УДК 331.5 DOI: 10.14451/1.256.669

исследование и анализ кадровых рисков организаций в цифровой среде

© 2026 **Махметова Айна-Жан Ербулатовна**
Кандидат экономических наук, доцент, доцент кафедры Отраслевое управление и экономическая безопасность. Саратовский государственный технический университет имени Гагарина Ю. А., Россия, Саратов.
E-mail: makhmetovaae@sstu.ru

© 2026 **Петров Антон Маркович**
Кандидат экономических наук, доцент, ведущий научный сотрудник Научно-исследовательского института развития образования. Российский экономические университет имени Г. В. Плеханова, Россия, Москва.
E-mail: petrov-am2000@yandex.ru

© 2026 **Пихтильков Иван Леонидович**
Аспирант кафедры Отраслевое управление и экономическая безопасность. Саратовский государственный технический университет имени Гагарина Ю. А., Россия, Саратов.
E-mail: pikhtilkov@inbox.ru

Ключевые слова: кадровые риски, механизм, управление, диагностика, HR, цифровизация, оценка, угрозы, информационная безопасность.

В данной статье исследуются кадровые риски организаций в условиях цифровой трансформации экономики, кардинально изменяющей трудовые отношения, компетенции персонала и механизмы обеспечения кадровыми ресурсами хозяйствующих субъектов. Цель исследования. Кадровая безопасность на современном этапе является одним из ключевых компонентов безопасности предприятия (организации). Именно поэтому оценка и диагностика причин и рискообразующих факторов в цифровой среде позволят получить полную информацию, необходимую для разработки эффективной модели управления кадровыми рисками и обеспечения экономической безопасности. Следовательно, возникает необходимость в совершенствовании методов их диагностики и адаптации к новым условиям. Цель работы – на основе исследования теоретических аспектов анализа и оценки рискообразующих факторов, причин и угроз их возникновения, выявить инструменты управления кадровыми рисками организаций в цифровой среде.
В статье представлен аналитический обзор рисков в цифровой среде, отдельно выделен блок кадровых рисков организаций в разрезе отраслей экономики. Представлены основные индикаторы оценки внутренних и внешних рискообразующих факторов в условиях цифровизации HR-процессов. Обоснован механизм управления кадровыми рисками в условиях цифровизации HR-процессов. Материалы и методы. Исследование проводилось по официальным данным Росстата за 2023–2025 гг., использовались материалы аналитических центров, материалы профессиональных сообществ, контент-анализ, а также дискурсивный анализ отчетной документации.

Результаты. Итоги проведенного исследования позволили выявить источники и причины возникновения кадровых рисков, методы их оценки. Доказано, что под влиянием цифровых технологий и постоянной трансформации HR появляются новые кадровые риски. Заключение. На основе анализа рискообразующих факторов предложен механизм управления кадровыми рисками в условиях цифровизации HR-процессов.

Введение

Реализация национального проекта «Экономика данных и цифровая трансформация государства» основана на сборе, анализе и мониторинге достаточного объема информации, что зачастую повышает значимость ключевых параметров и свойств получаемой информации, в частности, точности, объективности, доступности и достоверности. В результате сбора и обработки новых данных возникают различного рода риски, связанные в том числе с факторами внутренней и внешней среды, а также деятельностью самого персонала, что приводит к возникновению новых кадровых рисков, обусловленных усиливающимся процессом цифровизации.

По данным аналитических исследований, новые кадровые риски составляют до 80% от всех угроз. Страховая компания Allianz, опросив более 3000 экспертов по риск-менеджменту, включила кадровые риски в десятку основных рисков, представляющих угрозу функционированию организаций [13; 16]. По мнению экспертов, к числу основных кадровых рисков на современном этапе функционирования организаций относят: риск дефицита высококвалифицированных кадров, риск неконтролируемого повышения заработных плат, риск цифровизации бизнес-процессов, риск устаревания знаний, риск повышения неопределенности внешней среды, риск инфантилизации персонала (рост категории поколения Z в структуре трудоспособного населения) [2].

Методы и результаты исследования

Проблематика исследования причин возникновения кадровых рисков в организациях и факторов, оказывающих влияние на механизм управления ими в условиях трансформации кадровых процессов, привлекают особое внимание и отражены в многочисленных научных работах.

