Акчурин Ришат Ринатович
студент
АОЧУ ВО «Московский финансово-юридический
университет МФЮА»
г. Москва

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ КАДРОВОЙ БЕЗОПАСНОСТИ В ВЫСОКОТЕХНОЛОГИЧНЫХ ОРГАНИЗАЦИЯХ: СУЩНОСТЬ, РИСКИ И НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ

Аннотация: *в статье рассматриваются теоретико-правовые основы кадровой безопасности как функциональной составляющей экономической безопасности организации. Проведён критический анализ научных подходов к определению понятия «кадровая безопасность» применительно к высокотехнологичному сектору. Систематизированы кадровые риски, характерные для операторов дата-центров, включая квалификационные риски, риски нелояльности, информационные угрозы и риски, порождаемые неправомерным поведением самого работодателя. Дана оценка нормативно-правового и организационного обеспечения кадровой безопасности, обоснована ключевая роль локального нормотворчества в преодолении разрыва между рамочным федеральным регулированием и отраслевой спецификой деятельности.*

Ключевые слова: *кадровая безопасность, экономическая безопасность, кадровые риски, высокотехнологичный сектор, коммерческая тайна, локальное нормотворчество, информационная безопасность, дата-центры.*

Введение

Обеспечение защищённости хозяйствующих субъектов от внутренних угроз в условиях цифровой трансформации приобрело системный характер. Для высокотехнологичных предприятий – в том числе операторов дата-центров – персонал одновременно выступает главным производительным ресурсом и потенциальным вектором риска. Ошибка при подборе работника, слабая адаптация, конфликт интересов, нелояльность, утрата квалификации или несанкционированное

распространение служебной информации способны обернуться финансовыми потерями, срывом производственного процесса и репутационными последствиями.

Специфика операторов дата-центров состоит в том, что их персонал взаимодействует с высоконагруженным оборудованием, энергосистемами, клиентскими данными и закрытыми конфигурационными параметрами. Кадровая ошибка здесь имеет иную цену, нежели в традиционном сервисном бизнесе: простой мощностей, утечка технических сведений или конфликтное увольнение инженера с уникальной компетенцией могут затронуть операционную устойчивость и исполнение договорных обязательств перед клиентами.

Несмотря на значительный массив научных публикаций по кадровой безопасности, проблематика организаций, работающих с критической цифровой инфраструктурой, остаётся недостаточно изученной. Настоящая статья направлена на заполнение этого пробела: систематизировать теоретические подходы, классифицировать отраслевые кадровые риски и оценить достаточность действующего правового регулирования применительно к операторам дата-центров.

1. Сущность кадровой безопасности и её место в системе экономической безопасности организации

Кадровая безопасность традиционно рассматривается как подсистема экономической безопасности организации. В.К. Сенчагов связывал экономическую безопасность с защищённостью интересов и способностью системы к развитию, что позволяет трактовать её не только как защиту от ущерба, но и как условие нормального воспроизводства экономических отношений [1]. Структура экономической безопасности охватывает финансовую, информационную, правовую, технико-технологическую, имущественную и кадровую составляющие, которые на практике взаимосвязаны: финансовая устойчивость зависит от дисциплины работников, информационная безопасность – от их поведения, правовая безопасность – от соблюдения процедур приёма, обработки персональных данных, режима коммерческой тайны и увольнения.

В академической литературе выделяются три основных подхода к пониманию кадровой безопасности. Первый рассматривает её как направление кадровой работы, нацеленное на сохранение и развитие кадрового потенциала. Второй определяет её как предотвращение негативного воздействия на экономическую безопасность через снижение рисков, связанных с персоналом и трудовыми отношениями [2]. Третий трактует её как состояние защищённости организации от кадровых угроз [3]. Для высокотехнологичных компаний наиболее продуктивным представляется синтез этих подходов, поскольку угроза здесь возникает как из действий нелояльного сотрудника, так и из банального дефицита компетенций.

Принципиально важно, что персонал выступает одновременно субъектом угроз и объектом защиты. По мнению П.А. Ибрагимова и Х.Г. Гусайниева, кандидаты, действующие и бывшие сотрудники могут создавать угрозы для организации, однако сами работники также подвержены рискам со стороны работодателя – управленческих ошибок, конфликтной среды, нарушений трудовых прав [4]. Кадровая безопасность не должна строиться как система тотального подозрения; её задача – снижать вероятность ущерба через правомерные процедуры и чёткое распределение ответственности.

