УДК 336.64:519.23
DOI: 10.17586/2310-1172-2026-19-2-43-52
Научная статья
Язык статьи – русский

Использование инструментов проактивного подхода управления рисками предприятия в условиях развития информационных технологий и искусственного интеллекта

Канд. экон. наук, доц. **Мартыненко О.В.** martynenko@igps.ru
Канд. экон. наук **Полещук С.М.** sv.poleshchuk@gmail.com
Канд. пед. наук, доц. **Печеневская М.А.** pechenevskaja76@mail.ru
Канд. экон. наук. **Скоробогатов М.В.** mvskor@rambler.ru
Исаев А.А. artem_isaev1@mail.ru
Санкт-Петербургский университет Государственной противопожарной службы Министерства чрезвычайных ситуаций России имени Героя Российской Федерации генерала армии Е.Н. Зиничева
Россия, Санкт-Петербург

Актуальность исследования заключается в необходимости решения современных проблем кибербезопасности, с которыми сталкиваются предприятия, с помощью проактивного управления и с учетом текущих изменений в цифровых технологиях. Так, в статье рассматриваются особенности применения в условиях цифровизации и распространения применения искусственного интеллекта инструментов проактивного подхода к управлению рисками предприятия. Применение данного метода способствует опережающему выявлению и предупреждению рисков относительно реактивного подхода управления ими. Ключевой элемент такого подхода – карта рисков, позволяющая систематизировать и приоритизировать киберугрозы, связанные с использованием интеллектуальных технологий, выступающая предметом исследования. Применение данного инструмента в проактивном управлении позволит формировать эффективную стратегию кибербезопасности и повышения устойчивости предприятия к современным цифровым рискам. Целью исследования является анализ возможностей применения карты рисков как инструмента проактивного управления для обеспечения кибербезопасности предприятия в условиях ускоренного развития информационных технологий и искусственного интеллекта. Объектом исследования данной работы выступают процессы управления предприятием в рамках обеспечения кибербезопасности предприятия. В ходе исследования были использованы следующие методы: анализ и синтез, индукция и дедукция, систематизация и обобщение научных данных, сравнительный и логический анализ, а также методы визуализации и экспертной оценки рисков. Сутью эксперимента выступает проверка способности карты рисков как инструмента проактивного подхода управления предприятием к снижению уровня рисков в моделируемой ситуации. Результаты исследования направлены на обоснование эффективности применения карты рисков в системе управления кибербезопасностью организации и могут быть использованы при разработке практических рекомендаций по повышению уровня защищённости предприятий от современных киберугроз. Результаты исследования рекомендованы к применению в процессе управления предприятиями.

Ключевые слова: кибербезопасность, проактивное управление, риски, карта рисков, искусственный интеллект, информационная безопасность, экономическая безопасность, управление предприятием.

Ссылка для цитирования:
Мартыненко О.В., Полещук С.М., Печеневская М.А., Скоробогатов М.В., Исаев А.А. Использование инструментов проактивного подхода управления рисками предприятия в условиях развития информационных технологий и искусственного интеллекта // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2026. № 2. С. 43-52. DOI: 10.17586/2310-1172-2026-19-2-43-52.

Scientific article
Article in Russian

Using tools for a proactive approach to enterprise risk management in the context of developing information technology and artificial intelligence

Ph.D. **Martynenko O.V.** martynenko@igps.ru
Ph.D. **Poleshchuk S.M.** sv.poleshchuk@gmail.com
Ph.D. **Pechenevskaya M.A.** pechenevskaja76@mail.ru
Ph.D. **Skorobogatov M.V.** mvskor@rambler.ru
Isaev A.A. artem_isaev1@mail.ru
Saint-Petersburg University of State Fire Service of Emercom of Russia
Russia, Saint Petersburg

The relevance of this study lies in the need to address modern cybersecurity challenges faced by enterprises through proactive management, taking into account ongoing changes in digital technologies. This article examines the application of proactive risk management tools in the context of digitalization and the widespread use of artificial intelligence. This method facilitates the proactive identification and prevention of risks, compared to a reactive approach to risk management. A key element of this approach is a risk map, which allows for the systematization and prioritization of cyber threats associated with the use of intelligent technologies, which is the subject of this study. The use of this tool in proactive management will enable the development of an effective cybersecurity strategy and increase the enterprise's resilience to modern digital risks. The aim of this study is to analyze the potential of using a risk map as a proactive management tool to ensure enterprise cybersecurity in the context of the accelerated development of information technology and artificial intelligence. The object of this study is enterprise management processes within the context of ensuring enterprise cybersecurity. The following methods were used in the study: analysis and synthesis, induction and deduction, systematization and generalization of scientific data, comparative and logical analysis, as well as visualization and expert risk assessment methods. The experiment aimed to test the ability of a risk map as a proactive management tool for mitigating risks in a simulated situation. The results of the study are aimed at substantiating the effectiveness of risk mapping in an organization's cybersecurity management system and can be used in developing practical recommendations for improving enterprise security from modern cyberthreats. The results of the study are recommended for use in enterprise management.
Keywords: cybersecurity, proactive management, risks, risk mapping, artificial intelligence, information security, economic security, enterprise management.

For citation:
Martynenko O.V., Poleshchuk S.M., Pechenevskaya M.A., Skorobogatov M.V., Isaev A.A. Using tools for a proactive approach to enterprise risk management in the context of developing information technology and artificial intelligence. *Scientific journal NRU ITMO. Series «Economics and Environmental Management».* 2026. № 2. P. 43-52. DOI: 10.17586/2310-1172-2026-19-2-43-52.

