

УДК 331

КОРПОРАТИВНАЯ И КАДРОВАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

Леонов С.А.

*к.э.н., доцент кафедры экономической теории
ФГБОУ ВО «Санкт-Петербургский государственный университет
промышленных технологий и дизайна»
г. Санкт-Петербург, Россия*

Аннотация

Настоящая статья описывает основы управления корпоративной безопасностью организации. Детально раскрывается содержание корпоративной безопасности и подсистем безопасности. Описывается место и роль кадровой безопасности в системе управления организацией. Автором проведена систематизация и обобщение знаний в контексте обеспечения корпоративной безопасности в целом и кадровой безопасности предприятия в частности.

Ключевые слова: корпоративная безопасность, кадровая безопасность, система управления, защита бизнеса, система безопасности.

CORPORATE SECURITY AND PERSONNEL SECURITY IN THE ENTERPRISE MANAGEMENT SYSTEM

Leonov S.A.

*candidate of economic sciences, associate Professor of the department of economic theory
FSBEI HE «Saint Petersburg State University
of Industrial Technologies and Design»
St. Petersburg, Russia*

Annotation

This article describes the fundamentals of corporate security management in an organization. The content of corporate security and its subsystems is explained in detail. The place and role of personnel security in the organization's management system are described. The author has systematized and summarized the knowledge in the context of ensuring corporate security in general and personnel security of the enterprise in particular.

Keywords: corporate security, personnel security, management system, business protection, security system.

В настоящее время экономическая активность предприятий постоянно растет, поэтому вопросы корпоративной безопасности имеют первостепенное значение. Корпоративная безопасность (КБ) – это комплексная система мер и стратегий, которые ориентированы на обеспечение безопасности активов и сотрудников предприятия, защиту коммерческой тайны, предупреждение утечки информации, рисков и угроз со стороны конкурентов, мошенников и других внешних факторов. Важность этой стороны бизнеса обусловлена необходимостью защитить материальные и интеллектуальные активы и исключить возможные угрозы для стабильности и развития компании [4].

В настоящее время существует множество научных работ, посвященных вопросам обеспечения корпоративной и кадровой безопасности в системе управления предприятиями и организациями. Среди таких работ следует отметить исследования А.Л. Вайновского, О.Е. Лозицкой, И.Н. Махмудовой, А.С. Молчан и др. авторов [1, 5, 6, 7]. Вместе с тем следует отметить, что данные вопросы требуют дальнейшего исследования и систематизации.

КБ достигается рядом мероприятий, направленных на уменьшение рисков в бизнес-процессах:

1. Создание организационно защищенной структуры – это формирование такой управленческой и организационной структуры предприятия, в которой учтены все возможные риски, а механизмы принятия решений максимально прозрачны. Для этого нужно правильное разделение полномочий и ответственности между сотрудниками, создание правил внутреннего контроля и аудита, внедрение системы комплексной оценки рисков на всех уровнях структуры. Основной задачей структуры является блокирование решений, которые могут угрожать стабильности и безопасности бизнеса.

2. Защита бизнеса – это комплекс мероприятий для обеспечения различных видов КБ – кадровой, экономической, кибербезопасности и других. Для этого реализуются программы, которые предотвращают утечку конфиденциальной информации, обеспечивают юридическую защиту и т. д.

3. Обеспечение безопасности в переходный период при наследовании компании или изменении юридического статуса владельца – это меры по юридической подготовке и поддержке процессов смены владельца или структурных изменений в организации. В этом случае необходимо гарантировать законность перехода прав собственности, предусмотреть меры защиты от потенциального разглашения коммерческой тайны, утечки клиентов и сотрудников. Это требует тщательной работы юристов и корпоративных консультантов по подготовке соответствующих документов и соглашений, которые обеспечат стабильность функционирования компании в переходный период.

Все эти меры должны реализоваться на постоянной основе, чтобы создать устойчивую и защищенную бизнес-среду для объектов обеспечения безопасности – целевой среды, защита которой направлена на предотвращение любых форм угроз, рисков или нарушений. Это может быть физическое имущество, информация, жизнь и здоровье людей, социальная структура или процессы, требующие защиты от внешних и внутренних угроз. Безопасность такого объекта является приоритетной для функционирования и развития любой организации или структуры.

Объекты обеспечения безопасности на предприятии представлены в табл. 1.

