Оценка инсайдерских угроз в системе кадровой безопасности организации

Assessment of Insider Threats in the Personnel Security System of the Organization

УДК 330.101

DOI: 10.12737/1998-0701-2022-8-10-36-40

П.В. Симонин, канд. экон. наук, доцент департамента менеджмента и инноваций, факультет «Высшая школа управления», Финансовый университет при Правительстве Российской Федерации

e-mail: pvsimonin@fa.ru, simoninp-v@mail.ru

Т.Б. Курбацкая, канд. психол. наук, доцент, доцент кафедры «Экономическая теория и менеджмент», РОАТ Российский университет транспорта

e-mail: alterego123@yandex.ru

П.Т. Сизов, магистрант кафедры «Экономическая теория и менеджмент», РОАТ Российский университет транспорта

e-mail: pt-siz@yandex.ru

P.V. Simonin, Candidate of Economic Sciences, Associate Professor, Department of Management and Innovation, Faculty of Higher School of Management, Financial University under the Government of the Russian Federation

e-mail: pvsimonin@fa.ru, simoninp-v@mail.ru

T.B. Kurbatskaya, Candidate of Psychological Sciences, Associate Professor, Department "Economic Theory and Management", ROAT Russian University of Transport

e-mail: alterego123@yandex.ru

P.T. Sizov, Master's Degree Student, Department of Economic Theory and Management, ROAT Russian University of Transport

e-mail: pt-siz@yandex.ru

Аннотация. *В статье рассматриваются проблемы и пути решения инсайдерских угроз в системе кадровой безопасности организации и доказывается, что персонал организации нуждается в защите и одновременно может выступать источником угроз и опасностей. Обосновывается необходимость использования методики оценки инсайдерских угроз в системе кадровой безопасность на основе выделения групп инсайдеров: фактических работников, ранее высвобожденного персонала, деловых партнеров и других пользователей.*

Ключевые слова: инсайдерские угрозы, экономическая безопасность, проприетарная информация, кадровая безопасность, персонал.

Abstract. *The article discusses the problems and ways of solving insider threats in the organization's personnel security system, proves that at the same time the organization's personnel needs protection, and can act as a source of threats and dangers. The necessity of using a methodology for assessing insider threats in the personnel security system based on the identification of a group of insiders: actual employees, previously released personnel, business partners and other users is substantiated.*

Keywords: insider threats, economic security, proprietary information, personnel security, personnel.

Концепция «безопасности человека» родилась в начале 1990-х годов, заменив идею «общей безопасности». Безопасность человека подразумевает сотрудничество в борьбе с общими угрозами для человечества в целом, такими как глобальное потепление и пандемии.

Парадигмальное понимание системы кадровой безопасности неразрывно связано с инновациями, которые связывают науку и технику в области информации и коммуникаций с социальной инфраструктурой, гарантируя, что новые системы, полезные для общества, появляются и внедряются на основе проверенных технологий[7].

Вопросы безопасности приобрели особое значение для поддержания стабильного развития российского общества и государства в условиях постоянных непредсказуемых социально-экономических изменений. Одновременно значимость кадровой безопасности подтверждается и исследованиями по проблемам реализации отдельных видов безопасности. Так, в глобальном исследовании по информационной безопасности аудиторской

компании «Ernst and Young» отмечалось, что человек остается самым слабым местом в обеспечении информационной безопасности [2].

Понятие «кадровая безопасность» представляет собой процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом. Оценивая кадровую безопасность с точки зрения управления, видно, что она занимает доминирующее положение по отношению к другим элементам экономической безопасности, так как она «работает» с людьми (персоналом, кадрами), она является первичной составляющей [3].

Одновременно растет понимание того, что безопасность персонала — это система политик, стандартов, процедур и технических мер, которые в совокупности снижают риск использования законного доступа к активам в несанкционированных целях. В частности, такая политика направлена на смягчение «инсайдерской угрозы» и связанных с ней рисков, причинами которых являются неотъемлемые уязвимости, возникающие в результате случайных, небрежных или преднамеренных (злонамеренных) действий сотрудников [5].