В целях минимизации кадровых угроз важно учитывать природу их возникновения, а именно источники, причины и рискообразующие факторы, способные спровоцировать наступление неблагоприятного события. В работе Митрофановой А. Е. выделены основные источники возникновения кадровых рисков: внешняя среда, неэффективность системы управления персоналом; поведение персонала [9]. Также подходы к классификации кадровых рисков с различными критериальными признаками представлены в работах многочисленных авторов, отмеченных в том числе в статье Сушко Н. А., Ковтуненко А. А. [14].

В исследованиях выделяется достаточное количество факторов риска, включая установки и мотивы самих людей, которые могут выступать основными причинами, побуждающими сотрудников к негативным действиям или бездействию [7; 14].

Наряду с этим, многие исследователи предлагают традиционный вариант классификации кадровых рисков через ключевые функции системы управления персоналом (риски подбора, развития и увольнения), поведения персонала (риски, связанные с умышленным и неумышленным поведением, кибербуллинг, риск нарушения цифровой этики, агрессивные комментарии), психофизиологические (риск перегрузки, стресс), и способов воздействия на персонал (негативное воздействие внутренних и внешних факторов). Подход же авторов с позиции учетной политики позволяет выделить кадровые риски: организационно-финансовые, квалификационные, поведенческие и функциональные [6].

В рамках анализа кадровых рисков организаций, связанных с выполнением трудовых функций, выделяют профессиональные риски [3], которые обеспечивают безопасность производства. В законодательстве (ТК РФ, приказ Роструда, приказы Министерства труда РФ и пр.) установлен ряд требований к оценке профессиональных рисков по классам вредности и опасности, а также требования к аккредитации специалистов, отвечающих за их оценку [5; 11].

Анализ кадровых рисков, применяемый экспертами, осуществляется достаточно стандартными методами диагностики и оценки рисков предприятий (организаций) [6]. Как правило, выделяют расчетно-аналитические методы: анализ чувствительности, метод Монте-Карло, экономико-статические методы, метод сценариев, экспертные методы, дерево решений, матричный метод, метод аналогий, фотохронометраж и т. д. Анализ кадровых рисков возможен на основе использования SWOT-анализа HR-политики, анализа показателя текучести, опросов удовлетворенности и вовлечённости сотрудников и HR-метрик.

Несмотря на появление цифровых технологий, классические методы оценки рисков являются базой, а правильный выбор и сочетание различных методов представляют детальную и комплексную диагностику выявленных рисков. Именно новые технологии являются основным драйвером эволюционных подходов к оценке рисков.

Эволюционное развитие инструментов оценки рисков [6; 12; 15]:

1. 2010 бумажные журналы и чек.
2. 2011 ручной анализ данных.
3. 2015–2020 Excel-матрицы.
4. 2021 автоматизация оценки.
5. 2025 развитие интегрированных платформ, использование VR-тренажеров, IoT-датчиков.
6. 2026 полностью автоматизированная оценка, предиктивная аналитика, проактивное управление данными.

В то же время наличие определенных кадровых рисков обусловливает необходимость всестороннего анализа их классификации, а также разработки механизма управления ими. Одним из инструментов выявления и оценки кадровых рисков выступает кадровый аудит, который включает различные методы и параметры проверок кадровых процессов. По результатам проведенного аудита применяют профилактические или корректирующие методы управления рисками. Сюда следует отнести: создание и внедрение регламентированной кадровой политики, стандартизацию кадровых процессов (подбора, адаптации, оценки, развития и увольнения), внедрение или обновление программы наставничества, обучение менеджеров навыкам командной работы, внедрение цифровых HR-систем и платформенных решений.

В целом, механизм управления кадровыми рисками представляет собой непрерывный процесс, который включает диагностику, оценку, мониторинг и минимизацию угроз, связанных с персоналом.

Ключевые этапы управления кадровыми рисками:

- Идентификация и диагностика (HR-аудит: анализ HR метрик).
- Оценка и приоритезация (ранжирование рисков, выявление размера ущерба).
- Разработка и внедрение мер реагирования (обучение, усиление безопасности и т. д.).
- Мониторинг и контроль (управление рисками, корректировка стратегии).

Как отмечают исследователи [15], структурный блок управления кадровыми рисками предполагает уровневую систему с позиции управляющей подсистемы: стратегический (высшее руководство), тактический (риск – менеджмент, служба), оперативный (руководители структурных подразделений).