Таблица 1. Объекты обеспечения безопасности на предприятии

Объект	Описание
Операционная деятельность, бизнес-процессы	Совокупность действий, необходимых для функционирования и развития предприятия – производство, маркетинг, продажи, логистика и другие. Устранение и минимизация простоев и потерь
Физические лица	Защита здоровья, жизни, личных данных и прав руководства компании, сотрудников с трудовыми и гражданско-правовыми договорами, контрагентов, партнеров и клиентов
Материальные	Предотвращение краж, повреждений и утраты ценностей имущества компании – зданий, техники, оборудования, товаров, сырья и другого

Объект	Описание
активы	имущества
Нематериальные активы	Предотвращение незаконного использования, копирования или утраты интеллектуальной собственности (авторские права, патенты, товарные знаки), конфиденциальной информации, бренда и деловой репутации
Финансовые средства	Защита от мошенничества, краж, присвоения средств и финансовых манипуляций наличных и безналичных денег, финансовых инструментов и ценностей
Информация и информационные системы	Защита информационных данных, систем их обработки и хранения (компьютерные сети, программное обеспечение, базы данных) от несанкционированного доступа, утечек данных, вирусных и хакерских атак, и других угроз информационной безопасности

Составлено автором на основе [8].

Финансирование системы КБ оказывает непосредственное влияние на эффективность работы предприятия, на стабильность и надежность бизнеса. Система безопасности не является производственной сферой и напрямую не генерирует доход, однако играет важную роль в защите активов компании, так как снижает потенциальные потери и риски.

Высокий уровень корпоративной безопасности предприятия требует значительных финансовых вложений – приобретения современного оборудования, систем мониторинга и контроля, программного обеспечения для защиты информации, обучения сотрудников и регулярных аудитов. Кроме финансирования технического обеспечения, необходимо вкладывать средства в создание корпоративной культуры сотрудников и контроль за соблюдением мер безопасности. Первоначальные инвестиции окупаются в долгосрочной перспективе за счет предотвращения инцидентов, связанных с КБ.

Корпоративная безопасность включает в себя несколько подсистем. Подсистема КБ представляет собой часть общей структуры и направлена на

предотвращение определенного спектра угроз и обеспечение стабильности и устойчивости функционирования организации.

Подсистемы КБ и их задачи представлены в табл. 2.

Таблица 2. Подсистемы и задачи подсистем КБ

Подсистема	Объект обеспечения КБ	Задачи
Информационная	Информация и информационные системы	Конфиденциальность, целостность и доступность информации; защита от информационных угроз; снижение рисков потери информации или доступа к ней посторонних лиц
Экономическая	Экономические интересы и стабильность предприятия	Защита материальных и нематериальных активов; управление финансовыми ресурсами; сохранность и приумножение капитала; защита интеллектуальной собственности; снижение производственных, финансовых и инвестиционных рисков
Кадровая	Персонал и предприятие (недобросовестные действия сотрудников)	Снижение рисков, связанных с человеческим фактором; подбор, адаптация и обучение кадров; соответствие их поведения корпоративным стандартам, этическим нормам и законодательству; защита от действий персонала, которые могут нанести вред предприятию (неисполнение обязанностей, злоупотребления, утечка конфиденциальной информации); защита от лиц, представляющих угрозу безопасности предприятия
Физическая	Персонал, имущество и инфраструктура предприятия	Минимизация возможности несанкционированного доступа, вандализма, краж, террористических актов, природных и техногенных катастроф
Личная	Владельцы и топ-менеджеры, которые имеют право на принятие	Контроль в онлайн-пространстве; охрана жизни и здоровья; защита от давления, шантажа, угроз, насилия

Подсистема	Объект обеспечения КБ	Задачи
	стратегических решений	
Инженерно-техническая	Персонал, имущество, окружающая среда, инфраструктура предприятия (природные стихии и чрезвычайные ситуации)	Управление рисками, связанными объектами инфраструктуры, производственными процессами и технологическим оборудованием; меры по предотвращению чрезвычайных ситуаций и минимизация их последствий
Производственная	Персонал, имущество, окружающая среда, инфраструктура предприятия (вредное воздействие технических систем)	Надежность технических систем и средств предупреждения аварий, индивидуальной и коллективной защиты; безопасность технологий и конструкций
Техническая	Конфиденциальная информация	Снижение возможности целенаправленного электромагнитного излучения для нарушения работы технических средств и потери данных; обеспечение конфиденциальности данных; исключение утечки информации через акустические и визуальные каналы
Кибербезопасность	Компьютерные системы, сети и данные	Конфиденциальность, целостность и доступность информационных систем; защита информации и систем от нелегального использования, изменения или раскрытия, от хакерских атак и киберугроз; устранение последствий успешных хакерских атак
Экологическая	Персонал, население	Соблюдение экологических норм и стандартов; рациональное использование

