КАДРОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Санникова Анастасия Андреевна, Махмудова Ирина Николаевна

Самарский национальный исследовательский университет имени академика С.П. Королёва, г. Самара

Аннотация. В статье рассматриваются реальные и потенциальные угрозы безопасности организации, которые возникают вследствие неграмотной работы с персоналом. В результате формируются, так называемые, «чёрные лебеди» или ситуации, способные вывести организацию из состояния равновесия. Раскрыты виды кадровых угроз в сфере информационных ресурсов организации. Выявлены причины утечки информации и методы нейтрализации угроз.

Ключевые слова: кадровые угрозы, утечка информации, безопасность организации, коммерческая тайна, убытки.

Мировая статистика годами демонстрирует увеличение количества случаев утечки данных в организациях. Одной из причин, создающей возможность появления кадровой угрозы является диджитализация экономики и переход на новый уровень понимания ценности цифровых технологий, ресурсов и знаний. С одной стороны, информатизация способствует эффективному ведению бизнеса и обеспечивает конкурентоспособность компаний, корпораций и государства в целом. С другой стороны, всегда остается риск безвозвратной потери данных, если оборудование выйдет из строя, при несанкционированных действиях самого персонала или хакерских атаках.

По типу реализации утечку информации можно разделить на два вида: физическая и информационная. *Информационные каналы* наиболее подвержены утечке информации, как по объему, так и по потенциальной возможности, в сравнении с *физическими каналами*. Вместе с тем, бывает так, что даже небольшая по объему потеря информации, но важная и секретная, может принести предприятию гораздо больше вреда, чем потеря нескольких гигабайтов персональных данных.

Наиболее распространенный *физический канал утечки информации* связан с классическим документооборотом — обменом документами внутри организации, с клиентами и поставщиками услуг и товаров, а также архивным хранением.

Причины утечки информации [1]:

– в результате перехвата документа после его печати (например, когда принтер вышестоящего руководства находится в общем офисном пространстве),

– вследствие несвоевременного уничтожения документов (если компания не проводит соответствующего обучения сотрудников и экономит на шредерах),

– свободного доступа к шкафам с архивными документами (отсутствие сейфов),

– некорректного переноса и уничтожения документов при переездах или реорганизации компаний и т. п.

Для того, чтобы предотвратить утечки информации путем выноса оборудования, компании требуется позаботиться об организации безопасного физического периметра, охране доступа в серверные помещения и на объекты, в которых размещаются резервные копии данных и электронных архивов.

Потере информации способствует и *объединение сотрудников в одном помещении*. Компактное размещение или использование стеклянных (прозрачных) перегородок между рабочими местами персонала служит драйвером риска утечки информации по визуальному и акустическому каналам.

Для защиты информации необходимо обеспечить конфиденциальность работы ключевых сотрудников (отдельные кабинеты, отсутствие людей «за спиной») и изоляцию помещений для переговоров.

«Утечка данных» с информационных каналов в большинстве случаев происходит по неосторожности или незнанию сотрудниками соответствующих регламентов и инструкций, определяющих правила пользования информационными ресурсами, а также неосведомленность о положениях, определяющих порядок действий для обеспечения безопасности компании. Сотрудники организации должны быть *проинформированы о недопустимости ведения некоторых типов переговоров вне защищенных зон*, например, в столовых или кафе [2].

Довольно часто сотрудники переходят на непроверенные сайты, теряют мобильные устройства, носители информации, оставляя их без своего контроля, защищают электронные данные простыми паролями, используют служебную почту для личных целей. Несанкционированно они переносят информацию с бумажного носителя на электронный носитель или работают с домашнего компьютера, не защищенного от внешнего воздействия различных хакерских программ.

Когда сотрудник незаконно ознакомился или незаконно использовал информацию, которая составляет коммерческую тайну, по закону он

обязан возместить работодателю убытки, которые понесла или может понести компания, в связи с этим. В данном случае под *убытками* понимаются [3]:

– расходы, которые компания, чье право нарушено, может произвести за повреждение (восстановление) файлов или оплату за нарушение прав.