Теоретическое обоснование экономического значения кадровой безопасности опирается на концепцию человеческого капитала Г. Беккера: профессиональная подготовка и накопленный опыт формируют особый вид капитала, потеря которого обходится организации значительно дороже, чем затраты на подбор замены [5]. Ресурсный подход Дж. Барни дополняет эту логику: квалифицированная команда, корпоративные знания и межфункциональное доверие являются ресурсами, которые ценны, редки, трудно копируемы и сложно заменимы, – то есть составляют основу устойчивого конкурентного преимущества [6]. Если организация не защищает такие ресурсы от утраты, выгорания или перехвата конкурентами, она теряет часть экономической основы своей деятельности.

Кадровая безопасность имеет чёткую правовую границу. Работодатель вправе проверять квалификацию кандидата, устанавливать режим коммерческой

тайны, разграничивать доступ к информации и применять дисциплинарные меры, однако все эти действия должны соответствовать трудовому законодательству, принципу недопустимости дискриминации и требованиям к обработке персональных данных. Нарушение этих правил само превращается в источник риска: незаконное увольнение, дискриминационные проверки или неправомерный сбор сведений о работнике влекут трудовые споры, административную ответственность и утрату доверия персонала.

Для операторов дата-центров кадровая безопасность неотделима от непрерывности производственных процессов. Если критическая операция зависит от одного инженера, болезнь или конфликтное увольнение этого специалиста могут нанести ущерб, несопоставимый с формальным нарушением дисциплины. Угрозой становится не только нелояльность, но и отсутствие передачи знаний – зависимость от персональных компетенций, которые нигде не задокументированы. Поэтому кадровая безопасность требует должностных инструкций, наставничества, регламентов передачи опыта и кадрового резерва.

2. Классификация кадровых рисков применительно к высокотехнологичным организациям

Разграничение понятий «кадровый риск», «кадровая угроза» и «кадровая опасность» имеет не только теоретическое, но и практическое значение. Риск выражает вероятность неблагоприятного результата, связанного с работником, трудовыми отношениями или управленческой ошибкой. Угроза указывает на конкретный источник возможного ущерба – лицо, решение, процедурную уязвимость. Опасность описывает состояние, при котором условия для реализации риска уже сложились, но ущерб ещё можно предотвратить. Организация, работающая только с угрозами, реагирует поздно – расследует утечку или ищет замену ушедшему специалисту. Работа с рисками позволяет действовать превентивно.

Первое основание классификации – источник риска. Внутренние риски формируются внутри организации: приём неподходящего кандидата, нарушение дисциплины, конфликт в подразделении, разглашение служебной информации, злоупотребление доступом к ресурсам. Внешние риски действуют из внешней

среды: дефицит квалифицированных специалистов, переманивание сотрудников конкурентами, недобросовестные действия соискателей, рост киберугроз. И.Н. Махмудова и Н.В. Соловова связывают внешние риски с конкурентной средой и информационными атаками, а внутренние – с поведением персонала и состоянием управленческих процедур [7].

Второе основание – характер ущерба. Имущественные риски проявляются в хищении или порче оборудования. Финансовые риски возникают при ошибках расчётов, сговоре при закупках, штрафах за нарушения законодательства. Информационные риски выражаются в утечке персональных данных или разглашении коммерческой тайны. Правовые риски связаны с трудовыми спорами и незаконными увольнениями. Репутационный ущерб возникает, когда кадровый конфликт выходит за пределы организации. А.Р. Алавердов предлагает более детальную классификацию – по прогнозируемости, управляемости, характеру потерь, этапам работы с персоналом и возможности страхования [8].

Применительно к операторам дата-центров каждый из перечисленных видов риска приобретает специфическое содержание. Квалификационный риск здесь не сводится к формальному несоответствию образования: работник может иметь профильный диплом, но не иметь практического опыта с конкретным типом оборудования или конфигурацией сети. Ограниченность рынка инженерных специалистов в регионах присутствия дата-центров усиливает зависимость от удержания ключевого персонала. Снижение квалификационного риска требует системного наставничества, периодической оценки компетенций и документирования технологических знаний.

Информационные риски в дата-центрах отличаются повышенной латентностью. Сотрудник получает доступ к закрытым параметрам конфигурации оборудования, программным интерфейсам, клиентским данным и схемам инфраструктуры. По данным аналитического отчёта InfoWatch о российских утечках информации ограниченного доступа за 2023–2024 гг., в 2024 году было зафиксировано 778 случаев потери конфиденциальных сведений, причём доля инцидентов, связанных с умышленными действиями внутренних нарушителей, составила

18,5% [9]. Это подтверждает, что технические меры защиты не могут полностью заместить кадровые процедуры.

Специфическим для майнинговых дата-центров является риск инсайдерского использования мощностей в личных интересах – несанкционированное выделение вычислительных ресурсов в обход учётных систем. Он обнаруживается не сразу, поскольку не всегда отражается в видимых отклонениях операционных показателей, и требует технических средств мониторинга в сочетании с кадровыми контрольными процедурами.