Подсистема	Объект обеспечения КБ	Задачи
	и окружающая среда (негативное воздействие производственной деятельности предприятия)	природных ресурсов; переработка и утилизация отходов; предотвращение аварий и загрязнений; мониторинг и контроль за состоянием окружающей среды на всех этапах производственного процесса
Правовая	Интересы предприятия	Соблюдение налогового и трудового законодательства; уменьшение правовых рисков, защита интересов и активов компании от правовых угроз; предотвращение и оперативная реакция на правовые нарушения, конфликты и споры
Репутационная	Деловая репутация, общественное восприятие и имидж предприятия	Разработка системы мер, направленных на идентификацию, анализ и контроль информационных угроз; формирование позитивного имиджа компании среди клиентов, партнеров, инвесторов и целевой аудитории

Составлено автором на основе [8].

Различные подсистемы КБ позволяют организации эффективно противостоять внутренним и внешним угрозам. Для этого необходимо разработать мероприятия по каждой из подсистем безопасности, чтобы обеспечить защиту своих ресурсов, персонала и данных.

1. Информационная:

- разработка политики информационной безопасности, создание правил и процедур обработки и защиты данных, определение ответственности сотрудников;

- обучение персонала принципам информационной безопасности и правилам безопасного пользования данными;

- управление рисками и разработка стратегии их снижения;

- постоянный контроль информационных систем;

- защита от вирусов, вредоносного и шпионского ПО, спама и фишинга;
- системы обнаружения и предотвращения вторжений (IDS/IPS), мониторинг сетевого трафика на предмет подозрительной активности и блокировка угроз в реальном времени;
- шифрование данных – использование криптографических технологий для защиты конфиденциальности данных при их передаче и хранении;
- резервное копирование важных данных для предотвращения потери информации;
- многофакторная аутентификация для защиты аккаунтов от несанкционированного доступа.

2. Экономическая:

- проведение внутреннего и внешнего аудита для оценки финансового состояния, контроль за соблюдением законодательства и внутренних процедур;
- управление рисками – анализ и оценка финансовых рисков, разработка стратегий для их минимизации;
- защита коммерческой тайны;
- осуществление деятельности в строгом соответствии с действующим законодательством (налоговое, антимонопольное, корпоративное право);
- оценка надежности партнеров и контрагентов;
- оптимизация затрат и разработка мер по снижению издержек;
- страхование финансовых рисков, связанных с возможными потерями, убытками или другими неблагоприятными событиями.

3. Кадровая:

- отбор кандидатов и проверка при приеме на работу рекомендаций, документов об образовании и других данных;
- обучение сотрудников нормам корпоративной политике безопасности;
- оформление соглашений о неразглашении конфиденциальных данных;
- регулярная оценка и аттестация персонала на соблюдение правил безопасности;

- разработка процедур увольнения сотрудников для предотвращения утечки данных и других вредоносных действий;
- система внутреннего контроля и аудита, мониторинг доступа к информационным ресурсам и работе с конфиденциальной информацией;
- управление кризисными ситуациями – разработка планов действий на случай внутренних конфликтов, утечек информации или других ситуаций, угрожающих безопасности организации.

4. Физическая:

- силами работников предприятия – установка систем видеонаблюдения и доступа, регулярное проведение инструктажей по безопасности;
- охрана внешними организациями – профессиональные охранные агентства обеспечивают физическую охрану объекта круглосуточно.