В целом, оценивая масштабы охвата цифровыми технологиями системы управления персоналом, можно сделать вывод о том, что практически все HR-технологии – подбор, адаптация, оценка и аттестация, обучение и развитие, аудит, кадровое делопроизводство, мотивация, увольнение персонала – подвергаются автоматизации

с использованием современных программных решений.

Данный факт позволяет выявить факторы возникновения рисков с учетом влияния цифровизации на кадровые процессы. Безусловно, под влиянием цифровых технологий (ИИ, интернет вещей, автоматизация производства и управления, цифровые двойники, цифровизация HR и рабочих мест, гиг-занятость и пр.) происходит постоянная трансформация HR, что приводит к появлению новых кадровых рисков.

Таким образом, проблематика исследования кадровых рисков в условиях цифровой трансформации обусловлена высокой зависимостью от современных технологий, недостаточной цифровой грамотностью отдельных категорий сотрудников и киберугрозами. Соответственно, к методам управления кадровыми рисками можно отнести как классические: избегание, снижение, трансфер (передача) и удержание (принятие), так и нетрадиционные — мониторинг и проверка персонала, DLP-системы (защита от утечек), обучение сотрудников эффективной работе с данными, адаптация и трансформация HR-инструментов с учетом новых требований.

Эмпирический анализ

Современные организации используют комплексные системы управления рисками, включающие кадровые риски в общую матрицу рисков бизнеса. Так, компания «Новатек» регулярно оценивает и выявляет риски, связанные с деятельностью персонала, и включает их в карту рисков. Исследования показывают, что штатные сотрудники чаще допускают действия, ведущие к росту киберрисков (10% сотрудников генерируют 73% рисков).

К основным индикаторам оценки внутренних и внешних рискообразующих факторов в сфере HR в условиях цифровизации следует отнести: человеческий фактор (умышленные и неумышленные действия), утечка конфиденциальных данных, дефицит специалистов по информационной безопасности с цифровыми компетенциями, недостаточный уровень цифровой грамотности (низкая кибергигиена), поведенческие факторы и условия труда (фриланс, платформенная занятость), сложности внедрения новых технологий, психологические барьеры (сопротивление, страх замещения ИИ). Зачастую кадровые риски могут быть обусловлены цифровым разрывом между поколениями (возрастной риск, компетентностной риск), угрозами информационной безопасности (инсайдерский риск, риск безопасности данных), неэффективной настройкой алгоритмов ИИ персоналом.

Приведенные данные РБК показали отсутствие в российской финансовой сфере за последние 2 года инцидентов из-за случайных действий персонала, в основном все выявленные инциденты умышленные, что предполагает использование средств защиты информации (DLP-системы). По данным ТАСС, Роскомнадзор зафиксировал 118 случаев компрометации баз персональных данных (в 2025 г.), 135 утечек (в 2024 г.) (рис. 1) [4].

К числу рискообразующих факторов кадровых рисков следует отнести количество кибератак за 2024–2025 гг., которые в наибольшей степени были выявлены в промышленных организациях (17%), государственном секторе (11%), IT-компаниях (9%) и телекоммуникации (7%) (рис. 2). Так, 69% кибератак на промышленные объекты вызваны методами социальной инженерии, 79% — с применением вредоносного ПО, в 50% — использовалось ВПО для удаленного управления, в 41% — шифровальщики [1].

Так, по прогнозной оценке, в отраслевых компаниях отмечается дефицит специалистов по информационной безопасности (ИБ): профессионалом широкого профиля со знаниями в области управления рисками, юриспруденции с развитыми гибкими навыками, специалистов со знанием скриптовых языков, узкоспециализированных кадров (инженеров по ИБ, специалистов по киберкриминалистике, аналитиков, специалистов по Data Science). По данным исследования, уровень зарплатных предложений таких специалистов находится в диапазоне от 80 тысяч рублей для начинающих в регионах до 700 тысяч рублей с опытом работы более 8 лет.

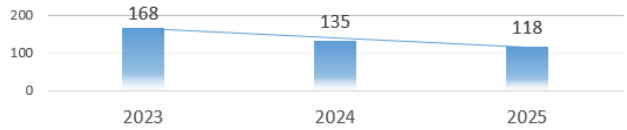

Рис. 1. Количество утечек данных за 2023–2025 гг.
Источник: составлено авторами по: [4].

