МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)

И.Н. МАХМУДОВА, Н.В. СОЛОВОВА

КАДРОВАЯ БЕЗОПАСНОСТЬ: ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ

Рекомендовано редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в качестве учебного пособия для обучающихся по основным образовательным программам высшего образования по направлениям подготовки 38.03.03, 38.04.03 Управление персоналом, 38.04.04 Государственное и муниципальное управление

САМАРА
Издательство Самарского университета
2022

УДК 347(075)
ББК 67.400.6я7
М364

Рецензенты: д-р экон. наук, проф. М.Н. Тюкавкин,
канд. экон. наук, доц. Ю.Н. Горбунова

Махмудова, Ирина Николаевна
М364 Кадровая безопасность: организация и управление : учебное пособие / *И.Н. Махмудова, Н.В. Соловова*. – Самара : Издательство Самарского университета, 2022. – 96 с. : с ил.

ISBN 978-5-7883-1755-7

Учебное пособие раскрывает актуальные аспекты организации и управления службы безопасности в организации. Содержание учебного пособия представлено в наглядной форме, удобной для освоения и структуризации теоретического знания. В рассмотренных материалах отражена концепция системы безопасности кадрового развития компании, политика и показатели её надёжности, раскрыты структура и функции управления службы кадровой безопасности, а также методы управления кадровыми рисками. Пособие включает практические упражнения для самостоятельной работы обучающихся, тестовые и кейс-задания.

Издание рекомендовано широкому кругу читателей – слушателям профильных программ бакалавриата и магистратуры, системы дополнительного образования и повышения квалификации, направлений подготовки 38.03.03, 38.04.03 Управление персоналом, 38.04.04 Государственное и муниципальное управление; специалистам в сфере кадровой безопасности и участникам бизнес-сообщества.

Подготовлено на кафедре управления человеческими ресурсами.

УДК 347(075)
ББК 67.400.6я7

ISBN 978-5-7883-1755-7

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Цифровая экономика уже внесла свои коррективы в деятельность современных предприятий. В деловой среде сложились новые конкурентные отношения в сфере рынков сбыта, финансов, человеческих и материальных ресурсов. Выживанию бизнеса угрожает неконтролируемое влияние внешней и внутренней среды. Согласно исследованию PwC, существует примерно равное количество случаев мошенничества, совершаемых внутренними и внешними преступниками (по 40% каждый) (PwC, 2020). Остальные преступления связаны в основном со сговором между ними.

Внешние риски определяются, прежде всего, тем, что:

– сфера конкурентных отношений чрезвычайно обостряется из-за внедрения новых цифровых технологий в деятельность современных предприятий, а значит, более рискованна;

– многие рыночные механизмы в области обеспечения экономической безопасности предприятий не работают, поскольку на предприятиях не сформирована целостная система мер безопасности, либо она действует фрагментарно. Хотя общие убытки от мошенничества (согласно исследованию PwC) за последние два года составили 42 млрд долларов США, только 56% компаний расследовали наихудший случай мошенничества (PwC, 2020);

– рынок деловой информации обеспечивает экономическую и кадровую безопасность организаций за счет конфиденциальности информации, которая не сформирована в достаточном объеме. Ни одно предприятие не готово поделиться секретами организации собственной службы безопасности, чтобы не подвергаться риску негативного воздействия извне.

Вопрос устранения кадровых угроз для обеспечения безопасности компании занимает центральное место в работе службы безопасности. Однако в оперативной практике оказывается, что большое количество кадровых угроз представлено большим разнообразием. Вот лишь некоторые данные. На долю сотрудников

приходится 62% утечек, а на подрядчиков – только 6%. Всего в прошлом году было зафиксировано 1556 случаев утечки данных от организаций по всему миру, что на 3,4% больше, чем в предыдущем году.

В 93% случаев утечки были связаны с кражей персональных данных и платежной информации. В 2020 году в связи с переводом компаний в удаленные районы Ростелеком зафиксировал 25% рост утечки персональных данных, что обостряет вопрос кадровой безопасности. Доля утечки коммерческой тайны составила 5,4%. Большая часть украденных персональных данных (94,6%) составила 44 «мега-утечки», в результате которых злоумышленникам стало доступно не менее 10 миллионов таких записей (Генеральный директор, 2017).

Многие кадровые угрозы связаны с использованием информационных технологий. В современном мире широко обсуждается проблема кибертерроризма и кибератак на предприятия. Киберпреступники наиболее активны в следующих областях кибератак: вредоносное ПО, веб-атаки, фишинг, атаки на веб-приложения, спам, DDoS-атаки, кража личных данных, нарушения безопасности данных, внутренние угрозы, ботнеты, физические манипуляции, утечки информации, вирусы-вымогатели, кибершпионаж, криптоджекинг (вредоносный майнинг) (McKinsey, 2020). Их скорость, масштабы и широта охвата секторов экономики впечатляют. Вот немного статистики. Хакеры пытались украсть информацию: в 30% атак они похищали личные данные, в 24% – учётные данные, в 14% – платёжную информацию. Уязвимости в сфере безопасности человеческих ресурсов связаны с масштабами распространения и растущей поверхностью кибератак. Сложность заключается в локализации данного географического пространства. Существует также организационная сложность противодействия этим атакам, поскольку источники кибератак децентрализованы, а сеть представлена широкой кибер-инфраструктурой. Согласно исследованию PwC, общее количество инцидентов информационной безопасности растет в среднем на 48% ежегодно (42,3 миллиона инцидентов означают, что в среднем ежедневно совершается 117 339 кибератак).

С ростом кибертерроризма стоимость защиты от киберугроз для бизнеса возрастает. В России 22% «руководителей» компаний,

затронутых этой проблемой, отметили, что понесенные убытки превысили 1 млн. долларов, что немного выше, чем в среднем по миру (19%). При этом 41% респондентов в нашей стране сообщили, что убыток не превышает 100 000 долларов (по всему миру 45% респондентов назвали такой же ущерб) (Bailey et al., 2020).

При этом для нейтрализации кадровых угроз полномочий и компетенции сотрудников службы безопасности организации явно недостаточно. В связи с этим необходимо рассматривать не отдельные меры, а комплекс действий, обеспечивающих целостную и эффективную систему безопасности.

В профиле факторов риска любой организации кадровые риски составляют значительную часть. Поэтому, прежде чем говорить об экономической безопасности организации в целом, необходимо тщательно выстроить систему кадровой безопасности.

Кроме того, поскольку каждой организации важно занять достойное место в конкурентной среде по отношению к другим организациям, то одним из самых дорогих и трудных для обеспечения преимуществ организации является ее интеллектуальный капитал и защита интеллектуальной собственности. Интеллектуальный капитал может многократно увеличивать рыночную стоимость самой организации, а значит, организация становится достаточно привлекательной для инвесторов. К тому же, интеллектуальный капитал организации является потенциальной целью для привлечения внимания со стороны как конкурентной разведки, так и промышленного шпионажа, и других методов недобросовестной конкуренции. Известны случаи кражи запатентованного продукта и использования его в личных целях с целью получения прибыли. Такой пример привел Костанянц, профессор кафедры управления фирмой Высшей школы корпоративного управления РАНХиГС: в российскую компанию был приглашен менеджер для разработки запатентованного продукта. Он украл компьютерные коды компании, уехал в США, где зарегистрировал свою компанию, а затем начал продвигать модифицированный продукт на российском рынке. В результате он был осужден по ст. 147 УК РФ за незаконное использование патентных прав (Толстоухова, 2018).

Само понятие «кадровая безопасность» двояко по своему содержанию. С одной стороны, она направлена на защиту прав сотрудников от противоправных действий работодателя, наносящих

им серьезный вред. Со стороны работодателя по-прежнему наблюдаются такие нарушения, как: задержка выплаты заработной платы; замена трудовых договоров гражданско-правовыми при приеме на работу граждан; нарушение режима труда и отдыха сотрудников (например, непредставление заслуженного отпуска или, наоборот, отправка работника в вынужденный (неоплачиваемый) отпуск); незаконное увольнение и многое другое.

С другой стороны, безопасность персонала включает защиту организации от несанкционированных действий или бездействия ее персонала. К ним относятся: кража, регистрация, сговор с конкурирующими сторонами, подлог, повреждение собственности работодателя, кража, разглашение конфиденциальной информации и многое другое.

Как видно, вопрос о создании в организации службы безопасности отнюдь не праздный. Это многоаспектная и многоуровневая деятельность, которая требует грамотной организации процессов и профессионального управления.

Вопросы организации системы и служб управления кадровой безопасностью и управления кадровыми рисками, потенциально или реально возникающими в работе конкретных предприятий, подробно освещены в рамках настоящего учебного пособия.

Структура содержания выстроена таким образом, чтобы подробно раскрыть все основные элементы системы кадровой безопасности, которые состоят из научной теории безопасности, политики и стратегии безопасности, средств и методов обеспечения безопасности, а также самой концепции безопасности предприятия.

Раскрыты особенности организации службы безопасности, её структурные элементы, а также субъект-объектные отношения безопасности в рамках её социально-трудового взаимодействия с другими структурными подразделениями организации. Разграничены особые функции и полномочия службы кадровой безопасности.

Учебное пособие предназначено для широкого круга читателей, на профессиональном уровне интересующихся вопросами кадровой безопасности в организации, обучающихся по направлениям 38.03.03, 38.04.03 Управление персоналом, 38.04.04 Государственное и муниципальное управление; специалистам в сфере кад-

ровой безопасности и участникам бизнес-сообщества. В пособие включены практические задания для закрепления материала и контроля полученных знаний, а также практические и ситуационные кейс-задания, позволяющие более глубоко исследовать реальные кадровые проблемы на рабочих местах.

Авторы желают всем успешного продвижения в изучении данного курса.

1. КОНЦЕПЦИЯ БЕЗОПАСНОСТИ КАДРОВОГО РАЗВИТИЯ КОМПАНИИ

1.1. Система безопасности предприятия, её элементы

Созданию службы безопасности обычно предшествуют два события:

1. Как реакция на внезапно возникшие реальные угрозы имуществу, физической расправы с персоналом и т.д.

2. Неудовлетворительное состояние безопасности предприятия.

В первом случае – служба безопасности:

- создаётся поспешно;
- способна лишь в некоторой степени отразить угрозы;
- способна в дальнейшем реагировать на появление кадровых угроз.

Таким образом реализуется принцип работы: «угроза – отражение». Понятно, что такая работа службы безопасности аварийная и не всегда способна вовремя, либо качественно отразить уже наступившее негативное событие. Остаётся риск рецидива преступлений, причём частота повторения кадровых угроз может нарастать.

Во втором случае, при неудовлетворительном состоянии безопасности предприятия проводится детальное изучение ситуации, чаще всего с привлечением сторонних специалистов, поскольку своих безопасников на предприятии не оказалось. В результате – формируется «реальное представление» о системе безопасности предприятия. И уже предпринимаются необходимые меры по выравниванию/оздоровлению ситуации на местах.

В качестве нормативно-правовой базы регулирования кадровых угроз на предприятии существует ряд законодательных норм, отраженных в федеральных законах. Приведём лишь некоторые из них:

– Указ Президента РФ № 361 «О борьбе с коррупцией в системе государственной службы».

– Федеральный закон РФ № 2446-1 «О безопасности».

– Федеральный закон «Об информации, информационных технологиях и защите информации».

– Закон РФ «О частной детективной и охранной деятельности в РФ».

– Федеральный закон РФ № 98-ФЗ «О коммерческой тайне».

– Федеральный закон РФ № 122-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам».

– Федеральный закон РФ № 230-ФЗ «О профессиональных стандартах».

– Федеральный закон РФ № 273-ФЗ «О противодействии коррупции».

– Федеральный закон РФ № 238-ФЗ «О независимой оценке компетенций».

– Федеральный закон РФ № 152-ФЗ «О персональных данных».

– Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Гражданский кодекс РФ №51-ФЗ (с изм. и доп.).

– Уголовный кодекс РФ № 63-ФЗ (с изм. и доп.).

Благодаря этим законам можно раскрыть сущность *безопасности*, в том числе, *кадровой*, описать элементы системы кадровой безопасности. Термин «*безопасность*» определяется в ст. 1 ФЗ «О безопасности» от 5 марта 1992 года как «*состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз*».

Сущность безопасности напрямую связана с понятием «развитие» и «устойчивость». *Безопасность* – это способность к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов.

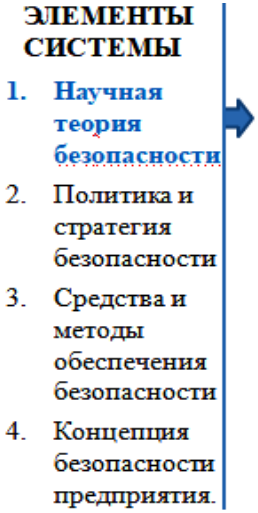
Исходя из данного определения, становятся понятными и *функции безопасности*, а именно: выявление, предупреждение, снижение, ослабление, нейтрализация, пресечение, локализация, отражение и устранение угроз.

Система безопасности организации – это комплекс организационно-управленческих, экономически-правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и ее персонала.

Вся *система кадровой безопасности* представлена четырьмя элементами. В неё входит:

1. Научная теория безопасности.
2. Политика и стратегия безопасности.
3. Средства и методы обеспечения безопасности.
4. Концепция безопасности предприятия.

Раскроем эти элементы.



Научная теория безопасности

Ни одна, даже хорошо развитая и стабильно действующая организация, не застрахована от неожиданностей, способных привести к серьёзным негативным последствиям. Такие события способны внести хаос в работу и дестабилизировать налаженные процессы в управлении персоналом, создать угрозу кадровой безопасности в организации. С точки зрения безопасности предприятия, *угроза* – это потенциальное или реально возможное событие, действие, процесс или явление, которое способно нарушить устойчивость и развитие компании и/или привести к остановке его деятельности.

Кадровых угроз для предприятия большое множество. Угрозы кадровой безопасности негативно сказываются на деятельности организаций.

Кадровая безопасность включает в себя широкий спектр угроз. По направленности воздействия различают угрозы, при ко-

торых объектом кадровой безопасности может выступать как сама организация, так и её персонал.

Со стороны организации угрозой может стать, например, незаконное увольнение сотрудника, либо перевод его на другую должность без согласия работника. В таких случаях приходится защищать права работника с привлечением третьей стороны. Нередко дело доходит до суда.

Вместе с тем и сам персонал часто грешит незаконными действиями, которые способны нанести серьезный ущерб организации. В данном случае речь идет о несанкционированном разглашении конфиденциальной информации, о приписках в финансовых документах, об использовании своего положения в должности для выполнения незаконных сделок. Отдельные сотрудники подвергаются психологическим манипуляциям и вербовке со стороны третьих лиц. В результате, они оказываются втянутыми в такие социально-трудовые отношения, где есть место не только неприятным случайностям (ошибкам), но также преднамеренным злостным нарушениям. И если ошибочные действия можно списать на некомпетентность работников, чрезмерную доверчивость или даже на недобросовестность, то подлоги, «слив» информации, использование в корыстных целях или добыча незаконными методами конфиденциальной информации – все это свидетельствует о целенаправленном подрыве устоев организации, возникновении кадровых угроз для экономической безопасности организации.

Термином «*риск*», как правило, характеризуют возможность возникновения нештатной ситуации или неблагоприятных последствий какого-либо события. Рисковые ситуации формируют уязвимость работника и коллектива, создают *кадровые угрозы* в организациях.

Ситуации риска отличаются некоторыми особенностями. Прежде всего, это связано с неопределенностью момента возникновения риска, характером и последствиями развития нештатной ситуации, а также с дефицитом времени и недостаточностью поступающей информации, определяющих последующее функциональное поведение работника, оказавшегося в данной ситуации.