5. Личная безопасность владельцев и топ-менеджеров, которые имеют право на принятие стратегических решений:

- предоставление квалифицированной физической охраны;
- использование автомобилей с повышенной степенью защиты и профессиональных водителей;
- обеспечение безопасности жилья и рабочего места – видеонаблюдение, контроль доступа, сигнализация и система быстрого реагирования;
- защита персональных данных, использование средств шифрования, безопасного хранения и обмена информацией;
- обнаружение и нейтрализация устройств для негласного сбора информации;
- обучение владельцев и топ-менеджеров основам безопасного поведения в Интернете, использование сложных паролей, двухфакторной аутентификации и других методов защиты цифровой идентичности;
- обучение основам самозащиты для повышения уровня личной безопасности при возможном нападении;

- обучение методам противодействия психологическому давлению и угрозам;
- юридическая помощь для защиты личных и профессиональных интересов;
- страхование жизни и здоровья.

6. Инженерно-техническая:

- обеспечение предприятия противопожарными системами и средствами пожаротушения;
- ограничение доступа на предприятие (турникеты, системы распознавания лиц и сетчатки глаз, карты доступа);
- размещение видеокамер на стратегически важных участках с централизованной обработкой данных;
- контроль периметра территории – с помощью ограждений, охранной сигнализации и регулярных патрулирований охранниками вдоль границ территории;
- установка систем сигнализации – охранная, противопожарная и тревожная сигнализации для быстрого реагирования на чрезвычайные ситуации.

7. Производственная:

- оценка рисков и анализ рабочих процессов на предмет выявления возможных угроз для безопасности сотрудников;
- разработка и внедрение стандартов безопасности и процедур, обновление нормативно-методических документов, требований законодательства;
- обеспечение сотрудников персональными средствами защиты – защитные очки, перчатки, шлемы и другие;
- организация тренингов, инструктажей и учебных занятий для сотрудников по вопросам производственной безопасности и мерам предотвращения несчастных случаев;

- технический контроль и обслуживание оборудования для предотвращения неполадок и аварийных ситуаций;
- организация безопасной рабочей среды, достаточной освещенности и чистоты на рабочих местах;
- регулярная организация медицинских осмотров сотрудников для раннего выявления признаков профессиональных заболеваний;
- обучение персонала действиям при несчастных случаях, авариях и пожарах, разработка планов эвакуации.

8. Техническая:

- установка на мониторы экранных фильтров, которые ограничивают угол обзора;
- расположение мониторов таким образом, чтобы экраны были направлены от проходов и мест общего пользования;
- контроль за вывозом информационных носителей;
- использование штор и пленок на окнах, которые препятствуют визуальному наблюдению;
- обустройство помещений звукопоглощающими материалами, установка шумоподавляющих устройств для снижения риска утечки информации по аудиальному каналу;
- ограничение использования мобильных устройств, способных записывать и передавать аудио, в критических зонах;
- использование генераторов, создающих “белый” или “розовый” шум для маскировки разговоров;
- использование экранированных и защищенных кабелей, специальных фильтрующих устройств и экранов в помещениях, где используется чувствительное оборудование, для защиты от побочных электромагнитных излучений.

9. Кибербезопасность:

- проведение регулярного анализа угроз и оценки уязвимостей в информационной инфраструктуре предприятия;
- шифрование данных и защита информации в хранилищах и при передаче по сети;
- установка и обновление средств антивирусной защиты на всех устройствах, подключенных к корпоративной сети;
- ограничение доступа к информационным ресурсам с помощью системы управления идентификацией и доступом (IAM), внедрение многофакторной аутентификации;
- обновление программного обеспечения и операционных систем для поддержания актуального уровня защиты;
- проведение регулярных тренингов для сотрудников по основам кибер гигиены и методам предотвращения кибератак;
- разработка и внедрение процедур восстановления данных и минимизации ущерба в случае нарушений в работе систем безопасности;
- создание и тестирование резервных копий важных данных;
- сотрудничество с профессиональными сообществами и службами кибербезопасности для обмена информацией о новых угрозах и методах защиты.

10. Экологическая:

- проведение экологических аудитов и оценки воздействия деятельности организации на окружающую среду, разработка мероприятий по снижению вредного воздействия;
- разработка экологической политики по сокращению отходов, эффективного использования ресурсов и минимизации выбросов в атмосферу;
- внедрение технологий, позволяющих снизить потребление энергии;
- использование систем фильтрации и очистки, сокращение выбросов загрязняющих веществ в атмосферу, почву и водоемы;

- рациональное использование воды, применение технологий очистки и повторного использования;
- внедрение системы раздельного сбора, утилизации и переработки отходов, сокращение объемов производственных и потребительских отходов;
- проведение регулярных тренингов и семинаров для сотрудников по экологической безопасности;
- создание запасов сырья и материалов для оперативного реагирования на экологические чрезвычайные ситуации (сорбенты для устранения разливов нефтепродуктов и др.).