Отдельного внимания заслуживают риски, порождённые неправомерным поведением самого работодателя. Незаконный отказ в приёме, дискриминационные требования, задержка заработной платы, нарушение режима рабочего времени, незаконное увольнение – все эти действия создают правовые, финансовые и репутационные последствия для организации. По имеющимся данным, около трети увольнений обусловлены конфликтом с руководством [10]. Конфликтное расставание может повлечь отказ передать дела, распространение негативной информации и сохранение несанкционированного доступа к корпоративным системам.

3. Нормативно-правовое и организационное обеспечение кадровой безопасности

Нормативная основа кадровой безопасности имеет несколько уровней. Федеральные законы устанавливают общие правила: как заключать и расторгать трудовой договор, как обрабатывать персональные данные, как вводить режим коммерческой тайны, как обеспечивать охрану труда и противодействовать коррупции. Локальные нормативные акты переводят эти правила на язык конкретной организации. Текущие управленческие документы – приказы, акты, журналы учёта, протоколы инструктажей – показывают, как правила применяются на практике.

Трудовой кодекс Российской Федерации образует фундамент кадровой безопасности, регулируя заключение трудового договора, права и обязанности сто-

рон, дисциплину труда, материальную ответственность, режим рабочего времени, охрану труда и порядок увольнения. Через трудовой договор работодатель получает право требовать исполнения трудовой функции и соблюдения внутреннего распорядка, однако договор не может заменить должностную инструкцию, регламент доступа к информации и правила обращения с имуществом.

Федеральный закон №152-ФЗ «О персональных данных» обязывает работодателя определять цель обработки, не собирать избыточных сведений, ограничивать доступ к данным и прекращать их обработку по достижении цели. Федеральный закон №98-ФЗ «О коммерческой тайне» связывает охрану конфиденциальных сведений с определением их перечня, ограничением и учётом доступа, регулированием порядка обращения с носителями. Принципиально важно, что режим коммерческой тайны имеет юридическую силу лишь при его надлежащем оформлении: формулировка о конфиденциальности в трудовом договоре без реальных процедур не защищает работодателя.

Антикоррупционное законодательство – Федеральный закон №273-ФЗ «О противодействии коррупции» – расширяет содержание кадровой безопасности за пределы классической трудовой дисциплины. В коммерческой организации антикоррупционные меры обычно выражаются в политике предупреждения коррупции, порядке уведомления о конфликте интересов, правилах работы с подарками и закупочных регламентах. Применительно к дата-центрам особую роль играет контроль закупочных решений, поскольку специалисты по оборудованию нередко участвуют в оценке и выборе поставщиков. Статья 204 УК РФ о коммерческом подкупе создаёт уголовно-правовые риски для лиц, наделённых полномочиями принимать юридически значимые экономические решения от имени организации, что требует системного выявления таких должностей и установления соответствующих ограничений.

Центральный вывод анализа нормативной базы состоит в следующем: федеральное законодательство задаёт лишь общие рамки, оставляя значительную часть регулирования на усмотрение работодателя. Оно регламентирует дисциплинарную ответственность, но не предоставляет эффективных инструментов

для превентивного управления рисками, характерными для высокотехнологичного сектора. Следовательно, основным механизмом обеспечения кадровой безопасности выступает локальное нормотворчество.

Локальные нормативные акты работают как инструмент кадровой безопасности при трёх условиях: они не противоречат закону, работники с ними ознакомлены, а организация применяет их последовательно. Формальное положение о коммерческой тайне не защищает организацию, если перечень конфиденциальных сведений не определён, доступ к ним не разграничен, а работники не понимают, какие действия запрещены. Исследование PwC по экономическим преступлениям 2024 года фиксирует, что наиболее разрушительными угрозами для компаний остаются киберпреступность, коррупция и мошенничество при закупках [11] – все они имеют выраженную кадровую природу и не перекрываются исключительно техническими средствами.

Организационная структура обеспечения кадровой безопасности должна распределять ответственность между несколькими функциональными блоками. Руководство утверждает политику безопасности и выделяет ресурсы. HR-служба отвечает за процедуры подбора, адаптации, обучения, оценки и кадрового документооборота. Юридическая служба проверяет соответствие локальных актов законодательству и сопровождает служебные расследования. ИТ-подразделение управляет учётными записями, правами доступа и журналами событий. Служба безопасности контролирует пропускной режим. Руководители подразделений обеспечивают повседневное соблюдение правил. Разрыв взаимодействия между этими субъектами – наиболее распространённая причина неэффективности системы кадровой безопасности на практике.