Психологи рассматривают *риск как «сознательно-волевую деятельность субъекта, связанную с преодолением неопределенно-*

сти в ситуации неизбежного выбора из нескольких альтернатив, в процессе которого есть возможность определить вероятность достижения поставленной цели» [А.П. Альгин, 1989; 1990]. То есть, ситуация кадрового риска формирует у работника активное восприятие действительности. В этом случае личный опыт и психологическая готовность конкретного работника в разрешении чрезвычайной и/или нестандартной ситуации формируют уникальную модель поведения. Это объясняет, почему в идентичных ситуациях каждый сотрудник поступает особым для него образом. Почему один работник способен и готов идти на сговор, преступление, способствовать разглашению конфиденциальной информации и коммерческой тайны, заниматься промышленным шпионажем и прочими неблаговидными и преступными действиями, а другой – нет [И.Н. Махмудова, 2020]. Таким образом, речь идет не о мотивационном факторе, как это принято считать в научной литературе, а о сформированном шаблоне мышления и поведения, если оно являлось положительным опытом в жизни конкретного человека.

Именно поэтому важно всячески обеспечивать контроль ситуации и не допускать возможности совершения неблаговидного выбора сотрудника, оказавшегося в нестандартной ситуации. Для этого параллельно с мерами контроля необходимо проводить профилактическое информирование персонала о возможностях и последующих угрозах как для самого работника, так и для организации, в случае нарушения кодекса и норм корпоративной этики, правил поведения в организации. Потребуется отрабатывать некоторые оперативные действия, чтобы избежать наступления нештатной ситуации.

Важным источником угроз является недостаток информации, спонтанные (неожиданные, бесконтрольные) действия других субъектов и уникальность самой ситуации.

В.А. Петровский в своих исследованиях надситуативной активности выявил *два основных типа риска*: мотивированный и немотивированный. Он связывает *мотивированный риск* с *расчетом шансов на успех* [Петровский В.А., 1992]. Это значит, что человек в ситуации выбора склонен идти на сближение с опасностью ради реализации наиболее предпочтительных (для себя или для конкретной специфичной ситуации, определяемой обстоя-

тельствами жизни человека) целей и достижения желаемых результатов. Иногда такую форму риска называют оправданной. Эту идею подтверждают исследования зарубежных и российских социальных психологов [Кленова М.А., 2010]. Однако, наряду с данной формой существует и другая, особая форма риска – «*риск ради риска*». Такая ситуация сближения с опасностью не имеет какой-либо внешней необходимости, а выполняется ради испытания остроты ощущений. Она не просто не оправданна, но и опасна для организации с точки зрения формирования кадровых угроз. Ситуация бесконтрольна, выполняется на уровне осознанного выбора работника, который получает эмоциональное наслаждение. А это, как известно, самые стойкие эмоции, которые человек стремится раз за разом возобновлять. Это и есть *мотивированный риск*.

Данный выбор позволяет максимально реализовать скрытые потенциальные человеческие возможности. Просчитать их заблаговременно не представляется никакой возможности. Можно лишь локализовать данные потенциальные угрозы системой профилактических мероприятий, повышающих *лояльность персонала организации* и формирующих *эмоциональную устойчивость личности*. В качестве мероприятий этому могут способствовать методы, повышающие самооценку личности и уровень его самоконтроля.

1.2. Классификация угроз безопасности

Кадровые угрозы можно классифицировать по разным основаниям:

По степени вероятности – невероятные, маловероятные, вероятные, весьма вероятные, вполне вероятные.

По степени удалённости – непосредственные, близкие (до 1 года), далёкие (свыше 1 года).

По степени развития – выделяют этап возникновения, экспансии, стабилизации и ликвидации.

По степени отдалённости угрозы в пространстве – это территория предприятия, прилегающая к предприятию территория, территория региона, страны, зарубежная территория.

По темпам нарастания – угрозы измеряются по месяцам, кварталам и годам.

По напряжённости – угрозы подразделяются на две группы:

а) нормальные, повышенные, близкие к пределу (порогу), избыточные;

б) определяют рост, стабильность или снижение.

По природе возникновения – бывают:

а) естественные/объективные, т.е. вызванные стихийными природными явлениями, не зависящими от человека, например, в результате наводнений, землетрясений, ураганов и проч.;

б) искусственные/субъективные, т.е. вызванные деятельностью человека, непреднамеренные/неумышленные и преднамеренные/умышленные угрозы.

Приведём пример намеренного создания кадровой угрозы на предприятии. В современной практике кадровую угрозу безопасности организации может создать, например, неумелое использование персоналом информационно-технических средств и специального оборудования, подвергающееся хакерским атакам, взлому криптоключей и запуском шпионских программ и вредоносных ПО. Такие действия извне отличаются своей непредсказуемостью и масштабностью урона для организации. В настоящее время появился новый термин – «*кибертерроризм*», с которым ведётся целенаправленная борьба во всем мире. Однако, пока безрезультатно. Кибертерроризм (это даже не хакерские атаки) вынуждает организации увеличивать финансовые вливания в создание защитных барьеров. С этой целью закупается дорогостоящее оборудование, вкладываются средства в закупку и установку новейших программных пакетов для отражения вирусных атак, в наём и обучение собственного персонала работе со специальными программами. Но реальность такова, что злоумышленники пока идут на шаг впереди, втягивая организации в процесс саморазрушения, в незапланированные финансовые расходы.

Также выделяют различные *виды угроз*: экономические, информационные, социальные, экологические, правовые, технические, организационные и криминальные.

Постановка проблемы формирования кадровых угроз и рисков в организации.

Самоконтроль часто идентифицируют как *стрессоустойчивость*. Однако, это не совсем правильно. Самоконтроль позволяет успешно действовать в условиях риска, достигать положительного результата *с учетом приоритета правил, требований, взятых на себя обязательств и специфики самой ситуации*. Это навязанная, натренированная, внешняя эмоциональная устойчивость, *внешний локус-контроль*.

Стрессоустойчивость, в большей степени, раскрывает *специфику физиологии человека, его способность переносить повышенные нагрузки на нервную систему*. Соответственно, это внутренняя эмоциональная устойчивость или *внутренний локус-контроль*.

Результаты научных исследований свидетельствуют о том, что у лиц с внутренним локусом контроля лучше развито умение использовать информацию в неопределенной ситуации, чем у лиц с внешним локусом контролем [Кочетков В.В., Скотникова И.Г., 1993; Рапохин Н.П., 1981]. Описанные выше исследования позволяют объяснить возникновение проблемной ситуации в области *формирования кадровых угроз, а также* способствуют постановке задачи об оценке вероятности наступления возможных рисков в организации. Кроме того, важно определить не просто готовность к риску специалистов службы безопасности, но и *соответствие специалиста своей должности.*

Готовность к риску специалистов службы безопасности (методы).

Благосклонность к рисковому поведению, как мы выяснили, определяется *ситуационными, мотивационными и личностными факторами,* а также *субъективным отношением человека*. Однако, неопределенность возникновения рискованной проблемной ситуации диктует необходимость предоставить некие гарантии, что специалисты службы безопасности готовы демонстрировать способность принимать качественные управленческие решения и транслировать адекватное ситуации поведение для локализации и нейтрализации угроз в организации.

Готовность к риску обычно сопровождается низкой мотивацией к избеганию неудач, и прямо пропорциональна числу допущенных ошибок.

Кроме того, интересными представляются результаты психологических исследований, которые зафиксировали тенденцию

снижения *готовности к риску* в соответствии с увеличением возраста и опыта специалистов. То есть, наиболее опытные работники менее готовы к риску, чем молодые сотрудники [Кленова М.А., 2010]. Для диагностики личности на мотивацию к избеганию неудач, а также для оценки зависимости уровня готовности специалиста к риску от его возраста, можно использовать следующие инструменты анализа:

– методику Т. Элерса в сочетании с диагностикой степени готовности к риску по методике А.М. Шуберта;

– опросник «Ценностные ориентации» М. Рокича;

– тест-опросник Н. Когана и М. Уоллаха;

– факторный анализ по различиям средних величин, определяемых с помощью t-критерия Стьюдента.

Чтобы минимизировать вероятность наступления опасных событий и сократить случаи угроз кадровой безопасности, необходимо вовремя диагностировать потенциально опасные ситуации, регламентировать порядок оперативных мероприятий по выходу из опасных ситуаций.

1.3. Цели, задачи и принципы построения системы безопасности

Под объектом безопасности предприятия понимают:

– степень устойчивости и развития предприятия;

– его способность противостоять угрозам.

В объекте безопасности предприятия можно выделить:

– различные *структурные подразделения* или *группы сотрудников* либо владельцы акций предприятия;

– ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые);

– различные виды деятельности (управленческая, производственная, снабженческая и т.д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, поз-

воляющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Цель определяет насущные *задачи* её достижения*:*

- выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию;
- обеспечение защиты технологических процессов;
- реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т.д.);
- своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;
- предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
- всестороннее изучение деловых партнеров;
- своевременное выявление и адекватное реагирование на дезинформационные мероприятия;
- разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;
- реализация мер по защите коммерческой и иной информации;
- организация мероприятий по противодействию недобросовестной конкуренции;
- реализация мер по защите интеллектуальной собственности;
- организация и проведение мер по предотвращению чрезвычайных ситуаций;
- выявление негативных тенденций среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;
- организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;
- разработка и реализация мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

– возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц, обеспечение защиты всех видов ресурсов предприятия.

В рамках научной теории необходимо обозначит принципы построения системы безопасности предприятия. *Принципы* – это правила, которым нужно неукоснительно следовать или соблюдать. Выделяют следующие принципы:

1. *Приоритет мер предупреждения* – своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

2. *Принцип законности* – меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

3. *Комплексное использование сил и средств* – для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

4. *Координация и взаимодействие внутри и вне предприятия* – осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа, совет и т.д.) безопасности предприятия.

5. *Сочетание гласности с конспирацией***.** Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль – предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6. *Компетентность*. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

7. *Плановая основа деятельности* – деятельность на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

8. *Принцип системности* – означает учёт всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

9. *Принцип экономической целесообразности*. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

ВОПРОСЫ И ЗАДАНИЯ

1. Вопросы для обсуждения

1. Почему угрозы информационной безопасности со стороны собственного персонала представляют для работодателя большую опасность, чем угрозы имущественной безопасности?

2. Почему угроза разглашения сотрудником конфиденциальной информации о клиентах организации представляет для нее большую угрозу, нежели разглашение иной конфиденциальной информации?

3. Какими средствами располагает государство для повышения степени защищенности работодателей от угроз по кадровому направлению их деятельности?

4. Как работодатель должен учитывать особенности национальной трудовой ментальности россиян при обеспечении безопасности по кадровому направлению деятельности организации?

5. Какие требования доктрины «развития человеческого капитала организации» имеют прямое отношение к проблеме обеспечении безопасности по кадровому направлению ее деятельности?

6. Раскройте политику и стратегию безопасности.

7. Кто является субъектом безопасности предприятия?

8. Что понимается под объектом безопасности?

9. Каковы средства и методы обеспечения безопасности?

10. В чём суть концепции безопасности предприятия?

11. Что понимается под угрозой безопасности? Какова классификация угроз?

2. Напишите эссе

1. «Человеческий фактор» в системе обеспечения безопасности современной организации.

2. Влияние трудовой ментальности россиян на проблему обеспечения безопасности организации.

3. Влияние философии предпринимательства на проблему обеспечения безопасности организации.

4. Конкуренция и проблема обеспечения кадровой безопасности современной организации.

5. Отраслевая специфика обеспечения безопасности по кадровому направлению деятельности в организациях, представляющих:

- реальный сектор экономики;
- военно-промышленный комплекс;
- финансовый сектор экономики;
- торговли и бытового обслуживания;
- сферу науки и научного обслуживания;
- в органах государственного управления.

3. Выполните тестовое задание

1. Обеспечение кадровой безопасности организации имеет цель:

а) защиту персонала организации от возможных угроз;

б) защиту организации от возможных угроз со стороны собственного персонала;

в) как защиту персонала организации от возможных угроз, так и защиту организации от возможных угроз со стороны собственного персонала.

2. Наиболее распространенной угрозой в адрес персонала организации выступает:

а) переманивание ведущих сотрудников организации конкурентами;

б) вербовка сотрудников организации;

в) покушение на руководителей организации.

3. В современных условиях наиболее опасной для организации угрозой со стороны собственного персонала является:

а) коррупция;

б) растраты и хищения денежных средств работодателя;

в) разглашение конфиденциальной информации.

4. В современных отечественных условиях наиболее распространенной угрозой со стороны персонала является:

а) коррупция;

б) мелкие хищения имущества работодателя;

в) разглашение конфиденциальной информации.

5. В отечественных условиях наиболее распространенной причиной разглашения персоналом конфиденциальной информации является…

а) злой умысел виновных сотрудников;

б) безответственность виновных сотрудников;

в) отсутствие у виновных сотрудников необходимых компетенций.

6. Наиболее эффективной группой методов противодействия угрозам кадровой безопасности организации являются:

а) профилактические методы;

б) пресекающие методы;

в) репрессивные методы.

7. Для воздействия на сотрудников, нанесших ущерб безопасности организации, в первую очередь, должны использоваться:

а) административные методы;

б) экономические методы;

в) психологические методы.

8. Наиболее опасной угрозой по кадровому направлению работы организаций, представляющих реальный сектор экономики выступает:

а) разглашение коммерческой тайны;

б) коррупция в форме взяток от поставщиков и подрядчиков;

в) разглашение конфиденциальной технологической информации.

9. Наиболее опасной угрозой по кадровому направлению работы организаций, представляющих финансовый сектор экономики выступает:

а) разглашение конфиденциальной информации клиентов;

б) коррупция в форме взяток от клиентов (заемщиков, страхователей);

в) разглашение коммерческой тайны.

10. Наиболее распространенной угрозой по кадровому направлению работы организаций, представляющих органы государственного управления, выступает:

а) хищение государственных средств;

б) коррупция в форме взяток от представителей бизнес-сообщества;

в) разглашение конфиденциальной информации

4. Практические задания

1. Проведите классификацию основных угроз безопасности организации со стороны ее персонала, заполнив для этого соответствующие графы таблицы.

Типовые угрозы информационной безопасности организации	Типовые угрозы имущественной безопасности организации

2. Сформулируйте положения по направлениям кадровой стратегии организаций – работодателей, способные оказать негативное влияние на их кадровую безопасность, заполнив для этого правую графу таблицы.

Направления кадровой стратегии	Недопустимые цели и приоритеты
Политика привлечения и сокращения персонала	
Политика развития персонала	
Политика мотивации персонала	
Политика психологической поддержки персонала	

3. Ориентируясь на приведенный ниже перечень, проведите классификацию основных методов противодействия угрозам по кадровому направлению деятельности организации, заполнив для этого правую графу таблицы (выберите из списка ниже).

Группы методов противодействия	Методы
Профилактические методы	
Пресекающие методы	
Репрессивные / карающие методы	

Перечень методов противодействия угрозам по кадровому направлению деятельности организации:

- увольнение сотрудника за нарушение принятых на себя обязательств перед работодателем;
- отказ в найме на работу;
- режимные мероприятия;
- экономические санкции к сотруднику;
- использование специальных технологий отбора кандидатов на трудоустройство;
- служебные расследования в отношении конкретных сотрудников;
- иск о возмещении сотрудником нанесенного имущественного ущерба;
- увольнение по результатам завершения испытательного срока;

- специальное обучение сотрудников;
- использование специальных программных средств защиты информации в электронной форме;
- иск о возбуждении в отношении сотрудника уголовного преследования;
- оперативный контроль над деятельностью сотрудника;
- регулярные проверки соблюдения в структурных подразделениях корпоративных стандартов;
- психологическая поддержка сотрудников;
- ограничение доступа к конфиденциальной информации и имущественным комплексам организации для ее сотрудников;
- разъяснительно-воспитательная работа с сотрудником;
- отказ в продлении трудового договора;
- перевод на другое рабочее место или в другое подразделение;
- использование специальных технических средств защиты имущества;
- увольнение по соответствующей статье ТК РФ;
- найм новых сотрудников только при наличии у них специальных рекомендаций от действующих сотрудников организации или ее доверенных бизнес-партнеров.