11. Правовая:

- регулярный правовой аудит и мониторинг законодательства, обеспечение актуальности документов, лицензий, процедур и договоров в соответствии с изменениями в законодательстве;
- регистрация и защита прав на интеллектуальную собственность, контроль за их соблюдением;
- управление правовыми рисками, разработка мер по их минимизации;
- стратегия юридической защиты, разработка адекватных юридических позиций;
- реализация комплаенс-программ.

12. Репутационная:

- регулярный мониторинг СМИ и социальных сетей, отслеживание упоминаний о компании и своевременное выявление негативных отзывов или информационных атак;
- разработка плана и четких инструкций для оперативного реагирования на возможные угрозы репутации;
- проведение PR-кампаний, информационных мероприятий, публичных акций и конференций для укрепления позитивного имиджа компании;
- публикация отчетов о социальной ответственности и успехах компании, информирование общественности о достижениях и инновациях;

– обучение сотрудников основам репутационного менеджмента и корпоративной этике для защиты репутации компании.

Система корпоративной безопасности предполагает целостный подход к решению всех видов задач. Для этого необходимо обеспечить эффективное взаимодействие всех подсистем, понимать актуальные угрозы и оперативно реагировать на меняющуюся ситуацию. Стратегия безопасности должна быть адаптирована к деятельности конкретной организации и предусматривать разработку индивидуальных защитных мероприятий для снижения потенциальных рисков. Комплексный и системный подход даст возможность добиться высокого уровня корпоративной безопасности.

Вопросы кадровой безопасности имеют большее значение для успешного функционирования и развития любого предприятия. На долю человеческого фактора приходится значительная часть проблем, с которыми сталкивается бизнес. Это объясняется тем, что именно сотрудники непосредственно участвуют в производственных процессах, управлении, принятии решений и взаимодействии с клиентами. Они являются основным активом любой компании, поэтому ошибки, недобросовестное поведение или злонамеренные действия со стороны персонала могут привести к критическим потерям, угрозе репутации и безопасности бизнеса. Именно кадровая безопасность помогает снизить риски, связанные с человеческим фактором, и создает фундамент для стабильного и успешного развития предприятия.

Основная особенность кадровой безопасности заключается в том, что сотрудники предприятия являются одновременно и потенциальной угрозой для деятельности организации, и критическим ресурсом для идентификации, предотвращения и устранения этих угроз. Эта двойственность делает работу по обеспечению кадровой безопасности особенно сложной задачей [2].

С одной стороны, сотрудники обладают доступом к важнейшим корпоративным активам, информационным базам, производственным процессам и ресурсам компании. Это предоставляет им возможность для потенциальных

Вектор экономики | www.vectoreconomy.ru | СМИ Эл № ФС 77-66790, ISSN 2500-3666

злоупотреблений, утечки информации, мошенничества и других действий, которые могут нанести ущерб интересам предприятия.

С другой стороны, персонал предприятия осуществляет все действия, направленные на обеспечение безопасности. Работники могут идентифицировать угрозы, принять немедленные меры по предотвращению и нейтрализации рисков, они же формируют культуру корпоративной безопасности внутри компании. Квалифицированные сотрудники способны вовремя заметить и отреагировать на любые отклонения от нормы, а это является основой эффективной работы по корпоративной безопасности.

Учитывая эту двойственность, роль кадровой безопасности заключается в защите от внутренних угроз и создании устойчивой и безопасной рабочей среды для успешного функционирования и развития предприятия. Это предполагает работу с персоналом, которая включает в себя следующие действия:

- строгий отбор кандидатов;
- непрерывную оценку лояльности и профессионализма сотрудников;
- обучение принципам безопасности;
- формирование среди персонала понимания личной ответственности за сохранность корпоративных активов.

Для этого создаются комплексные программы по подготовке и мотивации персонала, по организации внутреннего контроля и аудита, по обеспечению непрерывной деятельности в условиях кризисов и др.

