективной. Другими словами, систему безопасности в организации обеспечивает не только служба безопасности, но вся дирекция по персоналу и каждый отдельный сотрудник организации. В функции дирекции (службы) по работе с персоналом непосредственно входит обнаружение различного рода кадровых угроз.

Поскольку речь идет о службе конкурентной разведки, то следует определить само понятие. Разведка – это «сбор сведений о противнике или конкуренте для обеспечения своей безопасности и получения преимуществ в области вооруженных сил, военных действий, политики или экономики» [2]. Разведка может использовать как законные способы сбора информации (например, сбор и анализ данных из открытых источников, прослушивание радиоканалов из-за границы, наблюдение при помощи разведывательных спутников), так и незаконные операции, попадающие под понятия «шпионаж» или «кража информации».

Конкурентная разведка является вполне уместной и законной. Собранные ею разведданные преобразуются в новые направления и проекты для эффективного развития организации. В отличие от конкурентной разведки, промышленный шпионаж использует методы незаконного тайного хищения сведений с помощью специального оборудования (технических устройств) или персонального компьютера [3]. Доступными становятся данные, хранящиеся на сервере или в «облаке», на электронной почте, телефонные разговоры, то есть любая информация и на любом носителе [4]. Полученные сведения, составляющие коммерческую, налоговую или банковскую тайну, могут быть разглашены или незаконно использованы. В России промышленный шпионаж преследуется по закону [5–11]. В частности, за использование промышленного шпионажа предусмотрена статья 183 Уголовного кодекса с лишением свободы сроком до десяти лет.

Направления и меры противодействия кадровым угрозам

Как противостоять кадровым угрозам и промышленному шпионажу? Как обеспечить экономическую безопасность организации?

Прежде всего необходимо проводить комплекс мероприятий по управлению кадровой безопасностью, начиная с формирования сильной кадровой политики. Чтобы защитить организацию от потенциальных злоумышленников, нужно поставить первый барьер уже при отборе кадров при найме. Для этого требуются высокопрофессиональные рекрутеры, способные проводить качественную экспресс-диагностику всеми доступными методами оценки, как в работе с соискателем, так и с предоставлен-

ной им документацией. Важно перепроверить информацию. В работе с резюме использовать приемы «поиска узких мест», «чтения между строк», если потребуется, провести «контент-анализ». При проведении интервью использовать прием «если не секрет», «перехвата», задавать уточняющие вопросы – УУВ (универсальный уточняющий вопрос – «Уточните, пожалуйста, что вы имеете в виду, говоря...») – и, главное правило, не додумывать за соискателя то, о чем он хочет сказать!

Другое направление в нейтрализации кадровых угроз для обеспечения безопасности организации – это работа с действующим персоналом. И в этом направлении необходимо обеспечить проведение качественного инструктажа, подкрепленного регулярным контролем исполнения.

Требуется также проводить регулярное информирование персонала по поводу понимания, какая информация не составит угрозу безопасности, а какая является сугубо конфиденциальной и не подлежит разглашению. Вплоть до подписания документов о неразглашении коммерческой тайны. Именно на этом этапе важна четкая работа службы безопасности, которая должна отслеживать и вовремя пресекать (с помощью IT-служб и другими возможными средствами) случаи утечки информации.

Хорошую службу может сослужить продуманная система мотивации персонала. Важно при этом достигать не только полной удовлетворенности работников работой и результатами труда (читай – справедливой оплатой), но также предоставлять возможность открыто «выговориться» (система обратной связи), не опасаясь за свое положение и угрозы быть уволенным. Поскольку всегда найдется «доброжелатель» («случайный собеседник»), который готов выслушать все тайное и использовать полученную информацию для развала организации.

Поскольку сегодня повсеместно ведется электронный документооборот, создаются электронные хранилища с базами данных (необходимые для успешной и эффективной работы предприятия), то важным направлением обеспечения безопасности организации в плане хранения и передачи информации становится формирование мошной IT-службы, способной противостоять различного рода техническим сбоям и хакерским атакам. В октябре 2018 года Корпорация по управлению доменными именами и IP-адресами (ICANN) провела первую в истории замену криптографических ключей, которые служат защитой для системы доменных имен Интернета (DNS) [12]. Такая смена ключей (Key Signing Key, KSK) необходима для любого пользователя сети Интернет. Она повышает степень защиты информации. И в организациях в рамках обеспечения системы безопасности также рекомендуется время от времени с определенной регулярностью следить за сменой паролей на персональных компьютерах специалистов и служащих.