4. Определите основные проявления отраслевой специфики обеспечения кадровой безопасности организаций, представляющих различные сферы профессиональной деятельности, заполнив для этого соответствующие графы приведенной ниже таблицы.

Перечень элементов в системе безопасности	Основные сферы профессиональной деятельности			
	Реальный сектор экономики	Финансовый сектор экономики	Сфера торговли и бытового обслуживания	Сфера государственного управления
Главный субъект угроз				
Главный объект угроз				
Главная форма реализации угроз				

5. Сформулируйте особенности трудовой ментальности россиян, способные оказать влияние на кадровую безопасность организаций-работодателей, заполнив правую графу таблицы.

Направления проявления трудовой ментальности	Особенности менталитета
Отношение к трудовой деятельности	
Отношение к работодателю	
Отношение к коллегам	

2. СИСТЕМА КАДРОВОЙ БЕЗОПАСНОСТИ, ПОЛИТИКА, ПОКАЗАТЕЛИ НАДЁЖНОСТИ

2.1. Показатели надёжности системы безопасности. Политика и стратегия безопасности

Надежность и эффективность системы безопасности предприятия оценивается на основе одного критерия – степени отсутствия или наличия нанесенного ему материального ущерба и морального вреда.

Содержание этого критерия раскрывается через ряд показателей:

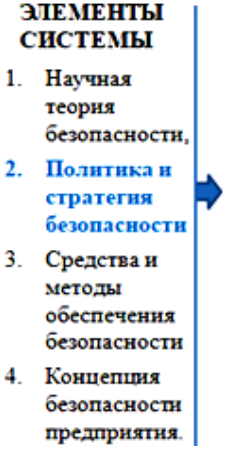
1) недопущение фактов утечки (разглашения) конфиденциальных сведений;

2) предупреждение или пресечение противоправных действий со стороны персонала предприятия, его посетителей, клиентов;

3) сохранность имущества и интеллектуальной собственности предприятия;

4) предупреждение чрезвычайных ситуаций;

5) пресечение насильственных преступлений в отношении отдельных (специально выделенных) сотрудников и групп сотрудников предприятия;



6) своевременное выявление и пресечение попыток несанкционированного проникновения на охраняемые объекты предприятия.

Политика и стратегия безопасности – это общие ориентиры для действий и принятия решений, которые облегчают достижение целей.

Такими *целями* могут быть:

1. Укрепление дисциплины труда и повышение его производительности.

2. Защита законных прав и интересов персонала.

3. Укрепление интеллектуального потенциала предприятия.

4. Сохранение и приумножение собственности.

5. Повышение конкурентоспособности производимой продукции.

6. Максимально полное информационное обеспечение деятельности предприятия и повышение его эффективности.

7. Ориентация на мировые стандарты и лидерство в разработке и освоении новой технологии и выпускаемой продукции.

8. Выполнение производственных программ.

9. Оказание содействия управленческим структурам в достижении целей предприятия.

10.Недопущение зависимости от случайных и недобросовестных деловых партнеров.

Общие ориентиры для действий и принятия решений:

- сохранение и наращивание ресурсного потенциала;
- проведение комплекса превентивных мероприятий по повышению уровня защищенности собственности и персонала предприятия;
- включение в деятельность по обеспечению безопасности предприятия всех его сотрудников;
- профессионализм и специализация персонала предприятия;
- приоритетность не силовых методов предотвращения и нейтрализации угроз.

Для успешного выполнения этой политики необходимо реализовать *стратегию безопасности*, под которой понимается *совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия.*

Выделяют три типа стратегий безопасности:

1. Ориентированные на устранение существующих или предотвращение возникновения *возможных угроз*.

2. Нацеленные на предотвращение воздействия существующих или возможных угроз на предмет *безопасности*.

3. Направленные на восстановление (компенсацию) *наносимого ущерба*.

2.2. Субъекты безопасности предприятия, их элементы

Субъекты безопасности предприятия делятся на две группы (рис. 1).

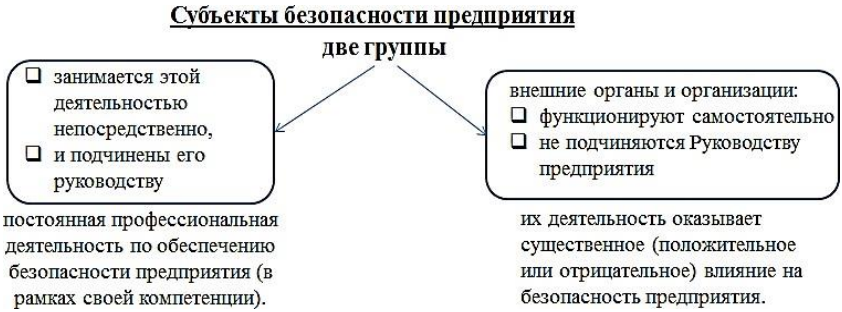


Рис. 1. Субъекты безопасности предприятия

К первой группе относятся:

Специализированные субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, строительная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетентности).

Полуспециализированные, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.).

Весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности.

Ко второй группе относятся:

Законодательные органы – законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

Органы исполнительной власти – принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования закона.

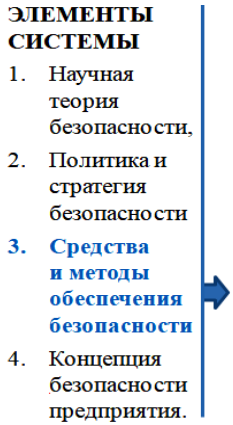
Суды. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в том числе в сфере кадровой безопасности.

Правоохранительные органы. Они осуществляют борьбу с правонарушениями, которые негативно влияют на состояние безопасности предприятия.

Научно-образовательные учреждения (для подготовки частных охранников и детективов) – они призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятия.

2.3. Средства и методы обеспечения безопасности. Этапы их применения

Все средства обеспечения безопасности предприятия подразделяются на семь групп. Среди них: технические, организационные, финансовые, информационные, правовые, кадровые и интеллектуальные. Применять данные средства обеспечения безопасности следует комплексно. Причем следует соблюдать этапы их применения. Так *на первом этапе* – используют исключительно финансовые средства. Важно понимать, что недостаточность именно этих средств обеспечивает всю дальнейшую работу по обеспечению безопасности на предприятии. Если данных средств будет недостаточно, то не будет никакой гарантии безопасности от кадровых и другого рода угроз. Среди принципов использования финансовых средств выделяют: их достаточность, целенаправленность и высокую отдачу применения (эффективность).



На втором этапе подключают формирование кадровых и организационных средств. Это значит, что должно быть достаточно кадров, занимающихся вопросами обеспечения безопасности; имеющиеся в наличии кадры должны отвечать высокому профессиональному уровню, который регулярно оттачивается и повышается.

Что же касается организационных средств, то создаются специализированные оргструктурные формирования, обеспечивающие безопасность предприятия.

На третьем этапе – осуществляется разработка системы правовых средств. С одной стороны, используются уже изданные вышестоящими органами власти законы и подзаконные акты. С другой стороны, разрабатываются собственные, локальные правовые акты по вопросам обеспечения кадровой безопасности.

Наконец, *на четвёртом этапе* привлекаются всевозможные технические, информационные и интеллектуальные средства.

Таким образом можно отметит понятность и последовательности логики применения всех имеющихся средств обеспечения безопасности в организации.

Методы воздействия на персонал в службе безопасности:

– методы диагностики угроз кадровой безопасности как со стороны внешних, так и внутренних факторов воздействия;

– методы, противостоящие потенциальной и/или реальной кадровой угрозе для организации.

Приведем классификацию методов диагностики кадровой безопасности (рис. 2)

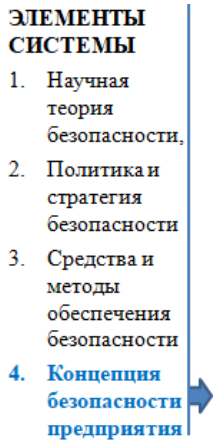
Методы целенаправленного воздействия	Методы тайного принуждения	Методы информационно-психологического воздействия
– Пресечение мошенничества. – Рейдерский захват. – Предотвращение коррупционной деятельности в организации. – Другое 	– Конкурентная разведка. – Вербовка работников. – Манипуляции, в том числе с использованием нейролингвистического программирования (НЛП). – Промышленный шпионаж. – Другое	– Нарушение прав работников на рабочем месте, дискриминация. – Психологическое насилие: моббинг, буллинг, харассмент. – Распространение слухов, сплетен, провокаций. – Утечка/похищение информации. – Несанкционированный сбор, хранение, обработка, использование данных сотрудников. – Передача персональных данных третьим лицам. – Другое

Рис. 2. Методы диагностики кадровой безопасности

2.4. Концепция безопасности предприятия, сущность, её структура и составные элементы

Определяющим и изначальным звеном при формировании системы безопасности является концепция безопасности организации.

Концепция – это официально утверждённый документ, в котором отражена система взглядов, требований и условий организации мер безопасности персонала и собственности предприятия. *Концепция* – это свод основных документов, касающихся:



– политики безопасности;
– стратегии безопасности;
– основных направлений;
– средств и методов ее обеспечения.

Выделяют некоторые требования к концепции безопасности:

– *Конструктивность* – добиться исходного состояния объекта при использовании необходимых и остаточных средств в достижении цели;
– Вписываемость в единую систему объектов;
– Открытость – давать возможность в её рамках реагировать на изменение условий реализации концепции и вносить коррективы в реализацию в случае их необходимости.

Структура концепции безопасности включает в себя три части:

1. *Описание проблемной ситуации в сфере безопасности предприятия*:

– Перечень потенциальных и реальных угроз безопасности, их классификация и ранжирование.
– Причины и факторы зарождения угроз.
– Негативные последствия угроз для предприятия.

2. *Механизм обеспечения безопасности:*

– Определение объекта и предмета безопасности предприятия.
– Формулирование политики и стратегии безопасности.

– Принципы обеспечения безопасности.

– Цели обеспечения безопасности.

– Задачи обеспечения безопасности.

– Критерии и показатели безопасности предприятия.

– Создание оргструктуры по управлению системой безопасности предприятия.

3. Мероприятия по реализации мер безопасности:

– Формирование подсистем общей системы безопасности предприятия.

– Определение субъектов безопасности предприятия и их роли.

– Расчет средств и определение методов обеспечения безопасности.

– Контроль и оценка процесса реализации концепции.

Структура концепции безопасности примерная, однако, она предусматривает все необходимые направления деятельности для обеспечения системы безопасности на объекте.

2.5. Кадровая безопасность организации как объект управления. Виды кадровой безопасности и кадровых угроз

Угроза кадровой безопасности организации – это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке её функционирования.

Обеспечение безопасности организации – это деятельность её должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения её нормального функционирования

Раскроем *сущность видов кадровой безопасности*.

Физическая безопасность объекта – это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, терроризм, стихийное бедствие) и от несанкционированного

проникновения на территорию (вандализм, кража, хищение и т.д.). Этот вид безопасности объекта обеспечивается *деятельностью сотрудников службы охраны* путём соблюдения пропускного объектового и внутриобъектового режимов с применением соответствующих *охранных технических средств и систем*.

К *техническим и инженерно-техническим охранным средствам и системам* относятся:

– Периметральные охранные системы.

– Системы охранной сигнализации.

– Системы пожарной сигнализации, пожаротушения и оповещения.

– Системы ограничения доступа.

– Системы управления доступом.

– Средства связи.

– Защитные инженерные средства (решетки, жалюзи, бронестёкла и др.).

Экономическая безопасность объекта – это состояние защищенности экономических интересов организации от внутренних и внешних угроз посредством минимизации коммерческих рисков, системы мер экономического, правового и организационного характера, разработанных администрацией организации. Экономическая безопасность характеризуется совокупностью качественных и количественных показателей и включает в себя следующие функциональные составляющие: финансовую, имущественную, валютную, кредитную, политико-правовую и др. Экономическая безопасность выступает материальной основой решения практически всех задач, связанных с функционированием организации.

Информационная безопасность – это охрана каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа. Защите подлежит любая документационная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении

конфиденциальной документационной информации собственником информационных ресурсов, т.е. самой организацией. Результатами реализации угроз информации могут быть:

– утрата (разрушение, уничтожение);
– утечка (извлечение, копирование, подслушивание);
– искажение (модификация, подделка);
– блокирование.

Существует два основных *принципа защиты информации*:

– разделение обязанностей;
– минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не смог нарушить критически важный для предприятия процесс. *Принцип минимизации привилегий* предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Юридическая безопасность – это охрана прав, порядка и условий осуществления конкурентной предпринимательской деятельности организации в рамках законодательства Российской Федерации.

Выделяют три основных направления юридической безопасности:

1. Взаимоотношения с органами государственной власти.
2. Защита от действий недобросовестных партнёров, заказчиков или контрагентов.
3. Создание условий для успешной производственной деятельности организации.

Интеллектуальная безопасность – это охрана прав на научные труды, промышленные образцы, товарные знаки, коммерческие наименования.

Гражданский кодекс РФ (ст. 138) «признает исключительное право (интеллектуальную собственность) ... юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Использование результатов интеллектуальной деятельности и средств индивидуализации может осуществляться третьими лицами только с согласия правообладателя».

Экологическая безопасность включает охрану окружающей среды, обеспечение безопасной работы экологически опасных объектов предприятия, предотвращение экологических катастроф.

Кадровая безопасность – это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет:

- рисков и угроз, связанных с персоналом;
- его интеллектуальным потенциалом;
- трудовыми отношениями в целом.

Виды угроз со стороны персонала могут выражаться в следующем:

1. Хищение имущества предприятия.
2. Использование ресурсов предприятия в собственных целях.
3. Умышленная порча и уничтожение имущества предприятия.
4. Получение заработной платы за невыполняемую работу.
5. Шантаж компетентностью (я – незаменимый работник).
6. Шантаж полномочиями (концентрация полномочий в одних руках).
7. Торговля коммерческими секретами.
8. Дисциплинарные нарушения.
9. Создание в коллективе невыносимого морально-психологического климата.

Кадровая безопасность включает обеспечение *физической безопасности* персонала. Физическая безопасность включает:

1. Личную безопасность руководителя.
2. Личную безопасность ведущих специалистов.
3. Безопасность всего персонала в целом.

Охрана первых двух категорий объектов регулируется Законом РФ «О частной детективной и охранной деятельности». Сюда относят физическую охрану руководителей и ведущих специалистов организации, а также охрану их жилья и средств передвижения и членов их семей. Личная безопасность обеспечивается целым комплексом оперативных и технических мер по охране лица как в обычных повседневных, так и в экстремальных условиях.

Охрана третьей категории объекта регламентируется Трудовым кодексом РФ (разд. X), Законом РФ «Об основах охраны труда в Российской Федерации» и нормативными правовыми актами

по охране труда. Это система охраны труда и техники безопасности в организации на основе производственной санитарии и психологии деловых отношений. Безопасные и здоровые условия труда в организации обеспечиваются комплексным взаимодействием как руководства организации, так и, не в последнюю очередь, усилиями самого персонала организации.

Кадровую безопасность в организации рассматривают с позиций:

- процесса обеспечения текущей и потенциальной защищенности *персонала* от разнообразных угроз со стороны организации, в трудовых отношениях (основным *источником угроз выступает работодатель*, грубо нарушающий права и гарантии работников);
- с точки зрения активной защиты, в которой *нуждается сама организация*.

