УДК 33

РОЛЬ КАДРОВОЙ БЕЗОПАСНОСТИ В ОБЩЕЙ СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Некрасова К.А.

Студент

Вятский государственный университет (ВятГУ),

Россия, Киров

Пестрикова А.С.

Студент

Вятский государственный университет (ВятГУ),

Россия, Киров

Селезнева Е.Ю.

Кандидат экономических наук, доцент

ВятГУ

Россия, Киров

Аннотация

В статье обосновывается ключевая роль кадровой безопасности в системе экономической безопасности предприятия. Анализируются внутренние угрозы, исходящие от персонала: от разглашения информации до прямого мошенничества и саботажа. Рассматриваются функциональные элементы кадровой безопасности (подбор, контроль, мотивация, лояльность), а также методики оценки кадровых рисков. Особое внимание уделяется взаимосвязи кадровой и финансовой, информационной и технико-технологической составляющих экономической безопасности. Предлагается матрица мероприятий по минимизации «человеческого фактора», доказывается, что без эффективной кадровой защиты все прочие подсистемы безопасности становятся уязвимыми.

Ключевые слова: кадровая безопасность, экономическая безопасность предприятия, внутренние угрозы, человеческий фактор, кадровые риски.

THE ROLE OF HUMAN RESOURCES SECURITY IN THE GENERAL SYSTEM OF AN ENTERPRISE'S ECONOMIC SECURITY

Nekrasova K.A.

Student

Vyatka State University (VyatSU),

Russia, Kirov

Pestrikova A.S.

Student Vyatka State University (VyatSU),

Russia, Kirov

Selezneva E.Yu.

Candidate of Economic Sciences, Associate Professor

VyatSU

Russia, Kirov

Abstract

The article substantiates the key role of human resources security in the economic security system of an enterprise. The article analyzes internal threats posed by personnel, from information disclosure to direct fraud and sabotage. It examines the functional elements of personnel security (recruitment, control, motivation, and loyalty), as well as methods for assessing personnel risks. Special attention is given to the interconnection between personnel, financial, information, and technical and technological components of economic security. The article proposes a matrix of measures to minimize the "human factor" and demonstrates that without effective personnel protection, all other security subsystems become vulnerable.

Keywords: personnel security, economic security of an enterprise, internal threats, human factor, and personnel risks.

Сейчас кадровая безопасность в России – это отказ от агрессивного роста в пользу выживания, переход к скрытым форматам сокращений и цифровая трансформация контроля. Рынок труда перешел из состояния острого дефицита кадров в новую фазу, где ключевыми трендами стали скрытая безработица, цифровой надзор и ужесточение судебной практики для работодателей. Основные тенденции сведены в таблицу 1.

Таблица 1 – Основные тенденции кадровой безопасности в России

Тренд	Суть	Статистика и факты
1. От найма к выживанию	Бизнес переходит от активного найма к стратегии выживания: сокращается штат, пересматриваются оргструктуры, точечно повышают зарплаты только ключевым сотрудникам.	– 25% компаний сокращали персонал в 2025 году (с 10% в 2023-м). – Сбер и ВТБ публично заявили о планах сократить до 20% сотрудников. – HR-эксперты прогнозируют, что трудовые конфликты станут устойчивым фоном для бизнеса в 2026 году.
2. Рост скрытой безработицы	Компании стараются избегать официальных увольнений, используя переход на неполный день, сокращение нагрузки и неоплачиваемые отпуска.	– Сокращенная нагрузка грозит до 5 млн человек в 2026 году. – Скрытая безработица привела к падению вакансий на 15-30% и росту числа соискателей на 10-20%. – На hh.ru осенью 2025 года вакансий стало на 26% меньше, а резюме – на 31% больше.
3. Цифровая гигиена и ИБ	Утечки данных по вине сотрудников становятся критической угрозой. Компании активно внедряют AI-системы для мониторинга и профилактики инцидентов.	– 52% московских компаний применяли увольнение как наказание за ИБ-инциденты, хотя в 62% случаев нарушения были случайными. – AI-системы позволяют поднять точность прогнозирования утечек до 94% (против 22% при традиционных методах).