– потерянные доходы, которые эта компания получила бы при обычных условиях, если бы ее право не было нарушено.

Та же самая обязанность – возместить ущерб – возлагается на сотрудников, которые нарушили подписанный ими документ о неразглашении конфиденциальной информации или коммерческой тайны.

Кроме того, обязанность возмещения ущерба лежит и на контрагентах, сделавших это вопреки гражданско-правовому договору. Пострадавшая сторона имеет право требовать возмещения, как реального ущерба, так и упущенной выгоды [3].

Таким образом, нетрудно заметить, что угрозу безопасности организации создаёт персонал.

Причиной негативных последствий поведения работников становится либо бесконтрольное отношение руководства организации к поведению своих сотрудников, либо их слабая работа по информированию персонала о потенциально возможных угрозах, которые могут возникнуть по причине необдуманного поведения. В этом ответственность лежит на руководителях.

С другой стороны, ответственность ложится и на плечи подчиненных, поскольку сознательно или неосознанно они нарушают предписанные правила и корпоративные нормы поведения, что приводит к угрозе безопасности компании.

Кадровая угроза со стороны надежности работника

Какие еще кадровые угрозы ожидают работодателей со стороны собственного персонала? Принимая на работу сотрудника, каждый руководитель должен быть уверен в его надежности. Это, прежде всего, связано с обеспечением безопасности компании и коллектива в целом. Выделим дополнительные источники для определения категорий рисков [4]:

1. *Риски, возникающие при формировании кадровой структуры*. На это может повлиять несоответствие качественного или количественного состава персонала, неэффективность процедуры подбора сотрудников, проблемы при адаптации, большая текучесть кадров.

2. *Риски могут появиться в процессе использования человеческих ресурсов*. К ним относятся низкая производительность труда, неэффективность использования рабочего времени, неисполнение установленных должностных функций, нарушение трудовой дисциплины, нанесе-

ние вреда имуществу предприятия, мошенничество, излишние траты, злоупотребления персонала.

3. *Риски, проявляющиеся в процессе формирования кадрового резерва*. Среди них можно отметить неэффективность обучения, недооценку творческого потенциала сотрудников, ошибки управления деловой карьерой, низкую мотивацию персонала, неэффективную работу с кадровым резервом или её отсутствие как таковой.

4. *Риски возникают на этапе увольнения персонала.* Это связано с судебными разбирательствами; увольнения в результате утечки конфиденциальной информации; в связи с демонстрацией конфликтного / рискогенного поведения в коллективе; как последствие от действий или бездействия, способствующего подрыву репутации фирмы.

Каждая из указанных выше категорий прямо или косвенно связана с проблемой надежности работника.

В первой категории рисков большое значение имеет оценка *корпоративной лояльности и психологической надежности сотрудника* в процессе подбора на ту или иную должность в организации.

Важным фактором надежности является *психологическая устойчивость* и, в целом, позитивные качества характера сотрудника, способность быстро реагировать на изменения в профессиональной среде.

Во второй категории рисков значение имеют вопросы *профессиональной надежности*, отражением чего является эффективность деятельности и использование актуальных (потенциальных) психологических качеств работника. Сотрудник должен уважительно относиться не только к своим коллегам и руководителю, но и к своей собственной деятельности.

В третьей категории рисков отражается проблема *надежности кадрового резерва*. Под кадровым резервом понимается группа сотрудников, потенциально способствующих выполнению какой-либо деятельности помимо их данных обязанностей.

В четвертой группе рискогенных факторов рассматривается вопрос надежности персонала с точки зрения *прогнозирования репутационных последствий для организации*. Из-за неправильного поведения сотрудника компания может понести значимые убытки. Например: если сотрудник неуважительно общался с клиентом и тот остался недоволен, в результате чего на страничках интернета был оставлен негативный отзыв с подробным объяснением, а пользователи прочитали и поддержали. Более того, они стали распространять информацию. В результате – компания теряет клиентов, акции компании падают. У потенциальных клиентов складывается опасение, что компания начала хуже работать, и ком-

пания действительно начинает хуже работать и терять деньги [5]. Такая цепочка может сложиться из-за некомпетентности персонала организации или пренебрежительного отношения к клиентам.