Речь идет об экономической безопасности, имидже и устойчивом развитии внутренних бизнес-процессов, об угрозах, создаваемых несанкционированными сознательными или неосознанными *действиями персонала данной организации***,** которые могут вступать в сомнительные с точки зрения закона трудовые отношения. В эту группу включим: коррупционную деятельность чиновников и лиц, принимающих решение, злоупотребляющих своим положением; сговор, передачу секретной информации третьим лицам или использование её не по прямому назначению; вербовку редких специалистов, переманивание их в конкурирующие организации; рейдерские захваты, другие виды насильственных действий, физическую расправу.

Как видно, *кадровую безопасность составляют риски со стороны персонала, которые возникают всегда и на всех этапах работы*.

Главный инструмент работы службы кадровой безопасности – тотальный контроль на всех участках работы персонала. Для этого применяют специальные средства, такие как видеонаблюдение, прослушивание телефонных разговоров, контроль доступа и работы компьютера, контроль использования рабочего и свободного времени сотрудников, контроль перемещений.

Важно также выстраивать качественное взаимодействие со службами управления персоналом в организации, начиная с этапа

подбора и найма кадров. Список «опасных» кандидатов – это люди, чья работа в организации или их последующее увольнение может вызвать различные проблемы.

Что касается *методов и техник* – они самые разнообразные и очень специфичные, законные, и не очень:

- *традиционный headhunting («хэдхантинг);*
- *talent raiding («кадровые налеты»);*
- *talent poaching («кадровое браконьерство»);*
- *executive search – «переманивание» лиц, принимающих решение;*
- *«агрессивный»* или «партизанский» рекрутинг.

В применении методов и техник необходимо разграничивать функции HR-структур и служб безопасности. Если менеджеры в большей степени связаны с оценкой деловых и профессиональных качеств кандидатов (например, при подборе кадров), то службы безопасности применяют в большей степени силовые методы, используют повышенный уровень секретности. А для обнаружения хищений применяется ТОП-5 методов безопасности:

1. Электронный контроль – видеокамеры, мониторинг трафика в сети.
2. Технические средства защиты – сигнализация, электронный доступ, турникеты.
3. Внезапные ревизии.
4. Беседы с работниками.
5. Наблюдение за действиями сотрудников и технологическими процессами.

ВОПРОСЫ И ЗАДАНИЯ

1. Вопросы для обсуждения

1. В каких организациях целесообразно использование стратегии упреждающего противодействия угрозам?
2. В каких организациях целесообразно использование стратегии пассивной защиты от возможных угроз?

3. Каким организациям целесообразно полностью отказаться от услуг частных детективных и охранных агентств?

4. Каким организациям целесообразно передать основные функции по обеспечению защиты кадровых угроз частным детективным и охранным агентствам?

5. Какие критерии могут использоваться для оценки работы службы безопасности организации?

6. Каковы основные направления взаимодействия службы безопасности с другими подразделениями?

7. Кто должен принимать окончательное решение о выборе варианта общей стратегии управления кадровой безопасностью в коммерческих организациях?

8. В чем заключается основное преимущество использования коммерческой организацией стратегии адекватного ответа на угрозы?

9. Какие основные федеральные законы входят в состав нормативно-методического обеспечения системы управления кадровой безопасностью?

10. Почему вице-президент по безопасности должен иметь беспрепятственный доступ не только к президенту, но и к собственникам коммерческой организации?

11. Почему угрозы безопасности по кадровому направлению имеют тесную взаимосвязь со всеми другими аспектами обеспечения безопасности организации?

2. Напишите эссе

1. Взаимодействие системы управления безопасностью с другими элементами комплексной системы корпоративного менеджмента.

2. Внутреннее нормативно-методическое обеспечение системы управления безопасностью организации.

3. Роль руководителей структурных подразделений в системе управления безопасностью организации.

4. Проблемы кадрового обеспечения деятельности службы безопасности организации.

5. Проблемы финансового обеспечения системы управления кадровой безопасностью организации.

6. Полномочия частных охранных предприятий и детективных агентств в современной России.

7. Взаимодействие службы безопасности и службы персонала.

8. Особенности организации службы безопасности в государственных учреждениях.

9. Особенности организации службы безопасности в корпорациях и в малом предпринимательстве.

3. Выполните тестовое задание

1. Наиболее затратной из возможных стратегий обеспечения безопасности организации-работодателя выступает:

а) стратегия упреждающего противодействия угрозам;

б) стратегия адекватного ответа на угрозы;

в) стратегия пассивной защиты от угроз.

2. Наиболее распространенной из возможных стратегий обеспечения безопасности организации-работодателя выступает:

а) стратегия упреждающего противодействия угрозам;

б) стратегия адекватного ответа на угрозы;

в) стратегия пассивной защиты от угроз.

3. Основным недостатком стратегии упреждающего противодействия угрозам выступает:

а) высокая ресурсоемкость;

б) высокая вероятность конфликтов с законом;

в) высокая вероятность конфликтов с конкурентами, клиентами, другими контактными аудиториями.

4. В стратегии обеспечения безопасности организации-работодателя необходимо отражать:

а) стратегический подход к организации службы безопасности;

б) стратегический подход к организации взаимодействия со сторонними подрядчиками, специализирующимися в этой области;

в) стратегические подходы к организации собственной службы безопасности и к организации взаимодействия со сторонними подрядчиками, специализирующимися в этой области.

5. Система управления собственной безопасности современной организации должна состоять:

а) из трех базовых элементов;

б) из пяти базовых элементов;

в) из шести базовых элементов.

6. Система управления безопасностью современной организации по кадровому направлению ее деятельности должна включать в себя:

а) две операционные подсистемы;

б) три операционные подсистемы;

в) пять операционных подсистем.

7. Блок обеспечения системы управления безопасностью организации по кадровому направлению ее деятельности должен включать в себя …

а) три направления;

б) пять направлений;

в) шесть направлений.

8. Наиболее важную роль в блоке обеспечения системы управления безопасностью современной организации играет:

а) технологическое обеспечение;

б) нормативно-методическое обеспечение;

в) информационное обеспечение.

9. В организациях, представляющих средний и малый бизнес, система управления безопасностью должна разрабатываться силами:

а) штатных специалистов собственной службы безопасности;

б) топ-менеджеров;

в) приглашенных консультантов.

10. Наиболее распространенным вариантом привлечения сотрудников частных детективных агентств к отражению угроз, связанных с кадровым направлением деятельности организации, выступает …

а) привлечение для выполнения конкретных заданий;

б) привлечение на основе договоров о постоянном бизнес-партнерстве с соответствующим агентством;

в) принципиальный отказ от услуг сторонних агентств.

4. Практические задания

1. Раскройте содержание основных элементов системы управления безопасностью организации по кадровому направлению деятельности, заполнив для этого соответствующие графы таблицы.

Элементы системы	Содержание элемента
Стратегия управления	
Операционные подсистемы	
Блок обеспечения системы	

2. Сформулируйте основные функции субъектов управления безопасностью организации по кадровому направлению ее деятельности, заполнив для этого правую графу таблицы.

Субъекты управления	Основные функции в рамках системы
Топ-менеджмент	
Служба безопасности	
Служба персонала	
Руководители структурных подразделений	

5. Кейс. Потеря или кража электронной подписи (ЭП)

Ситуация. Потеря или кража электронной подписи (ЭП) – редкая, но неприятная для владельца подписи ситуация. Чтобы минимизировать ущерб, нужно быстро заметить пропажу и отозвать сертификат.

Вопрос: Как выявить пропажу, что делать дальше и каких последствий опасаться?

Ответ-справка: ***Как понять, что электронная подпись пропала?*** Потеря и кража ЭП (или ЭЦП) очевидна, если из вашего офиса вынесли сейф, в котором лежал токен с подписью, носитель пропал из ящика тумбочки или вы думаете, что потеряли электронную подпись. Сложнее заметить пропажу подписи, если ее закрытый ключ скопировали с компьютера или подпись тайком оформил тот, кто завладел вашим паспортом.

О компрометации или краже электронной подписи можно узнать несколькими способами:

В своем профиле на Госуслугах. В разделе «Настройки и безопасность» – «Электронная подпись» *отобразятся все сертификаты* электронной подписи, в которых указаны ваши данные. Также в разделе «Последние действия» отразится, какие действия совершали с ЭП – например, оформляли ИП или ООО. Чтобы не пропустить подозрительных действий с подписью, настройте уведомления от Госуслуг.

Проверяйте свой личный кабинет в налоговой на сайте *nalog.ru*. Вы увидите, не пытался ли кто-то продать ваше имущество или подать отчетность от вашей компании. Здесь также можно настроить уведомления на электронную почту.

Проверьте свои последние действия в сервисах, где раньше использовали ЭП. Например, если вы вели электронный документооборот через сервис *Контур.Диалог* или отправляли заявки на участие в закупке через *Контур.Закупки*. Если мошенники, укравшие подпись, были в сервисе, вы это заметите.

Самый неприятный сценарий – узнать о краже после того, как преступники воспользуются вашей подписью: вам придет счет на оплату кредита, который вы не оформляли, или налоговая сообщит о недостоверной отчетности, которую вы не сдавали.

Что делать, если украли электронную подпись: инструкция

Шаг 1. Отзовите сертификат в удостоверяющем центре

Напишите в УЦ заявление на отзыв сертификата ЭП, как только поймете, что ваша подпись попала в руки посторонних. Чем раньше вы аннулируете сертификат, тем меньше незаконных операций от вашего имени они проведут.

Шаг 2. Подайте в налоговую заявление о недостоверности данных. Это шаг для тех, от чьего имени незаконно подали налоговую декларацию, зарегистрировали компанию или совершили другое действие в налоговой. Если за вас сдали отчетность, как можно скорее посетите ближайшую налоговую инспекцию и подайте заявление в произвольной форме о недостоверности сведений.

Шаг 3. Подайте заявление в полицию. Если действия посторонних с вашей электронной подписью причинили ущерб, то подайте заявление в полицию по месту своего жительства или по месту нахождения налоговой инспекции, в которой зарегистрировали фиктивное юрлицо. К заявлению приложите копии документов из УЦ. Если в полиции откажутся возбуждать дело, то можно обратиться в прокуратуру и Минкомсвязь.

Возможно, от вашего имени успеют провести незаконную сделку или подписать значимые документы. Тогда вы можете обратиться в суд и аннулировать договор или признать документы недействительными. Так, в октябре 2019 года суд признал недействительным договор купли-продажи квартиры, которую мошенники украли у москвича с помощью электронной подписи. Разбирательство заняло около полугода.

Как отозвать электронную подпись

Если вы потеряли ЭЦП или ее у вас украли, как можно скорее отзовите сертификат. Тогда посторонние люди не смогут им воспользоваться. Для этого напишите заявление на отзыв сертификата и передайте его в удостоверяющий центр, выпустивший сертификат.

3. СТРУКТУРА УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ

Охранно-сыскное подразделение = служба безопасности предприятия.

Особенности СБ выделяют её из других форм:

– частной детективной;

– частной охранной деятельности.

Особенности службы безопасности:

1. Особый порядок создания и ликвидации службы безопасности.

2. Обязательное наличие в структуре службы безопасности детективных и охранных подразделений.

3. Нет затруднений при определении числа охранников (здесь применима методика, принятая в органах внутренних дел), но сложно определить количество детективов и других сотрудников. Определения их числа зависит от опыта и интуиции руководителей СБ (нормативы на эти категории сотрудников отсутствуют).

3.1. Особый порядок создания и ликвидации службы безопасности

Под *предприятием*, которое вправе учреждать собственную службу безопасности, понимается исключительно коммерческая организация. Это могут быть: товарищества различного рода, акционерные общества, государственное унитарное предприятие, муниципальное унитарное предприятие.

Предприятие-учредитель представляет в органы внутренних дел (по месту своего нахождения) следующие документы:

1. Заявление о согласовании Устава службы безопасности.
2. Устав службы безопасности.
3. Лицензии на руководителя и персонал службы безопасности.

4. Сведения:

– о характере и направлениях деятельности службы безопасности;
– о составе и предполагаемой численности персонала;
– о наличии специальных средств;
– технических и иных средств, потребности в них;
– об оружии.

Учредителями службы безопасности не могут быть:

– физические лица (даже имеющие лицензии на осуществление частной детективной и охранной деятельности);
– не могут быть несколько юридических лиц;

Учредителем службы безопасности может быть только одно предприятие. При создании службы безопасности *предприятие-учредитель может предоставить* службе безопасности право открывать текущий и расчетный счет в банке (это должно найти отражение в Уставе).

Текущий счет предназначается только для операций, связанных с выдачей наличных денег. По *расчетному счету* проводятся операции по безналичным перечислениям. Но это не позволяет относить службу безопасности к юридическому лицу, так как его важнейший признак – наличие у него обособленного имущества – отсутствует. Данный порядок учреждения службы безопасности следует признать несовершенным.

Термин *«охранно-сыскное подразделение на предприятии»* (ст. 14 Закона РФ «О частной детективной и охранной деятельности в Российской Федерации») означает, что служба безопасности как оргструктурное формирование *может функционировать только в рамках юридического лица, т.е. предприятия-учредителя*.

Ликвидация службы безопасности может произойти:

– при добровольном отказе его персонала от выполнения своих обязанностей;
– по инициативе предприятия-учредителя;
– при ликвидации предприятия-учредителя;
– в случае аннулирования органом внутренних дел лицензий всем охранникам и детективам.

3.2. Обязательное наличие в структуре службы безопасности детективных и охранных подразделений

Такое сочетание детективных и охранных подразделений позволяет:

– наладить взаимодействие между ними;

– проводить комплексные мероприятия по предупреждению и пресечению правонарушений и т.д., что повышает эффективность деятельности службы безопасности.

Соотношение между группами детективов и охранников может быть различным. Это зависит от:

– финансовых возможностей учредителя;
– невозможности подбора в данной местности детективов;
– недопонимание со стороны предпринимателей роли и значения сыскных подразделений, другое.

Несмотря на отсутствие единых правил, при определении соотношения детективных и охранных подразделений внутри службы безопасности можно использовать критерии:

– наличие коммерческой тайны;
– состояние, структура и динамика;
– правонарушений на предприятии;
– наличие значительных материальных ценностей и валюты;
– реальная и потенциальная сумма нанесенного предприятию ущерба;
– имеющиеся факты промышленного шпионажа;
– реальность угроз физической расправы над сотрудниками предприятия со стороны преступных элементов;
– фактические возможности со стороны местных правоохранительных органов в оказании помощи предприятию в пресечении правонарушений;
– взаимоотношения с конкурентами и соблюдение правил функционирования рыночной экономики;
– степень правовой и иной подготовки сотрудников по вопросам обеспечения безопасности предприятия и т.д.

3.3. Определение численности сотрудников в структуре кадровой безопасности

Нет затруднений при определении числа охранников (здесь применима методика, принятая в органах внутренних дел), но сложно определить количество детективов и других сотрудников. Определения их числа зависит от опыта и интуиции руководителей СБ (нормативы на эти категории сотрудников отсутствуют).

Определим *структуру персонала службы безопасности*.

Закона РФ «О частной детективной и охранной деятельности в Российской Федерации» гласит, что *персонал службы безопасности* – это только те лица, которые в установленном порядке получили лицензии *детективов* и *охранников*. Имеются еще *руководители службы безопасности*, статус которых не определен.

В службе безопасности также работает и *вспомогательный персонал* – водители, программисты, секретари, машинистки и др. Их статус определяется должностными инструкциями, а численность данного персонала регламентируется существующими нормативами.

Типовая *стратегия службы безопасности* предусматривает три основных варианта противодействия кадровым угрозам.

ВАРИАНТ 1. СТРАТЕГИЯ УПРЕЖДАЮЩЕГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

Принципы реализации:

- приоритет профилактических методов противодействия возможным угрозам;
- возможность применения нелегитимных методов.