4. Негибкость сотрудников ведет к увольнению	Профессиональная негибкость, особенно в цифровых навыках, становится главной причиной увольнений. Компании активно следят за вовлеченностью в гибридном формате.	– Нежелание осваивать нейросети и автоматизацию – ключевая причина увольнений в 2026 году. – Работники из бэк-офиса, среднего менеджмента и начинающие специалисты в ИТ – в зоне риска из-за автоматизации. – Лучшая стратегия – не увольнять опытных, а дообучать их цифровым инструментам.
5. Ужесточение судов и госнадзора	Судебная практика усложняется, а контроль со стороны государства становится цифровым и непрерывным. Ошибки в документах и выплатах обходятся компаниям всё дороже.	– 71% трудовых споров выигрывают работники в суде. – Трудовая инспекция переходит к непрерывному цифровому мониторингу с автоматическими риск-метриками (задержки зарплат, аномалии в отчетности). – Суды детально разбирают нюансы трудовых отношений: гибридный график, системы мотивации, дисциплинарные взыскания.
6. «Каннибализация» кадров	Дефицит персонала (1,7 млн человек в год) приведет к тому, что богатые регионы будут переманивать квалифицированных специалистов у бедных, что усилит региональное неравенство.	– Ежегодно стране требуется ~1,7 млн новых сотрудников для компенсации выхода на пенсию 12,2 млн человек за 7 лет. – Это приведет к нулевой безработице и росту ценности человеческого капитала (работодатели начнут удерживать сотрудников старше 50-60 лет). – Главный риск – «высасывание» кадров из периферии, что может привести к деградации сервиса и производства в малых городах.

Кадровая безопасность предприятия – это состояние защищённости экономических интересов компании от угроз, источником которых является персонал, а также процесс предотвращения и нейтрализации этих угроз. В общей системе экономической безопасности принято выделять финансовую, информационную, технико-технологическую, экологическую, правовую и кадровую подсистемы. Однако первая особенность кадровой безопасности заключается в том, что она пронизывает все остальные: утечка информации, хищение средств, поломка оборудования – практически всегда совершаются конкретными людьми. Важно различать классический HR-менеджмент, нацеленный на эффективное использование трудовых ресурсов, и кадровую безопасность, ориентированную на минимизацию ущерба от этих же ресурсов. Например, система грейдов и KPI повышает производительность, но не исключает возможности сотрудника продать коммерческую информацию [7]. Поэтому задачи кадровой безопасности часто решаются службой безопасности совместно с отделом кадров, а иногда и в противоречии с ним, когда жёсткий контроль вступает в конфликт с доверием и корпоративной культурой. Основу нормативно-правового регулирования составляют Трудовой кодекс РФ (особенно раздел о материальной ответственности), [10] Федеральный закон «О коммерческой тайне», [11] Закон «О государственной тайне», [2] а также локальные акты предприятия – положения о коммерческой тайне, о работе с персональными данными, должностные инструкции. Отсутствие или формальный характер таких документов резко снижает возможность привлечь сотрудника к ответственности.

Спектр угроз кадровой безопасности чрезвычайно широк. Внешние угрозы с участием персонала включают переманивание ключевых специалистов конкурентами, известное как контрольный найм, подкуп или шантаж сотрудников для получения внутренней информации, а также инициирование проверок через анонимные жалобы. Пример из практики: конкуренты находят «нужного» бухгалтера и предлагают вознаграждение за выгрузку клиентской