Невозможно обойти стороной и правовой аспект обеспечения безопасности организации. Важно иметь не только юридический отдел в структуре организации, но и формировать правовую грамотность специалистов и руководителей, способных предусмотреть и на своем уровне ликвидировать потенциальные угрозы кадровой безопасности. Примером могут быть неправильно начисленная заработная плата; ошибки в оформлении договоров при приеме на работу (прежде всего терминологические) и при увольнении сотрудников; ошибки ведения финансовых документов; ошибки в принятии управленческих решений, оборачивающиеся конфликтом с персоналом, и др.

Заключение

Подводя итог, необходимо отметить следующее.

1. Методы «конкурентной разведки», в отличие от «промышленного шпионажа», являются вполне законными, а собранная ею информация преобразуется в новые направления и проекты для эффективного развития организации. Промышленный шпионаж, напротив, использует методы незаконного тайного хищения сведений с помощью специального оборудования, а полученные сведения, составляющие коммерческую, налоговую или банковскую тайну, могут быть разглашены или незаконно использованы. В связи с этим службе безопасности следует активно выявлять субъектов как источника кадровых угроз, привлекаемых к деятельности или осуществляющих промышленный шпионаж в организации.

2. Предложен комплекс мероприятий по управлению кадровой безопасностью, включающий формирование сильной кадровой политики, прежде всего на этапе найма персонала. В рамках работы с

действующим персоналом – проведение качественного инструктажа, подкрепленного регулярным контролем исполнения. Осуществлять регулярное информирование персонала по поводу понимания, какая информация является сугубо конфиденциальной и не подлежит разглашению. В рамках повышения мотивации персонала – сделать акцент на организации системы обратной связи. Для ведения электронного документооборота и обеспечения безопасности электронных хранилищ с базами данных – сформировать мощную IT-службу, способную противостоять различного рода техническим сбоям и хакерским атакам. Дополнительно формировать правовую грамотность специалистов и руководителей, способных предусмотреть и на своем уровне ликвидировать потенциальные угрозы кадровой безопасности.

3. Система безопасности организации не должна работать автономно от служб, причастных к работе с персоналом, если она хочет быть эффективной. Другими словами, систему безопасности в организации обеспечивает не только служба безопасности, но и вся дирекция по персоналу и каждый отдельный сотрудник организации. Предложено создание коллективной системы кадровой безопасности с целью обеспечения оперативно-тактических действий, оказывающих положительное воздействие на координацию и синхронизацию функционирования отдельных служб по локализации, нейтрализации и устранению кадровых угроз.

Библиографический список

1. Коммерческие тайны чаще всего выведывают через сотрудников. URL: https://rg.ru/2018/12/05/kommercheskie-tajny-chashche-vsego-vyvedyvaiut-cherez-sotrudnikov.html (дата обращения 27.08.2020)

2. Википедия. URL: https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B0 (дата обращения: 05.09.2020).

3. Кравцов А.А., Желнов И.И. О промышленном и экономическом шпионаже, а также недобросовестной конкуренции // Мир науки. 2014. № 1. С. 15. URL: https://www.elibrary.ru/item.asp?id=21610160.

4. Противодействие промышленному шпионажу: чем грозят незаконная конкуренция и кража информации. URL: https://www.hr-director.ru/article/65692-qqq-15-m9-protivodeystvie-promyshlennomu-shpionaju (дата обращения: 06.09.2020)

5. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (в ред. от 06.10.1997 № 131-ФЗ) (с изменениями на 29 июля 2018 года). URL: http://docs.cntd.ru/document/9004687 (дата обращения: 19.08.2020)

6. Об информации, информационных технологиях и о защите и информации: федер. закон от 27.07.2006 № 149-ФЗ (в ред. от 03.04.2020) // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3448. URL: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002006031000&docid=104 (дата обращения: 27.08.2020)

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 31.07.2020) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954. URL: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001996025000&docid=4886 (дата обращения: 13.09.2020).