К угрозам кадровой безопасности организации относятся: неблагонадежность сотрудников, их девиантное поведение, нелояльность, негативный социально-психологический климат, несовершенство корпоративной культуры, совершение ошибок при подборе персонала. Обобщая подходы к определению угроз кадровой безопасности, можно сказать, что они представляют собой сочетание факторов, которые представляют угрозу жизненно-важным интересам всех участников социально-трудовых отношений [1].

Практические потребности в разрешении проблем кадровой безопасности связаны с риском в системе «человек-ноксосфера-рабочая среда-конкуренты», подразумевающим потенциальную готовность субъекта угроз нанести ущерб объекту безопасности. Этот факт позволяет нам сделать вывод, что появление или отсутствие угрозы безопасности определяется наличием субъектных и объектных отношений.

Если следовать антропологической концепции безопасности, то предметом угроз кадровой безопасности являются люди. Неоклассическая теория экономики определяет человека, с одной стороны, как рационалиста, с другой стороны, как трудовой ресурс, который является источником дохода. В данном случае рационализм работника является экономической основой кадровых опасностей и угроз. При этом угрожать могут не только нынешние сотрудники, но и претенденты на вакантные должности, а также бывшие сотрудники организации.

В качестве объекта безопасности человека следует рассматривать организационные ресурсы работодателя, такие как: материальные, финансовые, имущественные, человеческие (трудовые), информационные и т.д. В этом случае объектом угроз могут выступать сотрудники организации, при этом речь идет не о кадровой безопасности организации, а о безопасности для персонала организации.

Таким образом, в субъектно-объектных отношениях кадровой безопасности персонал организации может выступать как в качестве субъекта, так и в качестве объекта угроз, что означает, что угроза безопасности персонала носит двусторонний характер. С одной стороны, персонал организации нуждается в защите, а с другой стороны — может выступать источником угроз и опасностей [8, с.2].

Например, количество преднамеренных утечек из коммерческих и государственных организаций в России только за 2020 г. выросло на 60%. В последнее время увеличилась интенсивность утечки корпоративных данных (с помощью фотографий и скриншотов экранов, а удельный вес таких «сливов» составляет 35% от общего количества). В то же время сотрудники с высокой цифровой грамотностью скрупулезно относятся к данным, таким образом, у инсайдера намного меньше шансов получить информацию, т.е. она до него не доходит благодаря бдительным коллегам. Одновременно около 80% нарушений приходится на сотрудников компаний, причем три четверти случаев — умышленные действия и приходятся они на период пандемии. Большой процент зафиксированных утечек по вине персонала предположительно связан с высоким уровнем выявления подобных инцидентов прежде всего в банках и в госорганах [4].

Очевидным является то, что получение ключевых документов путем доступа к ним

через виртуальную частную сеть и использование неавторизованной внешней коммерческой электронной почты (без использования авторизованного внутреннего почтового сервера) также могут являться причиной серьезной утечки данных [10, с.12–13].

В современном обществе люди используют различное цифровое оборудование, такое как: сотовые телефоны, ноутбуки, планшеты и персональные компьютеры, подключенные к Интернету, для общения друг с другом и обмена информацией. Следовательно, современная безопасность становится все более взаимосвязанной и зависимой от ИТ-безопасности.

Деформация институтов защиты данных в организациях связана с ИТ-безопасностью, которая включает в себя не только защиту систем организации от атак, но и предотвращение обмана и утечки ценной информации.

С одной стороны, благодаря интеллекту сообщества black hat («черная шляпа») существует множество методов взлома, таких как переполнение буфера, внедрение SQL и межсайтовые скрипты, которые могут быть использованы для атаки на компьютерные системы в целях доступа к конфиденциальной информации. Эти атаки зависят от использования уязвимостей программных систем, которые могут быть устранены путем своевременного обновления системы и дополнения производственной системы средствами безопасности, такими инструментами, как брандмауэр и система обнаружения вторжений.

С другой стороны, некоторые хакеры впервые применили искусство взлома (т.н. фрикинг) и различные виды атак социальной инженерии в целях обмана человека и получения ценной информации, такой как: имена учетных записей, идентификационные номера и даже пароли, которые могут быть использованы в дальнейшем [11].