базы. Однако наибольшую опасность представляют внутренние умышленные угрозы: прямые хищения денег, товаров и основных средств, фальсификация управленческой отчётности «под нужные показатели», саботаж в виде намеренного повреждения оборудования или срыва сроков, передача третьим лицам коммерческой тайны. Умышленные действия часто носят серийный характер и остаются незамеченными длительное время [1]. Парадоксально, но непреднамеренные действия сотрудников могут нанести не меньший ущерб. Низкая квалификация приводит к ошибкам в расчётах, что оборачивается штрафами и потерями. Выгорание и хроническая усталость – к нарушениям техники безопасности и авариям. Простая халатность в виде незаблокированного компьютера с отчётом или оставленного документа в копировальном аппарате создаёт бреши в информационной защите. Отдельного внимания заслуживают «серые зоны» современных форм занятости – аутсорсинг и удалённый персонал. Аутсорсинговый сотрудник имеет доступ к информационным системам, но формально не связан с компанией трудовым договором. Удалённый работник выпадает из привычного контроля, включающего видеонаблюдение и физическое присутствие на рабочем месте. Это требует дополнительных инструментов – DLP-систем, VPN-подключений с логированием, специальных пунктов в договорах гражданско-правового характера [3].

Статистика трудовых ресурсов РФ показывает глубокий структурный дисбаланс: исторически минимальная безработица сочетается с критическим сокращением кадрового резерва и демографическим сжатием. В таблице 2 представлены ключевые цифры [9].

Таблица 2 – Показатели трудовых ресурсов РФ (2025–2026 гг.)

Показатель	Значение	Динамика / Примечания
Численность рабочей силы	75,5–76,5 млн чел.	Стабильно; пик занятости (75 млн) достигнут в июле 2025 г.

Занятые в экономике	≈74,8 млн чел. (окт. 2025)	Число работающих выросло с 72 млн до почти 75 млн за 5 лет
Уровень безработицы	2,1–2,2%	Исторический минимум (2,1% в февр. 2026); РФ – 1-е место в G20 по минимальной безработице
Зарегистрированные безработные	273 тыс. чел. (I кв. 2025)	Резкий контраст с общей безработицей по методологии МОТ (1,77 млн)
Кадровый резерв («скрытый резерв»)	4,4 млн чел. (2025)	Сократился вдвое с 7 млн в 2021 г.; доля от занятых упала с 10% до 6%
В т.ч. безработные (активный поиск)	1,7 млн чел.	Категория кадрового резерва, готовая приступить немедленно
Работающие неполное время	1,6 млн чел.	Рост на 9,9% во II–IV кв. 2025 г. (скрытая безработица)
Работники, заявленные под риском увольнения	105 147 чел. (на 1 апр. 2026)	Рост на 43% с июня 2025 г.; наибольший прирост – в с/х и строительстве
Общее число вакансий	1,47 млн (дек. 2025)	Снижение на 13% год к году (с пика 2,1 млн в июне 2024)
Соотношение безработных на вакансию	1 : 1,2 (больше вакансий, чем безработных)	Масштабный кадровый голод; в отдельных регионах – 2,3 вакансии на соискателя
Трудоспособное население (2025)	≈75,9 млн чел.	41% – «миллениалы» (28–44 года); 35–37% – поколение X, близкое к пенсии; 24% – поколение Z
Сокращение трудоспособного населения	–1,5 млн чел. (2025 к 2024)	В 2026 г. ожидается ещё – 1,4 млн; структурное демографическое сжатие

Трудовые мигранты (общее присутствие)	5,7 млн чел. (нач. 2026)	Снижение на 10% за год (с 6,3 млн); из них по патентам – ~2,3 млн
Разрешения на работу для иностранцев	240 тыс. (2025)	Рост на 42% год к году; рекорд с 2017 г. Квота на 2026 г. – 278 940

Кадровый резерв в России практически исчерпан: число людей, готовых выйти на работу, сократилось с 7 до 4,4 млн человек — почти вдвое. Одновременно происходит демографическое сжатие: на рынок заходит малочисленное поколение 1990-х, а уходит многочисленное поколение X, разрыв достигает около 4 млн человек и к 2030 году может вырасти до 4,8 млн. Миграция даёт двойной эффект: общее число иностранцев сократилось на 600 тыс., но выдача разрешений на работу выросла на 42%. Наконец, на фоне рекордно низкой официальной безработицы (2,1%) растёт скрытая — 1,6 млн человек переведены на неполный день или находятся в простое, что почти на 20% больше, чем год назад.