Преимущества варианта:

- возможность эффективного решения возникающих у организации проблем, связанных с обеспечением собственной безопасности, практически без участия государства;
- возможность обеспечения эффективной поддержки других направлений внутрикорпоративного менеджмента.

Недостатки варианта:

- высокая вероятность конфликтов с действующим законодательством, конкурентами и собственными сотрудниками;

– необходимость дорогостоящей ресурсной поддержки – финансовой, кадровой, материально-технической.

ВАРИАНТ 2. СТРАТЕГИЯ ПАССИВНОЙ ЗАЩИТЫ ОТ УГРОЗ

Принципы реализации:

– приоритетная ориентация на защиту со стороны государства в лице правоохранительных и судебных органов;
– минимизация собственных затрат по рассматриваемому направлению деятельности.

Преимущества варианта:

– минимальные затраты на практическую реализацию стратегии;
– отсутствие угрозы конфликтов и, связанных с ними, проблем в отношениях с конкурентами, государством, собственным персоналом.

Недостатки варианта:

– полная зависимость безопасности организации от эффективности деятельности правоохранительных органов государства;
– ориентация на методы противодействия уже реализованным угрозам, которые являются менее эффективными по сравнению с профилактическими и пресекающими.

ВАРИАНТ 3. СТРАТЕГИЯ АДЕКВАТНОГО ОТВЕТА НА УГРОЗЫ

Принципы реализации:

– предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз;
– в порядке исключения допускается использование и не полностью легитимных методов, но лишь в отношении тех конкурентов или иных источников угроз, которые первыми применили подобные методы.

Факторы, определяющие выбор варианта стратегии противодействия кадровым угрозам:

– отрасль или сфера деятельности организации;
– степень агрессивности конкурентной стратегии организации;

– степень легитимности бизнеса организации;
– финансовые возможности организации к обеспечению безопасности;
– квалификация персонала службы безопасности;
– наличие поддержки со стороны органов государственной власти.

Можно выделить несколько *принципов* работы службы безопасности. Среди них:

1. *Координация и взаимодействие внутри и вне предприятия*. Она осуществляется на основе:
– взаимодействия и координации усилий всех подразделений, служб предприятия;
– установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия

2. *Приоритет мер предупреждения* – своевременное выявление тенденций и предпосылок, способствующих развитию угроз

3. *Законность* – это значит действовать:
– на основе закона;
– в рамках действующих правовых актов.

4. *Комплексное использование сил и средств***.** Для обеспечения безопасности:
– используются все имеющиеся в распоряжении предприятия силы и средства;
– каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия;
– организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

5. *Компетентность* – это значит решать вопросы обеспечения безопасности:
– на профессиональном уровне;
– в необходимых случаях специализироваться по основным его направлениям.

6. *Системность*, т.е.:
– учитывать все факторы, оказывающие влияние на безопасность предприятия;

– включать в деятельность по его обеспечению всех сотрудников подразделений;
– использовать все силы и средства.

7. *Сочетание гласности с конспирацией*
– доведение до сведения персонала предприятия и общественности (в допустимых пределах) мер безопасности;
– такая гласность должна дополняться мерами конспиративного характера.

8. *Принцип экономической целесообразности.* Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

9. *Плановая основа деятельности* выстраивается на основе*:*
– комплексной программы обеспечения безопасности предприятия;
– подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия;
– отдельных сотрудников.

Структуру службы безопасности изобразим схематично на рис. 3.

3.4. Основные структурные подразделения службы безопасности

Информационно-аналитический отдел, выполняющий функции «мозгового центра», в который стекается и анализируется вся информация об её деятельности, а также формируются рекомендации для руководства и других подразделений;

Отдел информационной безопасности, деятельность которого направлена на защиту любой конфиденциальной информации;

Рис. 3. Структура службы безопасности

Отдел физической защиты, деятельность которого направлена на защиту имущества и персонала и включающий в себя службу телохранителей и патрульно-постовую службу.

Отдел собственной безопасности, который обеспечивает защиту от угроз со стороны некомпетентных или нелояльных работников самой службы безопасности.

3.5. Взаимодействие службы безопасности с другими службами в рамках системы обеспечения кадровой безопасности в организации

Кадровые угрозы безопасности организации могут формироваться во всех сферах деятельности персонала. Поэтому службе конкурентной разведки необходимо, прежде всего, наладить тес-

ный контакт со службой управления персоналом в лице ее директора (а не с отделом кадров!). Отдельно стоит отметить, что кадрами занимается директор по персоналу (HR-департамент). Отдел кадров не имеет отношения к оперативной работе с персоналом. Ведет документальную работу с персоналом, фиксирует результаты работы каждого сотрудника в личных делах (т.е. работа с документами). Структурно отдел кадров подчиняется директору по персоналу вместе с отделом организации и мотивации труда, учебному центру (или отделу развития персонала), отдел аттестации персонала и социального обслуживания. Отдел подбора персонала в структуре организации может быть самостоятельным элементом, но также может быть службой в структуре отдела кадров. Как видите, практически все направления кадровой работы представлены отдельными структурными подразделениями или службами.

Производственный персонал контролируется линейными руководителями и их начальством. В связи с этим система безопасности организации не должна работать независимо от всех названных служб, если она хочет быть эффективной. Другими словами, система безопасности в организации обеспечивается не только службой безопасности, но и всей кадровой службой и каждым отдельным сотрудником организации. В функции управления (службы) по работе с персоналом напрямую входит обнаружение различного рода кадровых угроз.

Поскольку кадровые угрозы создаются собственным персоналом организации, обосновывается необходимость взаимодействия всех кадровых служб в рамках единой системы обеспечения кадровой безопасности и безопасности организации в целом. Взаимодействие осуществляется, прежде всего, со следующими структурными подразделениями в рамках организации:

а) *с маркетинговой службой*:

- выполняется совместное изучение и анализ конкурентов, подготовка аналитических обзоров и рекомендаций для руководства и подразделений организации;
- выполняются совместные поручения по сбору дополнительной информации об отдельных клиентах и партнёрах организации (в том числе и потенциальных);

б) *со службой персонала*:

- проводятся специальные проверки при найме новых сотрудников по заявке со стороны службы персонала;
- участие в первичном обучении вновь нанятых сотрудников;
- координация действий по контролю над лояльностью персонала и соблюдением ими правил обеспечения безопасности работодателя;

в) *с финансовой службой*:

- обеспечивается передача и обоснование заявок на финансовые ресурсы, необходимые для подразделения, отчеты об использовании выделенных средств;
- ведётся совместное расследование фактов нарушений корпоративной финансовой дисциплины (в случае прямых хищений и растрат);

г) *со службой информационных технологий*:

- осуществляются совместные действия по защите компьютерных сетей организации от несанкционированного проникновения и повреждения;
- при разработке службой компьютерного обеспечения новых программных продуктов проводится проверка их защищенности от соответствующих угроз.

Деятельность по обеспечению безопасности предприятия можно подразделить на три основных направления: внешние, внутренние и общесистемные (рис. 4).

Для расследования кадровых угроз применяется следующий алгоритм (рис. 5).

В оперативной практике оказывается, что большое количество кадровых угроз представлено большим разнообразием. В то же время для нейтрализации кадровых угроз полномочия и компетенция организации охранников явно не хватает. В связи с этим важно рассмотреть весь комплекс мер, составляющих целостную систему безопасности.

Рис. 4. Направления обеспечения безопасности предприятия

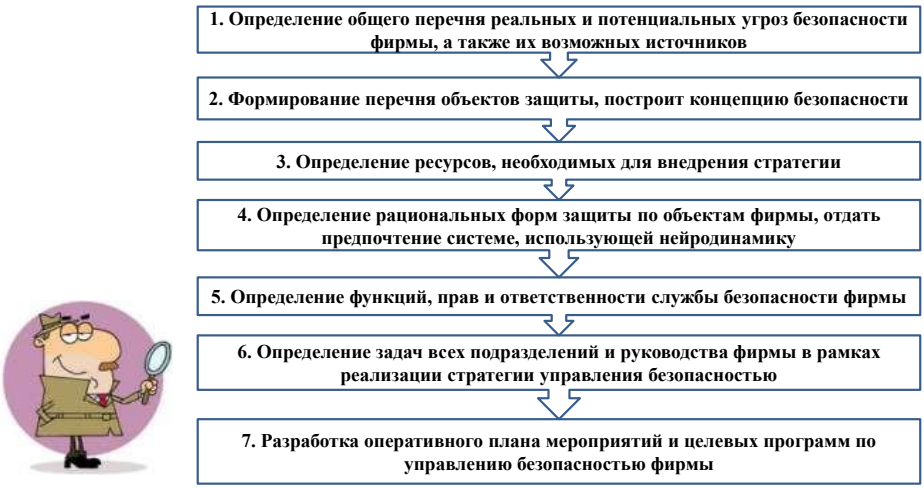


Рис. 5. Алгоритм расследования кадровых угроз

ВОПРОСЫ И ЗАДАНИЯ

1. Вопросы для обсуждения

1. Каковы основные структурные подразделения службы безопасности?
2. Кто должен принимать окончательное решение о выборе варианта общей стратегии управления кадровой безопасностью в коммерческих организациях?
3. В чем заключается основное преимущество использования коммерческой организацией стратегии адекватного ответа на угрозы?
4. Какие основные федеральные законы входят в состав нормативно-методического обеспечения системы управления кадровой безопасностью?
5. Почему вице-президент по безопасности должен иметь беспрепятственный доступ не только к президенту, но и к собственникам коммерческой организации?
6. Почему угрозы безопасности по кадровому направлению имеют тесную взаимосвязь со всеми другими аспектами обеспечения безопасности организации?

2. Подготовьте доклад

1. Технологии выявления потенциальных жертв вербовки и шантажа на стадии отбора кандидатов на трудоустройство.
2. Сплетни в коллективе: как эффективно манипулировать кадрами.
3. Дезинформация, распространение сведений, порочащих деловую репутацию компании.
4. Причинение вреда здоровью.
5. Управление вовлеченностью персонала и кадровая безопасность. Индекс вовлеченности: как повышать продуктивность сотрудников.
6. Нейролингвистическое программирование как метод манипулирования.

7. Понятие слуха, сплетни, провокации. Причины этих явлений.

8. Закон слухов. Классификация слухов. Сплетник в коллективе: как его вычислить и обезвредить.

9. Управление слухами и сплетнями. Как вычислить сплетников при приеме на работу.

10. Провокация как метод психологического воздействия.

11. Переманивание сотрудников как метод недобросовестной конкуренции на рынке труда.

12. Цели и методы вербовки сотрудников организации:

- конкурентами;
- криминалом;
- государственными структурами.

13.Предоставление подложного документа.

3. Выполните тестовое задание

1. Выберите из приведенного ниже перечня показатель надежности системы безопасности:

а) недопущение зависимости от случайных и недобросовестных деловых партнеров;

б) недопущение фактов утечки (разглашения) конфиденциальных сведений;

в) сохранение и приумножение собственности;

г) повышение конкурентоспособности производимой продукции.

2. Выберите из приведенного ниже перечня цель:

а) защита законных прав и интересов персонала;

б) сохранность имущества и интеллектуальной собственности предприятия;

в) своевременное выявление и пресечение попыток несанкционированного проникновения на охраняемые объекты предприятия;

г) предупреждение или пресечение противоправных действий со стороны персонала предприятия, его посетителей, клиентов.

3. Вставьте пропущенную фразу: Для успешного выполнения этой политики необходимо реализовать _____, под кото-

рой понимается совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия:

а) стратегию пассивной защиты от угроз;

б) стратегию адекватного ответа на угрозы;

в) стратегию упреждающего противодействия угрозам;

г) стратегию безопасности.

4. Выберите ориентир для действий и принятия решений:

а) профессионализм и специализация персонала предприятия;

б) недопущение фактов утечки (разглашения) конфиденциальных сведений;

в) укрепление дисциплины труда и повышение его производительности;

г) защита законных прав и интересов персонала.

5. Выберите принцип использования финансовых средств:

а) печатная и видеопродукция по вопросам сохранения конфиденциальной информации;

б) высокая отдача применения;

в) создание специализированных оргструкгурных формирований, обеспечивающих безопасность предприятия;

г) видео-радиоаппаратура.

6. Что относится к организационным средствам?

а) создание специализированных оргструкгурных формирований, обеспечивающих безопасность предприятия;

б) разработка собственных (локальных) правовых актов по вопросам обеспечения безопасности;

в) достаточность кадров, занимающихся вопросами обеспечения безопасности;

г) охранно-пожарные системы.

7. Какой признак относится к внешним органам и организациям?

а) занимается этой деятельностью непосредственно;

б) подчинены его руководству;

в) не подчиняются руководству предприятия;

г) постоянная профессиональная деятельность по обеспечению безопасности предприятия.

8. Какая характеристика относится к судебным органам?

а) призваны обеспечить научно-методическую проработку проблем безопасности предприятия;

б) обеспечивают соблюдение законных прав и интересов предприятия;

в) принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования законов;

г) законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

9. Что относится к механизму обеспечения безопасности?

а) принципы обеспечения безопасности;

б) расчет средств и определение методов обеспечения безопасности;

в) причины и факторы зарождения угроз;

г) контроль и оценка процесса реализации концепции.

10. Физическая безопасность объекта – это:

а) деятельность ее должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения ее нормального функционирования;

б) это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, стихийное бедствие, терроризм) и от несанкционированного проникновения на территорию (вандализм, кража, хищение и т.д.);

в) это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке ее функционирования;

г) периметральные охранные системы; системы охранной сигнализации; системы пожарной сигнализации, пожаротушения и оповещения.

4. Практические задания

Кейс 1. Перевод на нижестоящую должность

Ситуация. Одного из руководителей временно переводят на нижестоящую должность специалиста вследствие снижения объема «руководящей» работы и нехватки специалистов. Сотрудник согласен. При таком понижении за данным работником сохраняется прежний оклад – при том, что заработная плата специалиста в два раза ниже.

Вопрос: Вероятна ли подобная ситуация?

Как правильно оформить данное мероприятие при минимальном количестве документов?

Кейс 2. Реструктуризация организации

Ситуация. В организации происходит изменение структуры: формируется новое подразделение (расчетный счет, адрес, руководитель остаются прежними). В соответствии с этим происходят следующие изменения в кадрах: например, сотрудник был руководителем отдела логистики, а становится менеджером по логистике (при этом понижения в должности не происходит, не меняются должностные обязанности, оклад и место работы).

Вопрос: Какую запись при этом необходимо внести в трудовую книжку? Если написать «должность переименована», то работник может это понять, как перевод, т.е. кадровое понижение.

Кейс 3. Штатное расписание или приказ?

Ситуация. Объясните, что важнее в деятельности организации: штатное расписание или приказ о создании структуры предприятия?

Вопрос: В каком порядке вносятся изменения в данные документы (штатное расписание – оргструктура или наоборот)?

Задание 1. Проведите сравнительный анализ основных стратегий обеспечения безопасности организации по кадровому направлению деятельности, заполнив для этого соответствующие графы таблицы.

Возможные варианты стратегического подхода	Характеристики варианта		
	Преимущества	Недостатки	Рекомендации по применению
Вариант 1: Стратегия упреждающего противодействия возможным угрозам			
Вариант 2: Стратегия пассивной защиты от возможных угроз			

Задание 2. Проведите сравнительный анализ основных стратегических подходов к организации службы безопасности, заполнив для этого соответствующие графы таблицы.

Возможные варианты стратегического подхода	Характеристики варианта		
	Преимущества	Недостатки	Рекомендации по применению
Вариант 1: Создание полноценной службы безопасности			
Вариант 2: Минимизация собственной службы безопасности			

Задание 3. Проведите сравнительный анализ основных стратегических подходов к привлечению для обеспечения кадровой безопасности организации сторонних для нее специализированных подрядчиков, заполнив для этого соответствующие графы таблицы.