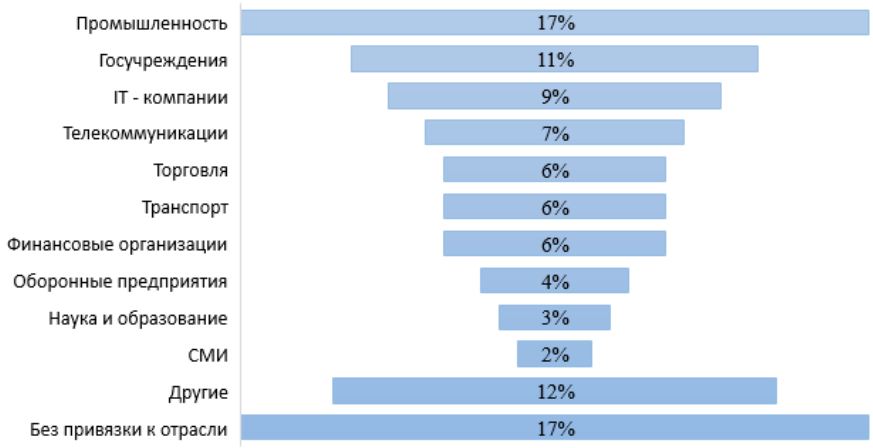

Рис. 2. Количество кибератак в разрезе отраслей экономики.
Источник: составлено авторами по: [1].

В этой связи, обучение сотрудников в сфере информационной безопасности является важным инструментом защиты от киберрисков. Эксперты отмечают, что киберугрозы становятся все более таргетированными и персонализированными, затрагивая важные системы управления бизнес-процессами.

Индикатор недостаточности уровня цифровой грамотности проанализирован в исследованиях Аналитического центра НАФИ, при этом выявлена наиболее уязвимая социальная группа, а именно сотрудники старше 55 лет по индексу цифровой грамотности (ИГ). Сравнение данных позволяет сделать вывод о том, что молодые специалисты могут выступать наставниками работников старшего возраста по показателям коммуникационной грамотности и навыкам решения проблем в цифровой среде (рис. 3) [17].

Решением данной проблемы является системное обучение, переобучение и развитие кадров в сфере информационной безопасности. Инвестиции в подготовку специалистов являются важной задачей современных организаций, позволяющей формировать кадровый потенциал с соответствующим уровнем цифровых компетенций. Данное решение существенно снизит риск цифрового разрыва между сотрудниками разных поколений в развитии соответствующих компетенций. К тому же, по мнению экспертов, к 2030 году люди старше 50 лет составят 49% населения и заинтересованы в обучении работе с искусственным интеллектом для повышения эффективности и сохранения конкурентоспособности.

Следует отметить, что для подготовки высококвалифицированных кадров для цифровой экономики, освоение цифровой грамотности и цифровых компетенций в рамках федеральной программы «Кадры для цифровой трансформации» (национального проекта «Экономика данных и цифровая трансформация государства») выделено 5,56 млрд рублей (в 2026 году), 6,13 млрд рублей (в 2027-м).

По данным «Авито Подработка» интерес к временной подработке соискателей 55–64 лет увеличился на 34%, а 44% опрошенных планируют подрабатывать в 2026 году. Данные тенденции показывают, что рынок труда становится более

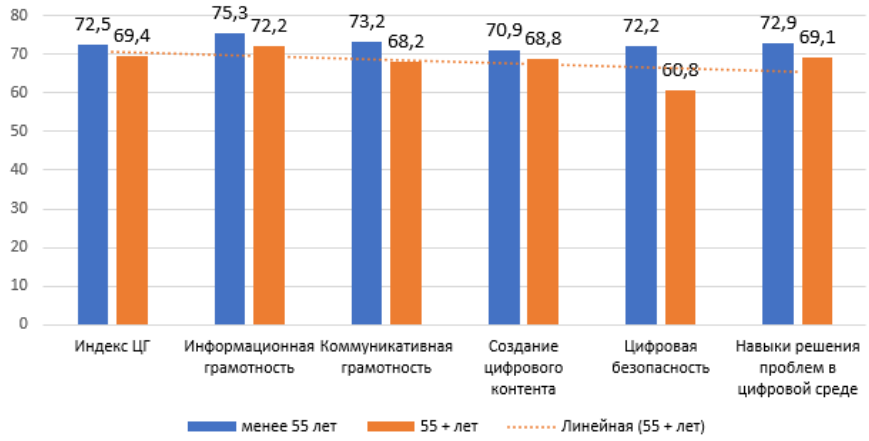

Рис. 3. Индекс ЦГ сотрудников (данные Аналитического центра НАФИ).
Источник: составлено авторами по: [17].