Сегодня нахождение новых способов оценки кадровых рисков, защиты данных в информационном пространстве, по сути, характеризует основную стратегию развития системы кадровой безопасности на предприятии. Зададимся вопросами: устойчив ли бизнес в ответ на инсайдерские угрозы, исходящие от персонала или бывших сотрудников? Адекватны ли предпринимаемые меры для предотвращения утечки информации? Как можно обнаружить и оценить риски, связанные с злонамеренными инсайдерами, партнерами и необразованными контрагентами?

Согласно опросу американских компаний, 60% организаций сталкивались с кражей проприетарной (фирменной) информации и в последние годы эта цифра росла в геометрической прогрессии. Так, например, американские компании по этой причине ежегодно теряют более 250 миллиардов долларов. Это привело к росту беспокойства руководства компаний и снижению уровня организационного доверия. По сути дела, для того, чтобы противостоять инсайдерским атакам, организациям необходимо разработать системы обнаружения инсайдерских угроз, позволяющие выявлять злоумышленников до того, как они смогут организовать свои атаки [6].

С позиции парадигмы кадровой безопасности существуют два основных типа инсайдеров: злонамеренные пользователи (те, которые намеренно наносят вред организациям) и непреднамеренные инсайдерские пользователи (те, которые случайно раскрывают конфиденциальные данные). В этой связи трудно не согласиться, что действия всех этих инсайдеров ставят под угрозу конфиденциальность, целостность и доступность бизнеса. Мотивы, стоящие за злонамеренными инсайдерами, могут включать: денежную выгоду, недовольного сотрудника, права, идеологию или внешнее влияние с последствиями мошенничества, саботажа, шпионажа и кражи или потери конфиденциальной информации.

Одной из узловых проблем кадровой безопасности является вредоносная инсайдерская угроза, т.е. когда работающий или бывший сотрудник, подрядчик или деловой партнер, который имеет или ранее имел авторизованный доступ к сети, системе или данным организации, намеренно превысил или неправильно использовал этот доступ таким образом, что это негативно повлияло на конфиденциальность, целостность или доступность информации организации или информации системы [9].

В современных условиях наличие инсайдерских угроз, формируемых в организациях различных форм собственности, является наиболее серьезной и актуальной проблемой.

В соответствии с представленной в табл. 1 методикой оценки инсайдерских угроз целе-

Таблица1

Пример оценки инсайдерских угроз в системе кадровой безопасности (разработка авторов)

Индексы	**Группы инсайдеров**			
	работники	**высвобожденные работники**	**деловые партнеры**	**другие пользователи**
	сотрудничают с организациями, не имеющими прямого отношения к компании: конкуренты компании или отдельные правительства стран («коллаборационисты»)	оказывают влияние независимо и злонамеренно, без внешнего воздействия или манипуляций («одинокие волки»)	партнеры или пользователи, которые считают, что на них не распространяется генерализация политики безопасности	сотрудники или сторонние пользователи, которые манипулируются для осуществления злонамеренных действий
Частные индексы инсайдерских угроз				
Индекс рисков раскрытия — $I_{(r)}$	конфиденциальная информация о клиентах	интеллектуальная собственность	финансовые ресурсы	параметры инсайдерских угроз
$I_{(r)}$ по отдельным факторам раскрытия	0,43	0,12	0,34	0, 296
Индекс доступа к компьютерным системам и данным компании – $I_{(d)}$	высокая степень доступа к компьютерным системам	средняя степень доступа к компьютерным системам	низкая степень доступа к компьютерным системам	
$I_{(d)}$ по отдельным факторам доступа	0,9	-	-	0,900
Индекс различия инсайдеров – $I_{(i)}$	уровень мотивации инсайдеров	осведомленность	уровень доступа и намерения	
$I_{(i)}$ по отдельным факторам различия	0,35	0,72	0,80	0,623
Интегральная оценка	Риск формирования инсайдерских угроз (RIU): <0,1 — очень низкий ≥ 0,1 и <0,4 — низкий ≥ 0,5 и <0,6 — средний ≥ 0,6 и <0,8 — выше среднего ≥ 0,8 и <1,0 — очень высокий			$\sqrt[3]{0,296 \cdot 0,9 \cdot 0,623} = 0,548$ (оценка: средний уровень инсайдерских угроз)

сообразно проводить такую оценку как минимум один раз в полугодие для различных групп инсайдеров: работников, ранее высвобожденного персонала, деловых партнеров и других пользователе.