Возможные варианты стратегического подхода	Характеристики варианта		
	Преимущества	Недостатки	Рекомендации по применению
Вариант 1. Отказ от привлечения сторонних подрядчиков			
Вариант 2. Передача сторонним подрядчикам основных функций по обеспечению безопасности			

4. ОСНОВНЫЕ ФУНКЦИИ СЛУЖБЫ КАДРОВОЙ БЕЗОПАСНОСТИ

4.1. Функции службы безопасности

Среди множества функций службы безопасности выделим наиболее важные внутренние функции:

1. Организация *служебного расследования*.
2. Планирование мероприятий по диагностике и разоблачению выявленных угроз.
3. Специальное *обучение собственных сотрудников и работников других подразделений* по выполнению ими соответствующих действий для сохранения правопорядка.
4. *Выполнение целевых запросов* в организации (налоговые, миграционные службы, психоневрологический диспансер, изучение кредитных историй и т.п.).
5. *Проверка подлинности документов* (паспорта, трудовой книжки).
6. *Сбор характеристик с прошлых мест работы* для проверки трудовых историй (конфликтности), финансовой стабильности (благонадежности), возможно, данные о родственниках, если есть в этом острая необходимость (смотря на какую должность претендует соискатель).

Внешние функции службы безопасности.

Внешние функции службы безопасности (СБ) определяются по видам предоставляемых услуг (применительно к деятельности СБ предприятия):

- обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий;
- консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;

- охрана имущества предприятий;
- защита жизни и здоровья персонала от противоправных посягательств;
- сбор информации для проведения деловых переговоров;
- изучение криминальных аспектов рынка;
- выявление ненадежных деловых партнеров**;**
- сбор сведений по гражданским делам;
- розыск без вести пропавших сотрудников предприятия;
- выявление некредитоспособных партнеров;
- поиск утраченного имущества предприятия;
- расследование фактов неправомерного использования товарных (фирменных) знаков предприятия;
- сбор информации о лицах, заключавших с предприятием контракты;
- расследование фактов разглашения коммерческой тайны предприятия;
- сбор сведений по уголовным делам;
- установление обстоятельств недобросовестной конкуренции со стороны других предприятий;
- проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Функции службы конкурентной (бизнес) разведки.

Для обеспечения экономического благополучия организации необходимо своевременно выявлять кадровые угрозы и адекватно реагировать на них. Для этого в структуре организации должна быть организована независимая информационно-аналитическая служба безопасности или служба конкурентной (бизнес) разведки. В её задачи входит сбор и предоставление руководителям соответствующих структур полной и актуальной бизнес-информации. Благодаря доступности такой информации принимаемые управленческие решения будут своевременными и оптимальными. В задачи сервиса входит:

- сбор, анализ и систематизация данных о бизнес-среде и кадровых угрозах внутри компании, т.е. выявление внешних и внутренних угроз для функционирования организации;

– выявление рисков и подготовка рекомендаций по вопросам правовой защиты от незаконных кадровых угроз;
– работа с финансовыми документами в инвестиционной сфере в России и за рубежом;
– применение методов конкурентной разведки при сборе информации о конкурирующих фирмах (анализ процессов и тенденций их развития, а также составление психологического портрета их лидеров);
– разработка концепции экономической безопасности организации, подготовка стратегического плана развития организации;
– разработка и реализация индивидуальных организационных, управленческих и финансовых проектов и технологий.

4.2. Сбор сведений по уголовным делам

В своей практической деятельности служба безопасности не должна выходить за пределы своих полномочий.

Уголовные дела, к расследованию которых подключается служба безопасности, условно можно разделить на две группы:

1. *Преступления против собственности учредителя* (кражи, грабежи, мелкие хищения, поджоги и т.д.).

2. *Преступления против персонала предприятия*. Обязательным условием сбора сведений о них является их связь с деятельностью предприятия-учредителя.

К расследованию уголовных дел, по которым работник предприятия является обвиняемым в совершении преступлений, возможно подключение сотрудников службы безопасности. Однако, делать это необходимо *только по указанию или с разрешения руководителя фирмы*.

Приведём пример. Кража личного имущества у сотрудника фирмы сама по себе *не обязывает* сотрудников

службы безопасности подключаться к расследованию этого преступления. Однако, *если среди этого имущества окажутся документы предприятия-учредителя*, то будет проводиться расследование.

Закон допускает сбор сведений по совершенному преступлению *только после вынесения постановления о возбуждении уголовного дела.*

На практике часто появляется значительный *отрезок времени (иногда в несколько суток) между событием* преступления, ставшим известным правоохранительным органам *и возбуждением уголовного дела.*

В таких случаях служба безопасности *не должна дожидаться возбуждения уголовного дела, а сразу приступать* к сбору сведений по совершенному преступлению. Одновременно следует направить в *правоохранительный орган,* производящий проверку, *письменное уведомление*.

4.3. Расследование фактов разглашения коммерческой тайны предприятия

Рост корпоративной преступности ведет к росту коррупции государственных служащих; росту уровня безработицы; уклонению от уплаты налогов; монополизации ряда сегментов экономики и снижению конкурентоспособности, что приводит к ухудшению инвестиционного климата и активизации процессов отмывания денег. В России проблема противодействия корпоративной преступности стоит не менее остро, чем в остальном мире. В настоящее время понятие корпоративной преступности довольно расплывчато и охватывает широкий спектр преступных действий, от мошенничества до коррупции. Сегодня наблюдается активный рост корпоративной преступности. Ущерб от экономических преступлений связан с финансовыми потерями и потерей активов, и компании также несут расходы на проведение расследований.

Среди лиц, совершивших экономические преступления, основная доля приходится на сотрудников компании (увеличилось с 46% в 2016 году до 52% в 2018 году), а количество руководителей

высшего звена среди злоумышленников тоже растет. Таким образом, доля руководителей высшего звена среди домашних правонарушителей увеличилась с 15% до 39% (PWC, 2018).

Увеличение количества новых видов преступной деятельности, которые можно отнести к категории корпоративных, во многом связано не только с деятельностью и мотивацией руководителей, но и с более крупными факторами, такими как недостатки в правовом регулировании процессов управления, использование материальных и иные ресурсов руководителей, недостаточный контроль со стороны правоохранительных органов и несовершенное уголовное законодательство, регулирующее ответственность за корпоративные преступления.

Коммерческая тайна – любая конфиденциальная информация, представляющая ценность для предприятия:

- *в достижении преимуществ* над конкурентами;
- *извлечения прибыли*.

Коммерческой тайной не является информация, относящаяся к государственным секретам, или специально охраняемая собственником (владельцем) – управленческая, производственная, научно-техническая, финансовая, торговая и иная деловая информация. Она становится коммерческой тайной только:

- *после утверждения руководством предприятия* «Перечня сведений, составляющих коммерческую тайну предприятия» и
- *объявления его под расписку всем причастным* к ней сотрудникам.

В Постановлении РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» (ред. от 03.10.2002) содержится разъяснение, какая информация не может считаться коммерческой тайной. Таким образом, не могут составлять коммерческую тайну:

- учредительные документы (разрешение о создании предприятия или договор учредителей) и Устав;
- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);
- документы о платежеспособности;

- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;
- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежах;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения;
- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Многие предприятия в целях развития своего бизнеса, заинтересованы сбором данных у конкурирующих с ними предприятий. В связи с этим, специальные службы и отделы занимаются конкурентной разведкой либо промышленным шпионажем. «Разведка» – это «сбор информации о противнике или конкуренте для обеспечения их безопасности и получения преимуществ». Она может использовать как легальные методы сбора информации (например, сбор и анализ данных из открытых источников, прослушивание радиоканалов из-за границы, наблюдение с использованием разведывательных спутников), так и незаконные операции, подпадающие под понятие «шпионаж» или «кража информации».

Конкурентная разведка уместна и законна. Разведка собирает информацию и трансформирует её в новые направления и проекты для эффективного развития организации. В отличие от конкурентной разведки, промышленный шпионаж использует методы незаконного тайного хищения информации с использованием специального оборудования (технических устройств) или персонального компьютера (Кравцов, Желнов, 2014).

Данные, хранящиеся на сервере или в «облаке», по электронной почте, при телефонных разговорах, т.е. любая информация и на любом носителе, становятся доступными.

Для защиты бизнес-сектора от промышленных шпионов необходимы серьезные вложения в технические средства защиты информации: приобретение видеокамер, диктофонов, так называемых «глушилок», защищающих конфиденциальность информации. В Японии компании тратят на такое оборудование почти 200 миллионов долларов в год, а американские корпорации тратят до 0,5 миллиарда долларов. В России компании используют человеческий фактор вместо того, чтобы покупать дорогое шпионское оборудование. Тем не менее, объем внутреннего рынка средств защиты информации, по некоторым данным, составляет около 150 млн долларов (HR Director, 2015). Полученная информация, составляющая коммерческую, налоговую или банковскую тайну, может быть раскрыта или использована незаконно. В России промышленный шпионаж преследуется по закону (Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственных секретах»; Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»; Уголовный кодекс Российской Федерации; Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»; Федеральный закон от 26.07.2006 г. № 135-ФЗ «О защите конкуренции»; Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»). В частности, ст. 183 Уголовного кодекса предусматривает лишение свободы на срок до десяти лет за использование промышленного шпионажа.

4.4. Направления и меры по противодействию кадровым угрозам

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

Прежде всего, необходимо провести комплекс мероприятий по управлению кадровой безопасностью, начиная с формирования сильной кадровой политики. Чтобы защитить вашу организацию от потенциальных злоумышленников, вам нужно поставить первое

препятствие в процессе отбора при приеме на работу. Для этого требуются высокопрофессиональные рекрутеры, способные провести качественную экспресс-диагностику всеми доступными методами оценки как в работе с соискателем, так и с предоставленной ему документацией. Важно перепроверить информацию. При работе с резюме используйте приемы «поиск узких мест», «чтение между строк», при необходимости проведите «контент-анализ». При проведении интервью используйте приемы «если не секрет», «перехват», задавайте уточняющие вопросы – UCQ (универсальный уточняющий вопрос – «Пожалуйста, поясните, что вы имеете в виду, когда говорите ...») и, главное правило, не продумывайте для соискателя то, что он хочет сказать!

Еще одно направление нейтрализации кадровых угроз для обеспечения безопасности организации – это работа с существующим персоналом. И в этом направлении необходимо обеспечить проведение качественного инструктажа, подкрепленного регулярным мониторингом эффективности. Также необходимо регулярно информировать персонал о понимании того, какая информация не представляет угрозы безопасности, а какая является строго конфиденциальной и не подлежит разглашению. Вплоть до подписания документов о неразглашении коммерческой тайны. Именно на этом этапе важна четкая работа службы безопасности.

Хорошо продуманная система мотивации персонала может сыграть свою роль. При этом важно добиться не только полного удовлетворения сотрудников работой и результатами работы (читай – справедливой оплаты труда), но и дать возможность открыто «высказаться» (система обратной связи), не опасаясь за свое положение и угрозы увольнения. Потому что всегда есть «доброжелатель» («случайный собеседник»), готовый выслушать все секреты и использовать полученную информацию для развала организации.

Поскольку сегодня электронный документооборот осуществляется повсеместно, создаются электронные хранилища с базами данных (необходимые для успешной и эффективной работы предприятия), важным направлением обеспечения безопасности организации в части хранения и передачи информации является формирование мощного ИТ-сервиса, способного противостоять разного рода техническим сбоям и хакерским атакам. В октябре

2018 года Корпорация по управлению доменными именами и IP-адресами (ICANN) осуществила первую в истории замену криптографических ключей, защищающих систему доменных имен (DNS) в Интернете (RG.RU, 2018). Этот ключ для подписи (KSK) необходим любому пользователю Интернета. Он повышает уровень информационной безопасности. А в организациях в рамках обеспечения системы безопасности также рекомендуется время от времени с определенной регулярностью контролировать смену паролей на персональных компьютерах специалистов и сотрудников.

Нельзя игнорировать правовой аспект обеспечения безопасности организации. Важно иметь в структуре организации не только юридический отдел, но и формировать правовую грамотность специалистов и руководителей, способных предвидеть и устранять потенциальные угрозы кадровой безопасности на своем уровне. Примером может быть – неправильно начисленная заработная плата; ошибки в исполнении договоров при приеме на работу (прежде всего терминологические) и при увольнении сотрудников; ошибки в ведении финансовых документов; ошибки в принятии управленческих решений, приводящие к конфликту с персоналом и т.д.

Механизм расследования преступлений представим на рис. 6.

Технологии также используются для отслеживания экономических преступлений. В России все больше и больше компаний используют технологии в качестве основного инструмента для выявления экономических преступлений, чем в мире в целом, особенно в таких сферах как выявление мошенничества, противодействие взяточничеству и коррупции, а также комплексная проверка надежности деловых партнеров.

Несомненно, киберпреступники берут на вооружение и технологии. В условиях пандемии, когда бизнес перешел в онлайн, а все коммуникации осуществляются через корпоративные сети, количество кибератак на бизнес-инфраструктуру неуклонно многократно увеличивается. По данным Group IB (2020), в 2019 году многие операторы программ-вымогателей отошли от атак на обычных пользователей и переключили свое внимание на компании из различных отраслей и государственные органы. Нападения на эти жертвы приносят большую пользу злоумышленникам. Обычно существуют следующие начальные векторы атаки:

Рис. 6. Механизм расследования преступлений

- вредоносные электронные письма;
- получение доступа к внутренней сети путем компрометации данных аутентификации;
- работа общедоступных приложений, в том числе связанных с VPN.

После первоначального компромисса; многие криптографические операторы сначала пытаются получить более высокие права доступа, а затем пытаются получить доступ к другим учетным записям с помощью различного программного обеспечения. Количество проданных доступов к корпоративным сетям увеличивается из года в год, но основной пик продаж пришелся на 2020 год, рост в 2,6 раза. Ожидается появление специализированных торговых площадок для размещения лотов с доступом к корпоративным сетям, что может привести к еще большему увеличению инцидентов.

Официальные данные также подтверждают эти тенденции. В первом полугодии 2020 года количество преступлений в сфере информационных технологий в России увеличилось на 91,7% по сравнению с аналогичным периодом прошлого года, а доля этих

противоправных действий в общей структуре преступности достигла 22,3% (МВД России, 2020).

В заявлении SEC США (2018) отмечается, что компании сталкиваются с постоянно меняющимся ландшафтом угроз кибербезопасности, в котором хакеры используют сложный набор инструментов для проведения кибератак, включая использование украденных данных доступа, вредоносных программ, программ-вымогателей, отлова и структурированных запросов. атаки языка ввода и распределенные атаки отказа в обслуживании, среди прочего (Комиссия по ценным бумагам и биржам (SEC), 2018). Цели кибератак широко варьируются и могут включать в себя кражу или уничтожение финансовых активов, интеллектуальной собственности или другой конфиденциальной информации, принадлежащей компаниям, их клиентам или их деловым партнерам.

Кибератаки также могут быть направлены на нарушение деятельности публичных компаний или их деловых партнеров. В целях защиты интересов инвесторов SEC потребовала от публичных компаний информировать инвесторов о значительных рисках и инцидентах в области кибербезопасности.

Требование является обязательным не только для компаний, подвергшихся кибератакам, но и для тех, кто подвержен значительным рискам кибербезопасности, но, возможно, еще не стал целью кибератак. Механизм защиты коммерческой тайны на предприятии представлен на рис. 7.

Каковы основные каналы утечки информации? Это:

- человек;
- документ;
- изделие-процесс.

По данным каналам утечки информации выделяют и направления расследования по факту разглашения коммерческой тайны. Зная источники, можно рассмотреть и механизм защиты коммерческой тайны на предприятии.