Кадровая безопасность предприятия занимает основное место в системе корпоративной безопасности, где она также выполняет двойную функцию. С одной стороны, она направлена на непосредственную защиту персонала, а с другой – на обеспечение иных видов безопасности организации, которые способствуют благополучию и защите сотрудников. Место кадровой безопасности представлено на рис. 1.

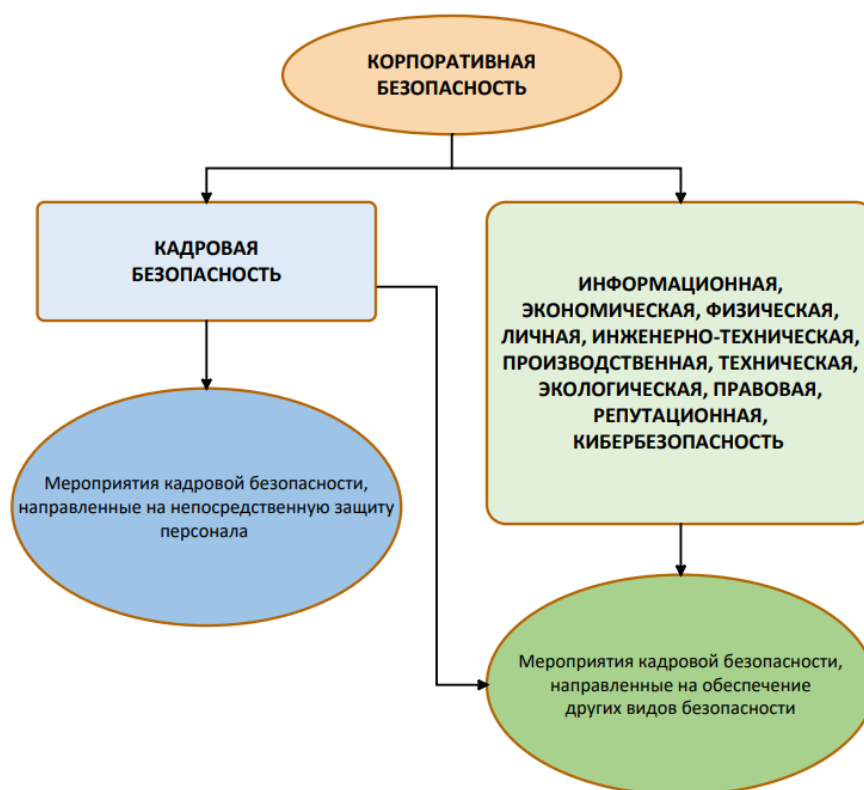


Рисунок. 1. Место кадровой безопасности в системе корпоративной безопасности (составлено автором на основе [2])

Мероприятия по обеспечению кадровой безопасности, направленные на непосредственную защиту персонала [3]:

1. Регулярное обучение и инструктажи персонала по вопросам безопасности труда помогают предотвращать несчастные случаи и профессиональные заболевания. Это тренинги по пожарной безопасности, правилам эвакуации, использованию средств индивидуальной защиты и т. д.

2. Организация курсов по управлению стрессом, предоставление услуг корпоративного психолога или доступ к психологической помощи онлайн снижают уровень профессионального выгорания и улучшают психологическое состояние сотрудников.

3. Медицинское обслуживание, регулярные медицинские осмотры, вакцинации, организация программ профилактики заболеваний поддерживают здоровье сотрудников и способствуют предотвращению распространения инфекционных заболеваний в коллективе.

Меры кадровой безопасности, которые направлены на обеспечение других видов безопасности:

1. Информационная безопасность – обучение персонала принципам и правилам работы с корпоративной информацией, в том числе с персональными данными, предотвращает утечки и несанкционированный доступ к конфиденциальной информации.

2. Экономическая безопасность – контроль и аудит финансовых операций, обучение работников правилам антифрода (меры по защите от мошеннических операций) помогают предупреждать финансовое мошенничество и убытки.

3. Производственная безопасность – выполнение норм промышленной безопасности, обеспечение безопасности производственных процессов и производственных помещений защищает сотрудников от несчастных случаев и аварий на производстве.

4. Экологическая безопасность – разработка экологической политики по сокращению отходов, эффективного использования ресурсов и минимизации выбросов в атмосферу улучшает экологическую обстановку и защищает здоровье сотрудников.

5. Физическая безопасность – организация инструктажей для сотрудников по вопросам безопасности и мерам предотвращения несчастных случаев снижает риск получения травм и улучшает физическое благополучие сотрудников.