Полученные результаты свидетельствуют о том, что в организации превалирует средний уровень инсайдерских угроз (54,8 %), влияющий на кадровую безопасность. Поэтому можно говорить об инсайдерских рисках

среднего размера, влияющих на кадровую безопасность, при которых организация может иметь устойчивую конкурентную позицию на основе партнерских отношений и, следовательно, среднюю надежность субъектов трудовых отношений и контрагентов.

Литература

1. *Ивашкина А.В.* Угрозы в кадровой безопасности и методы по их предотвращению / А.В. Ивашкина, У.П. Лебедева // Евразийский союз ученых. — 2018. — № 4–6 (49). — С. 71–77.
2. *Мешкова И.В.* Кадровая безопасность в системе национальной безопасности России // Миссия конфессий. — 2021. — Т. 10. — № 8(57). — С. 907–913.
3. *Молчанов М. А.* Кадровая безопасность как элемент экономической безопасности предприятий производственных отраслей // Мир современной науки. — 2014. — № 3(25). — С. 71–73.
4. Утечки данных в России. URL: https://www.tadviser.ru/index.php (дата обращения: 10.10.2022)
5. DWP Personnel Security Policy.– URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1050599/dwp-personnel-security-policy-version–2.pdf (дата обращения: 10.09.2022)
6. Ko, Li & Divakaran, Dinil Mon & Liau, Yung & Thing, Vrizlynn. (2016). Insider Threat Detection and its Future Directions. International Journal of Security and Networks. 12. 10.1504/IJSN.2017.10005217.
7. Koizumi, Hideaki. (2015). Engineering for Human Security and Well-Being. Engineering. 1. 282. 10.15302/J-ENG–2015066.
8. La identificación del sujeto-objeto de amenazas a la seguridad personal / Svetlana V. LOBOVA; Aleksei V. BOGOVIZ // Espacios. Vol. 39 (Number 24). Year 2018.Page 34. — URL: https://www.revistaespacios.com/a18v39n24/a18v39n24p34.pdf (дата обращения: 15.09.2022)
9. Mazzarolo, Guerrino & Jurcut, Anca. (2019). Insider threats in Cyber Security: The enemy within the gates.
10. Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization / Jawon Kim, Jaesoo Kim and Hangbae Chang. — DOI: 10.3390/su12156217 // Sustainability. — 2020. — 12, 6217.
11. Fan, Wenjun & Lwakatare, Kevin & Rong, Rong. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. International Journal of Computer Network and Information Security. 09. 1–11. 10.5815/ijcnis.2017.01.01.

ПРАВИТЕЛЬСТВОМ РФ ОПРЕДЕЛЕН ПОРЯДОК ОГРАНИЧЕНИЯ И ВОЗОБНОВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННОМ ИНФОРМАЦИОННОМ РЕСУРСЕ БУХГАЛТЕРСКОЙ (ФИНАНСОВОЙ) ОТЧЕТНОСТИ

Постановлением Правительства РФ предусмотрены случаи, при которых может быть ограничен доступ к информации, содержащейся в государственном информационном ресурсе бухгалтерской (финансовой) отчетности, в частности, если:

- организация включена в сводный реестр организаций оборонно-промышленного комплекса, предусмотренный постановлением Правительства РФ от 20 февраля 2004 г. № 96;
- организация включена в перечень стратегических предприятий и организаций, предусмотренный пунктом 2 статьи 190 Федерального закона «О несостоятельности (банкротстве)»;
- организация включена в перечень резидентов, предусмотренный частью 4.2 статьи 19 Федерального закона «О валютном регулировании и валютном контроле».

Утверждены Правила ограничения и возобновления доступа к информации, содержащейся в государственном информационном ресурсе бухгалтерской (финансовой) отчетности.

Признано утратившим силу постановление Правительства РФ от 22 января 2020 г. № 35 «Об освобождении организаций от представления обязательного экземпляра бухгалтерской (финансовой) отчетности в государственный информационный ресурс бухгалтерской (финансовой) отчетности».

Постановление вступает в силу с 1 января 2023 г.

https://sroaas.ru/pc/novosti/pravitelstvom-rf-opredelen-poryadok-ogranicheniya-i-vozobnovleniya-dostupa-k-informatsii-soderzhashch/
26 сентября 2022