Функциональная система обеспечения кадровой безопасности начинается с надёжного «входа» в компанию. Ошибка при найме обходится в среднем в 30–50% годового оклада работника с учётом времени на поиск, адаптацию и возможный ущерб. Поэтому базовое правило – проверка кандидатов, включающая подтверждение образования и опыта, запросы с предыдущих мест работы (особенно на предмет увольнения по компрометирующим статьям), проверку благонадёжности через открытые базы данных, такие как ФНС и служба судебных приставов. На чувствительных позициях – финансовый директор, главный бухгалтер, заведующий складом – допускается использование полиграфа, но с соблюдением трудового законодательства и при наличии письменного согласия кандидата. Однако ни одна проверка не даёт стопроцентной гарантии, поэтому необходимы постоянные организационно-управленческие меры. Ключевые из них: разграничение доступа к информации

по принципу необходимости знать, чёткие должностные инструкции с указанием меры ответственности, регламент работы с коммерческой тайной, включающий маркировку документов и журналы ознакомления, правила внутреннего трудового распорядка, запрещающие вынос документов и использование внешних носителей информации [5]. Эффективный способ снизить умышленные угрозы – сделать сотрудника заинтересованным партнером, разделяющим ответственность за успех компании. Материальная мотивация включает прозрачный бонус за отсутствие инцидентов для ключевых фигур. Нематериальная мотивация – это признание заслуг, карьерный рост, комфортная этическая среда. Практика показывает, что в компаниях с проработанной культурой лояльности количество внутренних хищений минимум в три раза ниже, чем в тех, где упор делается только на контроль. Контроль не должен быть тотальным, поскольку это демотивирует персонал, но он должен быть неотвратимым. DLP-системы фиксируют пересылку конфиденциальных файлов, видеонаблюдение контролирует работу с товарно-материальными ценностями, а выборочный аудит действий сотрудников даёт понимание «точек отказа» в системе безопасности. Параллельно с контрольными мероприятиями проводится обучение: инструктажи по информационной безопасности, разбор реальных кейсов ущерба без указания имён, тестирование персонала на знание регламентов. Важный элемент – горячая линия для анонимных сообщений о нарушениях коллег, которая позволяет выявлять скрытые угрозы [6].

Для количественной оценки эффективности кадровой безопасности предлагается использовать минимальный набор ключевых показателей, измеряемых ежеквартально. Текучесть кадров – норма не более 10–15% в год, при этом резкий рост является тревожным сигналом. Количество зафиксированных кадровых инцидентов – хищений, утечек, саботажа – в динамике позволяет судить об эффективности принимаемых мер. Доля кандидатов, прошедших полную проверку службой безопасности, отражает качество входного фильтра. Индекс лояльности персонала измеряется

анонимным опросом по шкале от 0 до 10 с помощью метода eNPS (метрика для оценки лояльности сотрудников к компании. Они показывает, насколько работники готовы рекомендовать организацию в качестве места работы). Также важен процент закрытых инцидентов с материальной компенсацией, показывающий неотвратимость ответственности. Полезна также матрица кадровых рисков, где риск рассчитывается как произведение вероятности наступления события на величину возможного ущерба. Например, утечка клиентской базы через рядового менеджера: вероятность выше средней, например, 0,6, а ущерб критический – 10 млн рублей, что даёт итоговый риск 6 млн рублей. Уход ключевого разработчика к конкуренту имеет среднюю вероятность 0,4 при ущербе 5 млн рублей, а значит, риск составит 2 млн рублей. Матрица позволяет ранжировать приоритеты защиты и обоснованно распределять ограниченные ресурсы на мероприятия по снижению наиболее опасных рисков [4].