гибким, а использование искусственного интеллекта переходит в системные элементы работы с персоналом [18].

Существенное влияние на процессы организации влияют кадровые риски работников, работающих в удаленном и гибридном формате. В данном случае, эти факторы и условия труда порождают такие риски, как риски снижения контроля и мониторинга, риски нарушения ТК РФ и норм охраны труда, риски, связанные с эмоциональным выгоранием, низкий уровень владения тайм-менеджментом, риски снижения работоспособности, риски, связанные с техническими сбоями.

Психологические барьеры, в частности, сопротивление со стороны персонала нововведениям зачастую носит временный характер. Для преодоления данного барьера экспертами предлагаются различные инструменты информационного воздействия на персонал (переговоры, разъяснения, вовлечение в процесс, мотивационные тренинги, соглашение, создание группы-проводников) (рис. 4). Таким образом, сопротивление персонала кадровым изменениям представляет собой показатель уровня сформированной компетентности управленческого персонала, а также потенциал успешного взаимодействия.

В отношении оценки и управления профессиональными рисками применяют современные инструменты: ИИ, умные датчики, VR-тренажеры, AR-инструкции, централизованные IT-системы, системы видеоаналитики, которые существенно снижают уровень травматизма и повышают общую культуру безопасности [10]. В частности, Новолипецкий металлургический комбинат применяет электронные наряды-допуски и IT-системы для глубокого анализа системных рисков и снижает уровень повышенной опасности на производстве. Группа компаний «А101» использует результаты анализа профессиональных рисков для совершенствования системы безопасности. Иркутская нефтяная компания оценивает риски и внедряет их в систему менеджмента охраны здоровья и безопасности труда (ISO 45001) [8].

ПАО «Сбербанк» в целях минимизации кадровых рисков использует комплексный подход, в частности, разработка программ обучения (Smart – развитие), взаимодействие с молодыми талантами (хакатоны, акселераторы, соревнования в Data Science), ротация и горизонтально-вертикальное продвижение, поиск и сохранение потенциала сотрудников.

В силу определенных причин в управлении кадровыми рисками могут возникнуть ошибки, усиливающие общие кадровые угрозы. В частности, использование и копирование лучших HR-практик без учёта специфики деятельности организации, недостаточная работа с молодыми

Рис. 4. Инструменты воздействия на персонал для преодоления сопротивления персонала HR-инновациям.

специалистами, проблемы обратной связи, отсутствие единой кадровой стратегии. Все перечисленные ошибки существенно снижают уровень вовлечённости на 15% и производительность на 30%, а также повышают уровень текучести на 25% [16].

Заключение

Таким образом, для снижения кадровых рисков необходим комплексный подход, в частности, развитие национальных решений в области информационной безопасности, модернизация HR-инфраструктуры, внедрение системного мониторинга и повышение уровня цифровой грамотности сотрудников, внедрение цифровых HR-систем, регулярное обучение специалистов кадровых служб, разработку четких регламентов и страхование трудовых рисков.

Реализация предложенного механизма управления кадровыми рисками в условиях цифровизации HR-процессов позволит организациям не только минимизировать существующие угрозы, но и выстроить проактивную систему раннего выявления и предупреждения новых рискообразующих факторов. Особую значимость при этом приобретает интеграция аналитических инструментов на основе больших данных и искусственного интеллекта в процессы принятия кадровых решений.