Режим доступа к объектам, помещениям и информационным системам образует операционный слой кадровой безопасности. Работник должен иметь права доступа, соответствующие его трудовой функции, а не сложившейся организационной привычке. Особого внимания требует процедура прекращения доступа при переводе и увольнении: блокировка учётных записей должна совпадать по времени с правовым прекращением трудовых отношений, а не следовать за ним

с задержкой. Отчёт ACFE о профессиональном мошенничестве 2024 года показывает, что значительная часть инцидентов связана с отсутствием внутренних контролей или обходом уже существующих процедур [12].

Для операторов дата-центров нормативно-правовое обеспечение кадровой безопасности требует учёта производственной специфики. Универсальная кадровая политика недостаточна: внутренние регламенты должны детально описывать режим допуска к техническим помещениям, порядок передачи смен, правила обслуживания высоконагруженного оборудования, процедуры документирования технических знаний при увольнении инженера. Формальный подход к ознакомлению сотрудников с должностными инструкциями в данной отрасли является системной уязвимостью.

Заключение

В результате проведённого анализа можем сформулировать следующие выводы.

Во-первых, кадровая безопасность для высокотехнологичных организаций не может сводиться к кадровому делопроизводству или административному контролю. Это сложная междисциплинарная система, требующая интеграции HR-департамента, юридической службы, ИТ-подразделения и службы безопасности.

Во-вторых, специфика операторов дата-центров определяет приоритетный набор кадровых рисков: квалификационный дефицит инженерно-технического персонала, высокая цена ошибки при обслуживании оборудования, латентные информационные угрозы, инсайдерское использование вычислительных мощностей, а также риски конфликтного увольнения специалистов с эксклюзивными компетенциями.

В-третьих, разрыв между требованиями федерального законодательства и реальной необходимостью защиты специфических отраслевых активов преодолевается исключительно за счёт развитой системы локальных нормативных актов, учитывающей уникальность бизнес-процессов. При этом локальные акты

эффективны лишь тогда, когда они не ограничиваются формальным ознакомлением работников, а подкреплены техническими средствами контроля и последовательным правоприменением.

Дальнейшие исследования в данной области могут быть направлены на разработку отраслевых методик оценки кадровых рисков для операторов дата-центров, а также на изучение практики построения систем локального регулирования кадровой безопасности в высокотехнологичном секторе российской экономики.

Список литературы

1. Сенчагов В.К. Экономическая безопасность России: Общий курс / В.К. Сенчагов. – М.: Дело, 2005. – 896 с. EDN POCTNV

2. Долженкова Ю.В. Управление кадровой безопасностью организации: теория и практика / Ю.В. Долженкова, М.С. Токсанбаева. – М.: Прометей, 2024. – 188 с.

3. Есикова Р.С. Кадровая безопасность как одна из составляющих экономической безопасности организации / Р.С. Есикова // Социально-экономические явления и процессы. – 2017. – №6. – С. 14–19. EDN YNXFUD

4. Ибрагимова П.А. Кадровая безопасность: риски, угрозы, пути совершенствования / П.А. Ибрагимова, Х.Г. Гусайниева // Региональные проблемы преобразования экономики. – 2021. – №5. – С. 112–118. DOI 10.26726/1812-7096-2021-5-127-133. EDN FOBENH

5. Беккер Г. Человеческий капитал: Теоретический и эмпирический анализ / Г. Беккер. – Нью-Йорк: NBER, 1964.

6. Barney J. Firm Resources and Sustained Competitive Advantage / J. Barney // Journal of Management. – 1991. – Vol. 17. No. 1. – P. 99–120.

7. Махмудова И.Н. Кадровая безопасность: организация и управление / И.Н. Махмудова, Н.В. Соловова. – Самара: Самарский университет, 2022. – 156 с. EDN CRRSBA

8. Алавердов А.Р. Управление кадровой безопасностью организации: учебник и практикум / А.Р. Алавердов. – М.: Юрайт, 2020. – 234 с.

9. InfoWatch. Россия: утечки информации ограниченного доступа, 2023–2024: аналитический отчёт. – М., 2025. – URL: https://www.infowatch.ru (дата обращения: 30.01.2026).

10. Цветкова И.И. Оценка кадровой безопасности предприятия с помощью индикаторного подхода / И.И. Цветкова, Н.И. Клевец // Бюллетень науки и практики. – 2017. – №1. – С. 88–94. DOI 10.5281/zenodo.244250. EDN XHXRKJ

11. PwC. Global Economic Crime Survey 2024. – London: Pricewaterhouse-Coopers, 2024. – URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (дата обращения: 30.01.2026).

12. ACFE. Occupational Fraud 2024: A Report to the Nations. – Austin: Association of Certified Fraud Examiners, 2024.