В рамках действующего механизма защиты информации следует уделить внимание пакету документов:

- Постановление РСФСР от 05.12.91 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;
- Положение по защите коммерческой тайны организации;

Рис. 7. Механизм защиты коммерческой тайны на предприятии

- Положение о конфиденциальном производстве в организации;
- Положение о службе безопасности организации;
- Положение о защите информации в отношении с контрагентами;
- Инструкция по защите конфиденциальной информации в информационной системе организации;
- Обязательство о неразглашении коммерческой тайны организации;
- Перечень сведений, составляющих коммерческую тайну.

По мере необходимости могут быть составлены и другие документы.

4.5. Меры предотвращения рисков

Трудоустройство граждан.

С лицами, кто претендует на должность, заключают один из видов контрактов:

– *коммерческий* (документ, представляющий собой договор поставки товаров или предоставления услуг);
– *трудовой* (вид трудового договора, заключающегося в письменной форме со всеми постоянными или временными работниками).

В контракте в письменной форме должны быть оговорены договорные условия с сотрудником:

– согласие лица на сбор информации о его биографических и других данных, характеризующих личность;
– особо оговорить, что такого рода сбор информации проводится как до вступления контракта в силу (например, во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Содержание информации в контракте о личности проверяемого:

– преступления и административные проступки, совершенные им в прошлом;
– судебные процессы по гражданским делам, в которых он выступал в качестве истца или ответчика;
– качество исполнения ранее заключаемых договоров с другими партнерами;
– участие в организациях, дискриминирующих по признакам пола, расы, цвета кожи, убеждениям, религиозной и национальной принадлежности;
– жизнь не по средствам;
– наличие значительных финансовых накоплений сомнительного происхождения;
– систематические посещения проверяемого лицами, не имеющими отношения к его служебным обязанностям;
– факты отказа от использования очередного отпуска;
– результаты различных тестов;
– семейные проблемы;
– долги и займы и т.д.;
– болезни, которые он перенес ранее;
– материальное положение;

- случаи увольнения с работы по отрицательным мотивам, не нашедшие отражение в трудовой книжке;
- аморальные проступки (пьянство, внебрачные связи, наркотики и т.д.);
- суждения бывших сослуживцев и руководителей о его профессиональных и моральных качествах;
- необоснованный и нелогичный отказ от продвижения по службе, перевода на новое место работы;
- жалобы клиентов и других лиц, контактирующих с проверяемым;
- прогулы и частые отвлечения от выполнения служебных обязанностей;
- задержки по надуманным предлогам на работе после окончания рабочего дня.

4.6. Розыск без вести пропавшего сотрудника

Деятельность службы безопасности по розыску без вести пропавшего сотрудника – это комплекс мероприятий, осуществляемых при тесном взаимодействии с органами внутренних дел с целью:

- установления фактических обстоятельств его исчезновения;
- фактического местонахождения.

Без вести пропавшим считается лицо, исчезнувшее внезапно, без видимых к тому причин, местонахождение и судьба которого остается неизвестной.

Группы случаев безвестного исчезновения сотрудников:

1. *Связанные с криминальным характером происшедшего* (убийство, наезд транспорта со смертельным исходом и т.д.).

2. *Некриминальное лишение жизни пропавшего* (самоубийство, утопление и т.д.).

3. *Объективно не зависящие от сознания и воли сотрудников и не носящие криминальный характер* (уход из дома вследствие психического заболевания, административный арест и т.д.).

4. *Проблемы личного и служебного характера* (семейные неурядицы, ссора с начальством и т.д.).

Сотрудники службы безопасности подключаются к розыску без вести пропавшего сотрудника *только если есть основания предполагать, что его отсутствие на работе приведет (может привести) к реальному или потенциальному ущербу предприятию.*

4.7. Как распознать неблагонадежного партнёра

Некредитоспособным признается тот партнер, у которого для получения кредита нет предпосылок, подтверждающих способность возвратить его.

Характеристики некредитоспособного партнера:

1. Неаккуратность при расчетах по ранее полученным кредитам.
2. Ухудшение текущего финансового положения.
3. Неспособность при необходимости мобилизовать денежные средства из различных источников.
4. Обналичивание денежных средств в объемах, превышающих размеры фонда зарплаты.
5. Удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты.
6. Совершение операций с банковскими документами необеспеченными кредитными ресурсами.
7. Нецелевое использование кредитных средств или их получение по фиктивным документам.
8. Попытка оттянуть выплату денежных средств партнеру при добросовестном выполнении им условий контракта и т.д.

Служба безопасности обязана выявлять некредитоспособных партнеров как до заключения, так и в процессе реализации договора и своевременно информировать об этом руководство предприятия.

Ненадёжность делового партнёра определяется:

1. Большим количеством сорванных по его вине сделок с другими фирмами.
2. Несвоевременным и некачественным выполнением условий заключенных договоров.
3. Значительным количеством в фирме ранее судимых лиц.

4. Фактами ведения против предприятия-учредителя экономического шпионажа.

5. Отсутствием доверия потребителей.

6. Испорченной репутацией среди деловых кругов.

7. Нерегулярной и ненадежной поставкой сырья и товаров.

8. Умышленным затягиванием деловых переговоров.

9. Предъявлением к нему значительного количества судебных исков.

10. Наличием большого долга.

11. Непрочной позицией на рынке.

12. Использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера.

13. Неуважительным отношением к авторскому или патентному праву.

Известно, что в рамках гражданского производства судами рассматриваются:

- споры о гражданском праве, затрагивающем права и законные интересы юридического лица (предприятия);
- по жалобе на действия административных органов или должностных лиц, совершенные с нарушением их полномочий;
- дела об установлении фактов, имеющих юридическое значение, рассматриваемые и разрешаемые судом.

Необходимость в сборе информации сотрудниками службы безопасности обычно возникает в следующих случаях:

1. Выявления свидетелей и документов.

2. Проверки достоверности информации участников процесса и подлинности доказательств, представленных на суде.

3. Возникновения необходимости проверки наличия основания для отвода в рассматрении дела.

4. Оказания помощи суду в установлении фактического местонахождения участников процесса.

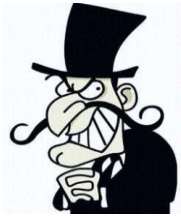
5. Выявления лиц, оскорбляющих или оклеветавших руководителей предприятия-учредителя.

6. Поиска утаиваемого от суда имущества процессуального противника, необходимого для погашения материального ущерба.

7. Необходимости выявления среди свидетелей лиц, которые в силу своих физических или психических недостатков не способны правильно восприинимать факты или давать о них правильные показания и т.д.

ВОПРОСЫ И ЗАДАНИЯ

1. Вопросы для обсуждения



1. Охарактеризуйте понятие и виды кадровых рисков
2. Раскройте основные способы и процедуры выявление кадровых рисков.
3. Какие вы знаете методы воздействия на кадровые риски?
4. Каким образом можно оценить эффективность управления кадровыми рисками?
5. Объясните, как вы понимаете следующие признаки агентурного внедрения в компанию через трудоустройство:

- кандидат часто менял места работы, жительства, зачастую каждые 3 ÷ 6 месяцев;
- необъясняемые «провалы» (нестыковки) в биографии;
- несоответствие образования и должностей, которые занимал кандидат;
- сокрытие образования, навыков или мест работы, имеющихся наград;
- иногда – работа в организациях, конкурирующих с вашей,
- наличие судимостей;
- работа в несуществующих организациях;
- излишне широкий круг «служебных» интересов и навыков;
- работа в «органах»;
- служба в армии (в т.ч. в различных спецвойсках), в охране (детективом) или на должностях, предполагающих активные контакты с правоохранительными органами или спецслужбами;
- кандидат имеет хорошее здоровье;

- претендует на ключевую должность, но заметно ниже своих возможностей, отказывается от других позиций, даже с лучшими условиями;
- не может сразу принять какого-либо решения («мне нужно подумать, посоветоваться»);
- у кандидата отсутствуют вредные привычки;
- подходит «под агента» (в т.ч. в силу свойств характера – настойчивости, харизматичности, наблюдательности, замкнутости и «незаметности», умения говорить много и ни о чем и т.п.);
- имеет широкие связи в различных сферах.

2. Подготовьте доклад

1. Кибертерроризм и защита персональных данных.
2. Обеспечение кадровой безопасности методом эгоскопии.
3. «Чипирование» сотрудников.
4. Кадровая безопасность и испытательный срок.
5. Кадровая безопасность и сценарии массового увольнения: «открытый» и «закрытый».
6. Безопасное сокращение штата.
7. Управление кадровой безопасностью организации в период массовых сокращений.
8. Соглашение о не конкуренции (не вступление в трудовые отношения с конкурирующими компаниями в течение 6 месяцев после расторжения договора).
9. Режим секретности – механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты. Санкции за неправомерное получение и (или) распространение этих сведений.
10. Коммерческая тайна: состав и объем сведений, методы защиты. Режим конфиденциальности и коммерческой тайны.
11. Особенности и последствия конкурентной разведки, меры противодействия.
12. Кадровая безопасность предприятия и «защитные» пункты в договоре.
13. Кадровая безопасность и целевая профессионально-психологическая подготовка сотрудников СБ.

14. Кадровая безопасность и увольнение сотрудников «по статье».

15. Заключительные этапы и процедуры отбора персонала. Матрица соответствия.

16. Внешние и внутренние угрозы кадровой безопасности, меры противодействия им.

17. Контроль персонала со стороны Службы безопасности в организации.

18. Вербовка: перечень таких рисковых должностей наиболее подверженных вербовке.

19. Хищение имущества предприятия, меры и средства противодействия.

20. Шантаж компетентностью (я – незаменимый работник), меры и средства противодействия.

21. Планирование персонала с точки зрения кадровой безопасности.

22. Шантаж полномочиями (концентрация полномочий в одних руках), меры и средства противодействия.

23. Торговля коммерческими секретами, меры и средства противодействия.

24. Дисциплинарные нарушения, меры и средства противодействия.

25. Получение заработной платы за невыполняемую работу, меры и средства противодействия.

26. Умышленная порча и уничтожение имущества предприятия, меры и средства противодействия.

27. Конкурентная разведка: особенности, организация, последствия для организации.

28. Бизнес – разведка как метод профилактики покушений.

29. Рейдерский захват и кадровая безопасность, меры и средства противодействия. Формирование «тревожного пакета». Защита инсайдерской информации. Создание детективно-маркетинговых служб.

3. Выполните тестовое задание

1. Стратегия безопасности – это…?

а) потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности;

б) совокупность наиболее значимых решений, направленных на достижение приемлемого уровня безопасности функционирования предприятия;

в) комплексное воздействие на потенциальные и реальные угрозы, позволяющее успешно функционировать в нестабильных условиях внешней и внутренней среды.

2. Что является главным критерием надежности и эффективности кадровой безопасности?

а) соответствие фундаментальным законам;

б) простота, экономичность формы;

в) отсутствие или наличие нанесенного организации материального или морального ущерба;

г) некое соглашение, конвенция.

3. Назовите общие ориентиры для действия и принятия решений при выявлении угроз и обеспечении безопасности организации:

а) получение достоверной информации для выявления закономерностей развития явлений и процессов;

б) сохранение и наращивание ресурсного потенциала;

в) обеспечение безопасности всех сотрудников организации;

г) способность к устойчивости и развитию в условиях внутренних и внешних угроз;

д) профессионализм и специализация персонала.

4. Какие цели ставит кадровая безопасность?

а) повышение конкурентоспособности производимой продукции;

б) обеспечение защиты технологических процессов;

в) укрепление дисциплины труда и повышение его производительности;

г) своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых выраба-

тываются соответствующие меры по недопущению возникновения реальных угроз.

5. Что такое угроза безопасности?

а) событие, действие или явление, финансовые, материальные ценности и информация, которые посредством воздействия на персонал, могут привести к нанесению вреда здоровью работников и ущербу организации, нарушению или приостановлению ее деятельности;

б) официально утверждённый документ, в котором отражена система взглядов, требований, условий организации мер безопасности персонала и собственности предприятия;

в) свод основных документов, касающихся политики, стратегии, основных направлений, средств и методов обеспечения безопасности;

г) комплекс организационно-управленческих, экономических, правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и её персонала.

6. Как служба безопасности определяет полномочия?

а) исходя из установок главного бухгалтера;

б) исходя из установок организации;

в) исходя из установок учредителя;

г) нет верного ответа.

7. Без вести пропавшим считается лицо, исчезнувшее внезапно, без видимых к тому причин, местонахождение и судьба которого остается неизвестной. На какие четыре группы можно разделить все случаи безвестного исчезновения сотрудников? (множественный выбор)

а) связанные с криминальным характером происшедшего (убийство, наезд транспорта со смертельным исходом и т.д.);

б) обусловленные некриминальным лишением жизни пропавшего (самоубийство, утопление и т.д.);

в) удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты;

г) объективно не зависящие от сознания и воли сотрудников и не носящие криминальный характер (уход из дома вследствии психического заболевания, административный арест и т.д.);

д) вызванные проблемами личного и служебного характера (семейные неурядицы, ссора с начальством и т.д.).

8. К каким уголовным делам есть возможность подключить службу безопасности:

а) по которым работник является обвиняемым в преступлении, но только с указания или разрешения руководства;

б) преступления против собственности учредителя;

в) преступления против персонала, против собственности учредителя;

г) все ответы верны.

9. Какой отрезок времени использует служба безопасности для устранения угрозы безопасности?

а) между совершением преступления и вынесением постановления судом;

б) после завершения преступления;

в) до совершения преступления;

г) верного ответа нет.

10. Что должна направлять служба безопасности в правоохранительные органы?

а) электронное уведомление;

б) письменное уведомление;

в) письменное и электронное уведомление;

г) лично доложить о происшествии.

4. Практические задания

Кейс 1. «Я люблю свою компанию»

Ситуация. Иногда руководство компании не учитывает, что отсутствие представления о целях компании, стратегических задачах, стоящих перед ней, ее организационной структуре и деятельности каждого подразделения может быть сильным демотивирующим фактором.

Сотрудник в такой ситуации чувствует себя отстраненным, неуверенным, поскольку не обладает информацией о векторе развития компании.

Задание:

Как улучшить психологический климат в коллективе, повысить мотивацию и каждому сотруднику ощутить свою значимость для компании? Предложите комплекс мероприятий, которые помогут сотрудникам ощутить себя командой с общими целями.

Кейс 2. Разглашение информации

Чтобы выполнить важный проект в срок, некоторые работники трудятся дома в выходные. Необходимую информацию и документы они копируют на флешки или отправляют на личную электронную почту. Однако такое усердие может обернуться против работника. В случае конфликта компания может заявить, что работник разгласил ее коммерческую тайну, отправив информацию по почте. Такая ситуация произошла с Екатериной Ивановой, работницей крупной российской IT-компании (ФИО работника изменены).

С января текущего года она трудилась на должности ведущего специалиста отдела МСФО. Через некоторое время у руководителя возникли претензии к работе Екатерины. По его мнению, она не справлялась с обязанностями. Руководитель начал намекать, что Екатерине пора увольняться. Она отказалась, тогда с Екатериной решили расстаться «по статье».

В компании сложилась такая практика, когда сотрудники брали работу на дом. Аналогично поступала и Екатерина, если нужно было завершить срочный проект. Однажды она отправила на личную почту несколько писем с документами, чтобы поработать в выходные дни. Об этом узнал руководитель. Он инициировал служебное расследование, по итогам которого Екатерину уволили по подп. «в» п. 6 ч. 1 ст. 81 ТК РФ. Ее обвинили в том, что она разгласила корпоративные секреты. Екатерина оспорила увольнение в судебном порядке.

Работницу уволили за разглашение информации компании. Причина – она отправила на личный e-mail служебные документы.

ПОЗИЦИЯ РАБОТНИЦЫ*: Доступ к почте есть только у неё.*

В суде Екатерина оперировала процедурными нарушениями при увольнении.