6. Инженерно-техническая безопасность – подбор квалифицированных инженеров и технических специалистов, постоянное обучение современным методам и нормам инженерно-технической деятельности гарантирует безопасную эксплуатацию оборудования и технологических процессов.

7. Личная безопасность лиц, принимающих решения – создание надежной системы физической и информационной защиты вокруг этих лиц, ограничение доступа к личной и корпоративной информации предотвращает возможные угрозы и обеспечивает их личную безопасность.

8. Правовая безопасность – обучение сотрудников правилам внутреннего документооборота, изменениям в законодательстве, нормах и стандартах снижает юридические риски и защищает сотрудников от возможных правовых нарушений.

9. Репутационная безопасность – тщательный подбор сотрудников, социальная адаптация в коллективе и постоянная внутренняя коммуникация формирует позитивный внутренний и внешний имидж компании и защищает ее репутацию.

10. Кибербезопасность – регулярное обучение персонала правилам информационной безопасности и использование системы контроля доступа к корпоративным данным уменьшают риски кибератак и защищают компанию от утечки конфиденциальной информации.

В результате можно сказать, что роль кадровой безопасности очень велика и является основной частью корпоративной безопасности компании. Именно человеческий фактор больше всего влияет на процесс деятельности предприятия, поэтому комплексные меры по обеспечению кадровой безопасности – это основа стратегии снижения рисков и создания безопасной рабочей среды.

Библиографический список:

1. Вайновский, А. Л. Корпоративная безопасность: сущность, влияние на экономическую безопасность бизнеса / А. Л. Вайновский // Экономическая безопасность строительной отрасли: опыт, проблемы, перспективы : Материалы региональной научно-практической конференции с международным участием, Санкт-Петербург, 27–28 апреля 2021 года. – Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2021. – С. 231-235.

2. Дедкова, Е. Г. Сущность кадровой безопасности и ее роль в системе обеспечения экономической безопасности / Е. Г. Дедкова, Ю. И. Симкина // Кросскультурные аспекты менеджмента в деятельности социально-экономических систем: материалы XIX международной научно-практической конференции. Орел, 11–12 апреля 2022 года / Редколлегия: И. А. Тренина [и др.]. – Орел: Орловский государственный университет имени И. С. Тургенева, 2022. – С. 423–435.

3. Кадровые риски и методы управления ими [Электронный ресурс] / Интернет-журнал “Власта-персонал” – 2024. – URL: http://vlasta-p.com/useful_info/kadrovye-riski-i-metody-upr-5/ (дата обращения: 28.03.2024).

4. Леонов С. А. Кадровая безопасность и основы безопасности труда [Электронный ресурс]: учебник / Леонов С. А., Попов Ю. А. — Санкт-Петербург: СПбГУПТД, 2025.— 146 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=202561, по паролю.

5. Лозицкая, О. Е. Кадровая безопасность в системе корпоративной безопасности организации / О. Е. Лозицкая, Е. Л. Соколова // Управление человеческими ресурсами – основа развития инновационной экономики. – 2014. – № 5. – С. 443-446.

6. Махмудова, И. Н. Ключевая роль системы кадровой безопасности в обеспечении корпоративной безопасности / И. Н. Махмудова, А. С. Васюхин // Инновационные стратегии управления человеческими ресурсами : сборник научных трудов V Всероссийской научно-практической конференции, Самара, 20 апреля 2023 года. – Самара: Общество с ограниченной ответственностью "САМАРАМА", 2023. – С. 152-160.

7. Молчан, А. С. Кадровая безопасность в системе корпоративной безопасности / А. С. Молчан, Т. А. Зобнина // Современная экономика России: опора на внутренние резервы и поворот на Восток : Материалы международной научно-практической конференции, Краснодар, 01 апреля 2015 года. Том 2. –

Краснодар: Краснодарский центр научно-технической информации, 2015. – С. 158-163.

8. Панкратьев, В. В. Корпоративная безопасность: методическое пособие [Электронный ресурс] / Официальный сайт "Корпоративная безопасность". – 2024. – URL: [https://https://www.vvpankrat.ru/moistatyiobezopasnosti](https://www.vvpankrat.ru/moistatyiobezopasnosti) (дата обращения: 29.03.2024).