Шантаж сотрудника.

Каждый рабочий день несет определенный набор функций и обязанностей, которые необходимо выполнять коллективу в организации. Но далеко не все могут справиться с возлагаемыми на них объемами работ. Человек индивидуален и обладает разной эффективностью выполнения задач. Если сотруднику не под силу выполнять тот объем работ, который ему определил руководитель, то рано или поздно уровень работоспособности работника снижается, и он начинает проявляться свои слабые стороны, поскольку восстановиться не успевает.

В последнее время сотрудники в силу тех или иных обстоятельств применяют в сторону руководства агрессивные инструменты воздействия: грозят жалобами в трудовую инспекцию, прокуратуру или разглашением коммерческой тайны. Как же правильно работодателю реагировать на подобные способы шантажа, ведь это может все больше и больше появляться в организации.

Способы шантажа со стороны работника [6]:

1. «Неповторимый работник».

Работники, которые занимают ключевые позиции в организации, могут продвигать политику собственной незаменимости, угрожать работодателю распространением секретной информации. Если все сотрудники будут согласны с мнение провокатора, то значит в компании плохо построен рабочий процесс. *«Неповторимый работник» очень опасен для организации*. Ведь сотрудник может не только уволиться, но и заболеть, уйти в отпуск и т.п. Руководитель повышает риски, когда ставит ставки на одного специалиста.

Для того, чтобы устранить проблему такого типа, следует распределить обязанности между другими работниками, на тот случай, если «неповторимый сотрудник» решить уволиться или уйти в отпуск.

2. Черная/серая зарплата.

Сотрудник, *получая зарплату в конверте, может угрожать руководителю* тем, что все расскажет налоговой или трудовой инспекции. Подобного шантажа работодателю не стоит бояться. *Трудовую инспекцию интересует жалобы о зарплате в конверте целой группы* сотрудников, а не одного человека. Тем более, доказать факт получения черной зарплаты достаточно сложно, т.к. данные выплаты организация тщательно скрывает. Нужно иметь на руках документы или инициировать следственный эксперимент с передачей меченых купюр, а это сделать совсем не легко.

Вдобавок ко всему сотруднику стоит учесть, что такие меры шантажа стоит использовать только при увольнении, т.к. дальнейшая работа с руководителем после подобного конфликта будет невозможна. В основном данный способ используют увольняющиеся сотрудники, чтобы добиться полной выплаты, как белой, так и черной зарплаты.

3. Лжесотрудники.

Иногда, *сотрудники сами плетут интриги* и собирают информацию о незаконных сделках организации, тем самым шантажируя работодателя. Но если фирма соблюдает законам и правила, то шантажиста можно передать в руки правосудия. Для этого необходимо подготовить подтверждения о данной деятельности и обратиться в надзорные органы. Согласно ст. 163 «Вымогательство» Уголовного кодекса *нарушитель может получить тюремный срок* до 4 лет. Есть и менее жесткие варианты решения проблемы, когда шантажист приговаривается к принудительным работам от 2 до 4 лет с ограничением свободы.

Также законом предусматривается наказание в виде ареста на 6 месяцев. В этом случае шантажисту требуется выплатить штраф, исчисляющийся размером прежней зарплаты и других доходов осужденного, которые были получены им за период до 6 месяцев, предшествующих совершению злодеяния.

В любом случае шантаж руководителя недопустим в организации. Работодателю нужно уметь правильно выходить из данных ситуаций, чтобы не допустить слив конфиденциальной информации, сохранить собственную репутацию и репутацию фирмы, удержать ценных сотрудников.

Вербовка персонала.

Бывают ситуации, когда работник начинает ненавидеть свое начальство, в том числе и собственную деятельность. Озлобленный сотрудник готов либо уволиться, либо сделать для компании любую гадость, лишь бы отомстить или защитить самого себя. В современном мире появилась такая разновидность шпионажа, как вербовка сотрудника. *Вербовка* — это комплекс разнообразных методов воздействия на сотрудника организации с целью получения какой-либо информации или достижения какой-либо цели.