Во-первых, она не разглашала секреты компании третьим лицам. Она лишь отправила документы на личную почту, чтобы поработать в выходные. Пароль от почты есть только у нее. У других лиц доступа нет. Поэтому и нет факта разглашения конфиденциальной информации.

Во-вторых, у нее не запрашивали объяснения по факту отправки письма с конфиденциальной информацией компании. Запросы касались только писем с учредительными документами. Получается, что работодатель нарушил процедуру применения дисциплинарного взыскания.

Более того, учредительные документы находятся в свободном доступе. Поэтому информацию из них разгласить нельзя.

На основании этих доводов Екатерина просила суд признать ее увольнение незаконным, обязать компанию выплатить заработок за вынужденный прогул и компенсировать моральный вред.

ПОЗИЦИЯ КОМПАНИИ: *Работница передала секреты третьим лицам*.

Основной задачей юристов компании было доказать, что работница разгласила секреты компании. Одного лишь факта отправки документов на личный е-майл было недостаточно. Предстояло обосновать, что секреты компании стали известны третьим лицам. Юристы использовали следующие доводы.

Работница оформила бесплатную почту на почтовом сервисе Google.com. Юристы обратили внимание суда на пользовательское соглашение этого сервиса. Оно предусматривает, что пользователь передает Google лицензию на использование материалов, которые пересылает в письмах. Следовательно, между Екатериной и Google действует лицензионный договор, заключенный в упрощенном порядке (ч. 5 ст. 1286 ГК РФ).

Таким образом, после отправки сообщения на личную почту третьи лица получили доступ к конфиденциальной информации компании. Поэтому уволили Екатерину по подп. «в» п. 6 ч. 1 ст. 81 ТК РФ правомерно. Исходя из этого, юристы просили суд отказать работнице в удовлетворении иска.

Вопрос:

Использование бесплатной почты – повод ли для увольнения?

Справка:

ПОЗИЦИЯ СУДА: *Увольнение правомерно***.**

Суд поддержал юристов компании. Он согласился, что работница не имела права отправлять секреты компании на личную электронную почту. В результате таких действий третьи лица получили доступ к конфиденциальной информации компании.

В итоге суд признал увольнение законным. При этом он оставил без внимания довод работницы, что компания не запрашивала у нее объяснения по факту отправки конфиденциальной информации на личную почту. Работница пыталась обжаловать решение в апелляцию, но безрезультатно.

Кейс 3. Увольнение по соглашению сторон

Ситуация

Широкую огласку в СМИ получил конфликт между сотрудниками и руководством издательского дома B2B Media (деловые журналы «Финансовый директор», «Коммерческий директор», «Индустрия рекламы», «HR Менеджмент», интернет-ресурсы Executive.ru, E-perspektiva.ru, Hrm.ru).

В конце 2021 года многим сотрудникам было предложено написать заявления об увольнении по соглашению сторон в связи с планируемым закрытием проектов издательского дома. Никаких компенсаций, кроме заработной платы, выплата которой задерживалась с ноября, компания не предлагала.

Сотрудники отказались писать заявления и в середине января 2022 года подали иски о выплате задолженности по заработной плате в Тверской районный суд города Москвы.

В процессе борьбы сотрудники использовали и другие методы:

- написали открытое письмо в Благотворительный фонд В. Потанина, выступавший партнером B2B Media по одному из онлайн-проектов;
- разместили в Интернете информацию о том, что происходит в компании;
- открыли специальный блог, в котором отражали хронику событий;
- давали ссылки на публикации об этой истории в различных СМИ;
- устроили пикет.

Вопрос:
Как разрешить ситуацию?
Какое решение должен принять суд?

Справка:
ПОЗИЦИЯ СУДА: В начале февраля суд удовлетворил иски, обязав издательский дом выплатить задолженность по заработной плате, пени за просрочку выплаты и компенсацию морального вреда.

7 февраля в компании был официально запущен процесс сокращения, согласно которому сотрудники должны были числиться в штате и получать зарплату до мая 2022 года (в приказе о сокращении был также объявлен официальный простой: сотрудники на работу не ходили и поэтому с февраля по май получали не 100% зарплаты, а 2/3).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Group IB (2020) Тенденции преступности в сфере высоких технологий 2020/2021. – [Электронный ресурс]. – Режим доступа: https://securityaffairs.co/wordpress/111434/cyber-crime/hi-tech-crime-trends.html
2. Makhmudova I.N., Ilyukhina L.A., Bogatyryova I.V. (2018) Personnel Safety In The System Of Economic Security And Personnel Management. // In V. Mantulenko (Ed). International Scientific Conference «Global Challenges and Prospects of the Modern Economic Development». The European Proceedings of Social &Behavioural Sciences, 57 (pp. 1859-1865). London: Future Academy DOI: https://dx.doi.org/10.15405/epsbs.2019.03.189.
3. McKinsey (2020). Исследование киберустойчивости IIF / McKinsey. Состояние кибербезопасности индустрии финансовых услуг (2020). – [Электронный ресурс]. – Режим доступа: ttps://www.mckinsey.com.
4. PwC (2018) Борьба с мошенничеством: какие меры принимают компании? Российский обзор экономических преступлений за 2018 год? – [Электронный ресурс]. – Режим доступа: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf.
5. PwC (2020 г.). 47% компаний мира столкнулись с мошенничеством за последние два года. – [Электронный ресурс]. – Режим доступа: https://www.eg-online.ru/news/420448/
6. PwC (2020 г.). Глобальный обзор экономических преступлений и мошенничества, подготовленный PwC, 2020 г. Борьба с мошенничеством: бесконечная битва. – [Электронный ресурс]. – Режим доступа: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.
7. Абдулла, В.Н. Влияние корпоративного управления и управления людьми на корпоративные финансовые преступления: концептуальный документ / В.Н. Абдулла, Р. Саид // Изменения в корпоративном управлении и ответственности. – 2018. – № 13. – С. 193–215.

8. Алалехто, Т., Ларссон, Д. (2012). Vem är den ekonomiske brottslingen?: En jämförelse mellan länder och brottstyper. Социологиск Форскнинг, 49 (1), 25–44.
9. Альгин, А.П. Риск: сущность, функции, детерминация, разновидности, методы оценки / А.П. Альгин. – Москва, 1990.
10. Альгин, А.П. Риск и его роль в общественной жизни / А.П. Альгин. – Москва: Мысль, 1989.
11. Ахим, М. В., Борлеа, С. Н. (2020) Экономическая и финансовая преступность. Исследования организованной преступности, 20. Springer.
12. Бейли, Т., Маруяма А. и Уолланс Д. (2020) Угроза энергетическому сектору: как устранить уязвимости кибербезопасности. – [Электронный ресурс]. – Режим доступа: https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities
13. Бойко, В.В. Энергия эмоций в общении: взгляд на себя и других / В.В. Бойко. – Москва: Информационно-издательский дом «Филинъ», 1996. – 472 с.
14. Борзунов, А.А. К вопросу о сущности понятия «кадровый риск» / А.А. Борзунов // Экономика и современный менеджмент: теория и практика: сб. статей по материалам XL междунар. науч.-практ. конф. – Новосибирск: СибАК, 2014.
15. Вербовка: альтернативный вариант подбора персонала. – [Электронный ресурс]. – Режим доступа: https://hr-portal.ru/print/94742.
16. Генеральный директор (2017). Количество утечек данных от российских компаний выросло на 80% в 2016 году. – [Электронный ресурс]. – Режим доступа: https://www.gd.ru/news/7175-qqn-17-m3-23-03-2017-chislo-utechek-dannyh-iz-rossiyskih-kompaniy-vyroslo-na-80-v-2016-godu?utm_source=www.gd.ru%20%20&utm_medium=refer&utm_campaign=Rubrcontentblock_news.
17. Готшалк, П. (2020). Корпоративные меры реагирования на финансовые преступления Springer Briefs по криминологии. Springer.
18. Грир, Би Джей (2017). Рост киберпреступности в США. – [Электронный ресурс]. – Режим доступа: https://www.researchgate.

net/publication/320781855_The_Growth_of_Cybercrime_in_the_United_States.
19. Гупта, ДК (2020). Растущие потребности в судебном аудите корпоративного и банковского мошенничества в Индии. – [Электронный ресурс]. – Режим доступа: https://ssrn.com/ abstract=3624001.
20. Директор по персоналу (2015). Противодействие промышленному шпионажу. – [Электронный ресурс]. – Режим доступа: https://www.hr-director.ru/article/65692-qqq-15-m9-protivodeystvie-promyshlennomu-shpionaju.
21. Ежова, О.Н. Психическое здоровье сотрудников ФСИН и методы его поддержания : учебное пособие / О.Н. Ежова. – Самара: Самарский юридический институт ФСИН России, 2008. – 135 с.
22. Как выявлять закрепление злоумышленников в сети? – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise.
23. 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).
24. Кленова, М.А. Риск и расчет в структуре ценностных ориентаций // Альманах современной науки и образования. – 2010. – № 11–1. – С. 80–83. – [Электронный ресурс]. – Режим доступа: https://www.gramota.net/articles/issn_1993-5552_2010_11-1_27.pdf .
25. Комиссия по ценным бумагам и биржам (SEC) (2018). Заявление комиссии и руководство по раскрытию информации о кибербезопасности публичных компаний. – [Электронный ресурс]. – Режим доступа: https://www.federalregister.gov/ documents/ 2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cy.
26. Комплексная психологическая диагностика сотрудников и кандидатов. Сайт. – [Электронный ресурс]. – Режим доступа: https://prof-dialog.ru/tests.

27. Кравцов, А.А. О промышленном и экономическом шпионаже, а также о недобросовестной конкуренции / А.А. Кравцов, И.И. Желнов // Мир науки. – 2014. – № 1. – С. 1–10.
28. Логвинова, С.Н. Профессиональное выгорание сотрудников уголовно-исполнительной системы / С.Н. Логвинова // Психологическое здоровье личности: теория и практика. III Всероссийская научно-практическая конференция. Сборник научных трудов. – С. 85–89.
29. Маршалл, Британская Колумбия, Йегер, ПК (1980). Корпоративная преступность. Свободная пресса.
30. Махмудова, И.Н. Методы обеспечения кадровой безопасности при подборе персонала: организация бизнес-процесса / И.Н. Махмудова // Международный научно-исследовательский журнал № 11 (65) Часть 4, Ноябрь. – Екатеринбург, 2017. – С. 178–184. ORCID: 0000-0002-9943-3839 ISSN 2303-9868 print ISSN 222-6017. – [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=30772835.
31. Махмудова, И.Н. Невостребованная занятость в цифровой экономике научно-практическая конференция «Экономика и управление в XXI веке: стратегии устойчивого развития», 5 июня 2018 г., г. Пенза, РФ. Ч. 1 / Под общ. ред. Г.Ю. Гуляева. – Пенза: МЦНС «Наука и Просвещение». МК-355. – 2018. – С. 84–88.
32. Махмудова, И.Н. От благонадежности к лояльности персонала для обеспечения кадровой безопасности организации / И.Н. Махмудова, Ю.А. Криворучко // Кадровик. – 2019. – № 7. – С. 93–100. – [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=39191900 (Дата обращения 10.03.2021 г.)
33. Махмудова, И.Н. Способы обеспечения кадровой безопасности на предприятии / И.Н. Махмудова, Ю.А. Криворучко // Наука XXI века: актуальные направления развития : сб. науч. ст. VIII Междунар. науч.-практ. конф., 5 февр. 2019 г. / ред. кол.: Г.Р. Хасаев, С.И. Ашмарина (отв. ред.) [и др.]. – Самара : Изд-во Самар. гос. экон. ун-та, 2019. – Вып. 1, ч. 1. – 371 с. С. 318–323; ISBN978-5-94622-893-0 ISBN978-5-94622-894-7 (ч. 1). – [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=37575305.

34. Махмудова, И.Н Влияние кадровых угроз на экономическую безопасность организации / И.Н. Махмудова // Вестник Самарского университета. Серия экономика и управление. – Самара : Издательство Самарского университета, 2020. – Т. 11. – № 4. – С. 83–89.
35. МВД России (2020). О состоянии преступности в Российской Федерации в 1 полугодии 2020 года. – [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/21551069/.
36. Меертс, К. (2019). Расследования: Кража сотрудниками собственности работодателя. В.Л. Шапиро и М.Х. Марас (ред.), Энциклопедия безопасности и управления в чрезвычайных ситуациях. Чам: Спрингер.
37. Международный валютный фонд (2001 г.). Справочный документ о злоупотреблениях в финансовой системе, финансовых преступлениях и отмывании денег. – [Электронный ресурс]. – Режим доступа: https://www.imf.org/external/np/ml/2001/eng/021201.htm
38. Миллиган, Э. (2020). Торговец Libor Том Хейс будет освобожден из тюрьмы в январе. https://www.bloomberg.com/news/articles/2020-11-02/convicted-libor-trader-hayes-to-be-released-from-jail-in-january.
39. Михайлова, А. Основные каналы утечки информации на предприятии / А. Михайлова. – [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/main-channels-information-leakage-in-enterprise.
40. Петровский, В.А. Психология неадаптивной активности / В.А. Петровский // Российский открытый университет. – Москва : ТОО «Горбунок», 1992. – 224 с.
41. Рапохин, Н.П. Исследование эмоционально-волевой устойчивости в условиях значимой деятельности / Н.П. Рапохин // Психологический журнал. – 1981. – Т. 2. – № 5. – С. 92–105.
42. РГ.РУ (2018). Защита доменных имен. – [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/10/11/chem-grozit-internet-polzovateliam-pervaia-v-istorii-smena-kriptograficheskih-kliuchej.html.
43. Ростелеком и Tadviser (2020). Сколько зарабатывает искусственный интеллект в России: исследования Tadviser и Росте-

леком. – [Электронный ресурс]. – Режим доступа: https://www.company.rt.ru/press/news/d457435/.
44. ТАСС (2020). В России 16% экономических преступлений совершается предпринимателями. – [Электронный ресурс]. – Режим доступа: https://tass.ru/ekonomika/8554543.
45. Титов, Д. Количество мошенничеств в российских компаниях резко возросло / Д. Титов // «Экономика и жизнь». – 2018. – № 19 (9735). – [Электронный ресурс]. – Режим доступа: https://www.eg-online.ru/article/372818/.
46. Толстоухова, Н. (2018). Коммерческая тайна чаще всего добывается через сотрудников / Н. Толстоухова. – [Электронный ресурс]. – Режим доступа: https://rg.ru/2018/12/05/ kommercheskie-tajny-chashche-vsego-vyvedyvaiut-cherez-sotrudnikov.html.
47. Хаснан, С. Детерминанты мошеннической финансовой отчетности: данные из Малайзии / С. Хаснан, Р.А, Рахман, С. Махентиран // Jurnal Pengurusan. – 2014. – № 42. – С. 103–117.
48. 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.
49. Шикман, М. (2013). Корпоративная преступность – Новые подходы и вызовы будущего. В Д. Чалета и М. Вршец (ред.), Управление корпоративной безопасностью – новые подходы и будущие вызовы (стр. 103-114). Институт корпоративной безопасности.

Учебное издание

Махмудова Ирина Николаевна,
Соловова Наталья Валентиновна

КАДРОВАЯ БЕЗОПАСНОСТЬ: ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ

Учебное пособие

Редактор Л. Р. Дмитриенко
Компьютерная верстка Л. Р. Дмитриенко

Подписано в печать 28.06.2022. Формат 60х84 1/16.
Бумага офсетная. Печ. л. 6,0.
Тираж 25 экз. Заказ . Арт. – 17(Р1У)/2022.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»
(САМАРСКИЙ УНИВЕРСИТЕТ)
443086, Самара, Московское шоссе, 34.

Издательство Самарского университета.
443086, Самара, Московское шоссе, 34.