8. Об оперативно-розыскной деятельности: федер. закон от 12.08.1995 № 144-ФЗ (ред. от 02.08.2019) // Собрание законодательства РФ. 14.08.1995. № 33. Ст. 3349. URL: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001995033000&docid=106 (дата обращения: 19.08.2020).

9. О безопасности: федер. закон от 28.12.2010 № 390-ФЗ (ред. от: 06.02.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_108546 (дата обращения: 19.08.2020).

10. О коммерческой тайне: федер. закон от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) // Собрание законодательства РФ. 09.08.2004. № 32. Ст. 3283. URL: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002004032000&docid=26 (дата обращения: 13.08.2020).

11. О защите конкуренции: федер. закон от 26.07.2006 № 135-ФЗ (ред. от 24.04.2020). URL: http://www.consultant.ru/document/cons_doc_LAW_61763 (дата обращения 19.08.2020).

12. Защита доменных имен. URL: https://rg.ru/2018/10/11/chem-grozit-internet-polzovateliam-pervaia-v-istorii-smena-kriptograficheskih-kliuchej.html (дата обращения: 15.08.2020).

References

1. Trade secrets are most often found out through employees. Available at: https://rg.ru/2018/12/05/kommercheskie-tajny-chashche-vsego-vyvedyvaiut-cherez-sotrudnikov.html (accessed 27.08.2020). (In Russ.)

2. Wikipedia. Available at: https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B0 (accessed 05.09.2020). (In Russ.)

3. Kravtsov A.A., Zhelnov I.I. Industrial and economic espionage, and unfair competition. *World of Science*, 2014, no. 1, p. 15. Available at: https://www.elibrary.ru/item.asp?id=21610160. (In Russ.)

4. Counteraction to industrial espionage: what is the threat of illegal competition and information theft. Available at: https://www.hr-director.ru/article/65692-qqq-15-m9-protivodeystvie-promyshlennomu-shpionaju (accessed 06.09.2020). (In Russ.)

5. Law of the Russian Federation dated July 21, 1993 № 5485-1 «Concerning State Secrets» (as amended on October 6, 1997 № 131-FZ) (as amended on July 29, 2018). Available at: http://docs.cntd.ru/document/9004687 (accessed 19.08.2020). (In Russ.)

6. Federal Law dated 27.07.2006 № 149-FZ (as amended on 03.04.2020) «On information, information technologies and on protection and information». *Collected Legislation of the Russian Federation*, 31.07.2006, no. 31 (part 1), Article 3448. Available at: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002006031000&docid=104 (accessed 27.08.2020). (In Russ.)

7. Criminal Code of the Russian Federation dated 13.06.1996 № 63-FZ (as amended on 31.07.2020). *Collected Legislation of the Russian Federation*, 17.06.1996, no. 25, Article 2954. Available at: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001996025000&docid=4886 (accessed 13.09.2020) (In Russ.)

8. Federal Law dated 12.08.1995 № 144-FZ «Concerning Investigative Activities» (as amended on 02.08.2019). *Collected Legislation of the Russian Federation*, 14.08.1995, no. 33, Article 3349. Available at: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1001995033000&docid=106 (accessed 19.08.2020). (In Russ.)

9. Federal Law dated 28.12.2010 № 390-FZ «On Security». Last updated: 06.02.2020. Available at: http://www.consultant.ru/document/cons_doc_LAW_108546 (accessed 19.08.2020). (In Russ.)

10. Federal Law dated 29.07.2004 № 98-FZ «On Commercial Secrets» (as amended on 18.04.2018). *Collected Legislation of the Russian Federation*, 09.08.2004, no. 32, Article 3283. Available at: http://www.szrf.ru/szrf/doc.phtml?nb=100&issid=1002004032000&docid=26 (accessed 13.08.2020). (In Russ.)

11. Federal Law dated 26.07.2006 № 135-FZ «On Protection of Competition». Last updated: 24.04.2020. Available at: http://www.consultant.ru/document/cons_doc_LAW_61763 (accessed 19.08.2020). (In Russ.)

12. Protection of domain names. Available at: https://rg.ru/2018/10/11/chem-grozit-internet-polzovateliam-pervaia-v-istorii-smena-kriptograficheskih-kliuchej.html (accessed 19.08.2020). (In Russ).