Специально обученные люди мониторят социальные сети, собирают информацию из других источников о сотрудниках компании (какие места часто посещают, чем увлекаются, слабые и сильные стороны человека), и если находят людей с девиантным (отклоняющимся) поведением, или обиженных на своего работодателя, то встречаются и пытаются их завербовать. Вербовщики предлагают человеку деньги за выполненные условия, либо используют шантаж, если есть за что зацепиться. По-

сле того, как сотрудник соглашается иметь дело с вербовщиками, то они начинают действовать вместе.

Сотруднику предлагают:

– подать заявление в суд на работодателя;

– создать чат для коллег с целью дискредитации руководящего состава фирмы;

– разместить в интернете негативные отзывы о компании;

– слить конфиденциальную информацию из компании, в которой он работает;

– подставить руководителя и т.п.

Целью вербовщика может являться:

– ухудшение климата в компании;

– переманивание сотрудника в другую организацию;

– смещение руководителя с поста;

– получение секретной информации;

– удаление конкурентов с рынка и т.п.

После того, как вербовщик добивается своих целей, он незаметно исчезает и ищет следующую «жертву» [7].

В бизнесе в наше время достаточно часто можно заметить использование такого типа шпионажа, т.к. кадровая безопасность в организациях усиливается, а методы сохранения информации ужесточаются.

Библиографический список

1. Михайлова А. Основные каналы утечки информации на предприятии. – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise (Дата обращения 13.12.2020).

2. Как выявлять закрепление злоумышленников в сети? – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise (Дата обращения 23.12.2020).

3. Как наказывать сотрудников, которые сливают информацию конкурентам. – [Электронный ресурс]. – Режим доступа: https://probusiness.io/law/6765-kak-nakazyvat-sotrudnikov-kotorye-slivayut-informaciyu-konkurentam.html (Дата обращения 23.12.2020).

4. Шипилов А.И. Как обеспечить надежность персонала? // Кадры предприятия. – №8. – Москва, 2004.

5. Борзунов А.А. К вопросу о сущности понятия «кадровый риск» // Экономика и современный менеджмент: теория и практика: сб. статей по материалам XL междунар. науч.-практ. конф. – Новосибирск: СибАК, 2014.

6. Шантаж на рабочем месте – чего следует ожидать и как поступить. – [Электронный ресурс]. – Режим доступа: https://expbiz.ru/biznes-stati/upravlenie-personalom/shantazh-na-rabochem-meste-chego-sleduet-ozhidat-i-kak-postupit.html (Дата обращения 23.12.2020).

7. Вербовка: альтернативный вариант подбора персонала. – [Электронный ресурс]. – Режим доступа: https://hr-portal.ru/print/94742 (Дата обращения 23.12.2020).

PERSONNEL SECURITY THREATS IN THE ORGANIZATION

Sannikova Anastasia Andreevna, Makhmudova Irina Nikolaevna

Samara national research University, Samara

Abstract. The article examines the real and potential threats to the security of the organization that arise as a result of illiterate work with the person. As a result, so-called "black swans" or situations are formed that can bring the organization out of balance. The types of personnel threats in the field of information resources of the organization are disclosed. The reasons of information leakage and methods of threat neutralization are revealed.

Keywords: personnel threats, information leaks, organization security, trade secrets, losses.

КАДРОВАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ: РИСКИ И ПОСЛЕДСТВИЯ

Карнаухова Ксения Юрьевна, Соловова Наталья Валентиновна

Самарский национальный исследовательский университет имени академика С.П. Королева

Аннотация. для эффективного функционирования компаний следует не только выстраивать и отлаживать кадровые процессы, но и рассматривать их с точки зрения обеспечения кадровой безопасности организации. Значительную угрозу для безопасности организации могут представлять ее сотрудники. При увольнении кадровые риски связаны именно с персоналом: нарушение конфиденциальности информации и ее хищение, неблагоприятный социально-психологический климат в коллективе, финансовые риски, ущерб деловой репутации компании, жало-