Библиографический список

1. CODE RED 2026: Актуальные киберугрозы для российских организаций. — URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (дата обр. 15.02.2026).
2. *Батоврина Е. В.* Кадровые риски в управлении персоналом российских инновационных организаций // Теория и практика общественного развития. — 2025. — № 11. — С. 42—53. — DOI: 10.24158/tipor.2025.11.3.
3. *Блинова У. Ю.*, *Евстафьева Е. М.* Оценка кадровых рисков в системе цифрового бухгалтерского учета // Бизнес. Образование. Право. — 2024. — 2(67). — С. 174—178. — DOI: 10.25683/VOLBI.2024.67.1008.
4. В России снизилось число утечек персональных данных в 2025 году. — URL: https://tass.ru/obschestvo/26216171 (дата обр. 20.02.2026).
5. *Долженкова Ю. В.*, *Камнева Е. В.*, *Сафонов А. Л.* Управление кадровой безопасностью организации: Учебник для бакалавриата и магистратуры / под ред. Ю. В. Долженковой. — 2-е изд. — М. : Прометей, 2024.
6. *Калмыкова О. Ю.*, *Гагаринская Г. П.*, *Чечина О. С.* Кадровый риск-менеджмент: инновации и практика // Вестник Евразийской науки. — 2020. — № 6. — URL: https://esj.today/PDF/74ECVN620.pdf (дата обр. 10.02.2026).
7. *Коновалова О. В.*, *Морозова И. В.*, *Козлова Е. Г.* Управление кадровыми рисками хозяйствующего субъекта в условиях цифровизации общества // Вестник Московского государственного областного университета. Серия Экономика. — 2020. — № 2. — С. 68—75. — DOI: 10.18384/2310-6646-2020-2-68-75.
8. Минимизация кадровых рисков в бизнесе: как защитить компанию от неожиданных потерь. — URL: https://maxistaff.ru/blog/kadrovye-riski-v-biznese (дата обр. 20.02.2026).
9. *Митрофанова А. Е.*, *Захаров Д. К.*, *Ашурбеков Р. А.* Кадровые риски и их оценка : учебное пособие. — М. : Инфра-М, 2024. — 137 с.
10. Оценка профессиональных рисков 2025–2026: от матриц до искусственного интеллекта. — URL: https://www.mostrudexpert.ru/infocentr/otsenka-professionalnyh-riskov-2025-2026-ot-matrits-do-iskusstvennogo-intellekta-polnyy-gid-po-sovremennym-podhodam (дата обр. 20.02.2026).
11. Приказ Минтруда России от 28.12.2021 года № 926 «Об утверждении рекомендаций по выбору методов оценки уровней профессиональных рисков и по снижению уровней таких рисков».

12. Рейтинг российских компаний по качеству управления персоналом. — URL: https://raex-rr.com/ESG/ESG_companies/HR_development/2025/analytics/HR_development_ranking/ (дата обр. 21.02.2026).
13. *Родин Д. В.*, *Шарашкина Т. П.* Кадровые риски и обеспечение кадровой безопасности на промышленном предприятии // Вестник Алтайской академии экономики и права. — 2025. — № 8—2. — С. 213—221. — URL: https://vaael.ru/ru/article/view?id=4293 (дата обр. 20.02.2026).
14. *Сушко Н. А.*, *Ковтуненко А. А.* Классификация рисков кадровой безопасности предприятия // Аллея науки. — 2022. — № 11. — URL: https://alley-science.ru/domains_data/files/1November2022/KLASSIFIKACIYa%20RISKOV%20KADROVOY%20BEZOPASNOSTI%20PREDPRIYaTIYa.pdf (дата обр. 20.02.2026).
15. *Тераз В. А.* Ижевск : учебно-методическое пособие. — Удмуртский университет, 2025. — 49 с. — URL: http://elibrary.udsu.ru/xmlui/bitstream/handle/123456789/23062/209%d0%bb%d0%b1_1001030139_10.04.2025.pdf?sequence=1 (дата обр. 10.02.2026).
16. Цифровой Армагеддон: Allianz определила главные бизнес-риски 2026 года. — URL: https://adpass.ru/biznes-riski-2026/ (дата обр. 20.02.2026).
17. Цифровой разрыв: каждый третий россиянин старше 55 лет боится остаться за бортом технологий. — URL: https://nafi.ru/polls/tsifrovoy-razryv-kazhdyy-tretiy-rossiyanin-starshe-55-let-boitsya-ostatsya-za-bortom-tekhnologiy/ (дата обр. 15.02.2026).
18. Число резюме людей 55–64 лет с компетенциями в сфере ИИ выросло на 21% / РБК. — URL: https://trends.rbc.ru/trends/social/699727bc9a794779fa3a192c?from=copy (дата обр. 20.02.2026).