Не менее важным аспектом выступает взаимосвязь кадровой безопасности с иными подсистемами экономической безопасности. Связь с финансовой безопасностью проявляется в том, что человек в бухгалтерии может неправомерно списать средства на «левые» счета, завысить затраты, скрыть кассовые разрывы или исказить управленческую отчётность. Кадровый контроль в этой сфере включает разделение обязанностей, обязательный ежегодный отпуск продолжительностью не менее двух недель (во время которого часто вскрываются махинации), а также внезапные проверки кассы и сверки с контрагентами. Все эти меры напрямую защищают финансовые потоки компании. Связь с информационной безопасностью критична: самый уязвимый элемент любой IT-защиты – это человек. Сотрудник, записавший пароль на стикер и приклеивший его к монитору, открывший фишинговое письмо от якобы руководителя, или сознательно переславший конфиденциальные файлы на личную электронную почту, сводит на нет миллионные инвестиции в межсетевые экраны, DLP-системы и антивирусное программное обеспечение.

Регулярное обучение персонала основам кибергигиены и жёсткая политика доступа к информации являются одновременно частью и кадровой, и информационной безопасности. Связь с технико-технологической безопасностью проявляется через нарушения инструкций по эксплуатации оборудования, игнорирование правил техники безопасности, работу в состоянии алкогольного или наркотического опьянения. Это кадровые причины поломок станков, аварий и даже человеческих жертв, что влечёт за собой колоссальные финансовые потери, остановку производства и уголовную ответственность для руководителей [8].

Таким образом, без эффективно выстроенной кадровой безопасности все остальные подсистемы экономической безопасности предприятия работают не в полную силу или не работают вовсе, поскольку основной носитель угроз – человек – остаётся вне зоны контроля. Именно поэтому кадровая безопасность должна рассматриваться не как вспомогательная функция, а как базовый, системообразующий элемент всей системы экономической защиты хозяйствующего субъекта.

Библиографический список:

1. Агеева А. Д., Сергеева И. А. Угрозы кадровой составляющей экономической безопасности предприятия и меры по её обеспечению //Проблемы и перспективы развития российской экономики. – 2021. – С. 209-211.
2. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (последняя редакция) КонсультантПлюс: справ.-правовая система. URL: [https://www.consultant.ru/document/cons_doc_LAW_2481/] (дата обращения: 11.05.2026).
3. Ибрагимова П. А., Гусайниева Х. Г. Кадровая безопасность: риски, угрозы, пути совершенствования //Региональные проблемы преобразования экономики. – 2021. – №. 5 (127). – С. 127-133.

4. Ильченко С. В., Алакоз С. Н., Садыхова Э. Н. Кадровая безопасность как инструмент обеспечения экономической безопасности организации //Бизнес и дизайн ревю. – 2024. – №. 3 (35). – С. 24-33.
5. Кайгородцева К. А., Тургаева А. А. Роль кадровой безопасности в аспекте экономической безопасности //Вестник евразийской науки. – 2023. – Т. 15. – №. 2S. – С. 35.
6. Кузнецова Н. В. Угрозы кадровой безопасности организации. – 2021.
7. Мингалеева Д. И. Кадровая безопасность как фактор обеспечения экономической безопасности организации //Экономика и социум. – 2023. – №. 3-1 (106). – С. 413-418.
8. Субботина Т. Н. Кадровая безопасность в структуре экономической безопасности: сущность и методология оценки //Вектор экономики. – 2022. – №. 9. – С. 75.
9. Труд и занятость в России. 2025: статистический сборник / Федеральная служба государственной статистики; редколлегия: С.М. Окладников (председатель) [и др.]. – Москва, 2025. – 172 с. – URL: https://rosstat.gov.ru/storage/mediabank/Trud_2025.pdf (дата обращения: 09.05.2026).
10. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (ред. от 29.12.2025, с изм. от 06.02.2026)// КонсультантПлюс: справ.-правовая система. URL: [https://www.consultant.ru/document/cons_doc_LAW_34683/] (дата обращения: 11.05.2026).
11. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (последняя редакция) // КонсультантПлюс: справ.-правовая система. URL: [https://www.consultant.ru/document/cons_doc_LAW_48699/] (дата обращения: 11.05.2026).