Введение

С развитием цифровых технологий растет и число киберугроз, которые представляют серьёзный вызов для хозяйствующих субъектов. Кибератаки становятся все более изощренными, наносят значительный финансовый ущерб, подрывают доверие клиентов и замедляют внедрение технологий. Для успешной цифровой трансформации предприятий важно не только развивать инновации, но и защищать финансовые активы и данные от утечек и несанкционированного доступа. Именно поэтому увеличение уровня кибербезопасности сегодня является одной из приоритетных задач для обеспечения экономической безопасности предприятий и всей страны [1].

Традиционные подходы к управлению рисками, ориентированные на реагирование на уже реализовавшиеся угрозы, в условиях высокой динамики цифровой среды и стремительного распространения информации становится малоэффективными. В этой связи наблюдается необходимость рассмотрения и последующего внедрения методов проактивного подхода, которые подразумевают выявление не содержания рисков, а их «источников». Содержание, виды рисков не являются предопределенными, так как могут возникать новые виды рисков, предусмотреть которые невозможно [2].

Одним из ключевых инструментов проактивного подхода является построение системы управления рисками на основе карты рисков. Применение данного инструмента позволяет идентифицировать угрозы предприятия и определять их приоритетность на основе вероятности возникновения и потенциального ущерба. Целью построения карты рисков является формирование основы для разработки комплекса мер по предупреждению угроз.

Методы и материалы

Исследование базируется на применении универсальных и специализированных исследовательских методов, включая наблюдение, обобщение, анализ и синтез, индуктивный и дедуктивный подходы, упорядочивание данных, сопоставление и логический разбор, построение организационных моделей, проведение экспертных оценок, визуализацию результатов в таблицах и графиках, а также использование структурно-функционального анализа.

Теоретической основой материала для исследования послужили труды представителей классических и современных отечественных и зарубежных научных школ в таких научных областях, как управление рисками, проактивное управление, функционирование субъектов в изменяющихся условиях, риски, цифровые технологии, кибербезопасность.

Информационной основой материала для исследования выступили нормативно-правовые акты, справочные документы, статистический и аналитический материал в области кибербезопасности, публикации в научных и научно-практических изданиях.

Киберугрозы, с которыми сталкивается предприятие, и их основные характеристики

Современное цифровое пространство характеризуется высокой динамичностью и необходимости обработки больших объемов информации, что непосредственно отражается на деятельности хозяйствующих субъектов. В данных условиях традиционные угрозы, наиболее часто связанные с техническими уязвимостями, постепенно уступают место новым формам опасностей, которые, связаны преимущественно с манипулированием информацией и компрометацией данных. Это, в свою очередь, расширяет зону появления возможных рисков, и усложняет процесс разработки мер по их предупреждению и ликвидации. Таким образом, современные цифровые условия формируют новые риски, проявляющиеся в конкретных формах угроз, с которыми предприятия сталкиваются ежедневно. На рис. 1 представлены наиболее характерные формы киберугроз предприятия.

Рис. 1. Формы современных киберугроз предприятия

Кибербезопасность предприятия выступает комплексной категорией, объединяющей технические, организационные и экономические аспекты зашиты информационных ресурсов и бизнес-процессов от киберугроз. Рисунок 1 позволяет выделить основные векторы риска: нарушение доступности к информационным системам, нарушение конфиденциальности и целостности информации, а также использование вредоносного ПО

и инструментов кибершпионажа в отношении данных предприятия [3]. Киберугрозы, представленные на рис. 1, приводят не только к прямым расходам и расходам на ликвидацию негативных последствий, но и к репутационному ущербу компании, снижению доверию со стороны контрагентов и клиентов. В долгосрочной перспективе это отражается на конкурентоспособности и финансовой устойчивости предприятия.

Быстрые темпы развития и внедрения технологий создают новые виды опасностей. Несмотря на повсеместное использование нейросетей, данный инструмент еще не стал главной причиной киберугроз предприятия. Так, случаи реального применения искусственного интеллекта (далее также ИИ) в сложных целевых атаках по итогам 2025 года остаются единичными, однако ИИ-инструменты уже сегодня позволяют киберпреступникам автоматизировать и удешевить создание фишингового контента и дипфейков, упростить масштабирование атак и улучшить процессы разведки. Эксперты утверждают, что в 2025 году ИИ массово использовался для генерации дипфейков, фишинговых рассылок и ресурсов для разведки и сбора информации о жертвах. Выявленные случаи использования нейросетей для написания вредоносного кода, скриптов, а также непосредственно участия в атаках в 2025 году носят пока лишь единичный характер. Последствия некоторых кибератак, полностью основанных на ИИ демонстрируют разрушительный потенциал цифровых инструментов нового поколения. Также эксперты утверждают, что вероятно, уже в ближайшее время мы столкнемся с полностью автоматизированными ИИ-атаками [4].

Отдельного внимания заслуживает автоматизация кибератак: злоумышленники с помощью алгоритмов машинного обучения анализируют большие объёмы данных, выявляют уязвимости информационных систем и выбирают наиболее эффективные методы атак. Следовательно, кибератаки становятся более точечными и менее зависимыми от человеческого фактора. Так же как указано выше практикуется применение искусственного интеллекта, но уже как инструмента обхода и адаптации к средствам защиты. Другую существенную угрозу представляет использование искусственного интеллекта в целях социальной инженерии. Алгоритмы способны генерировать персонализированные сообщения от имени руководства компании, сохраняя характерный стиль общения. Данный инструмент используется в целях информационных манипуляций, проблемой в данном случае является отсутствие установленной связи между профилем и реальным человеком [5]. В таблице 1 представлен наиболее исчерпывающий список угроз кибербезопасности предприятия, связанных с использованием искусственного интеллекта и их краткая характеристика.

Таблица 1

Угрозы кибербезопасности предприятия, связанные с использованием искусственного интеллекта, и их краткая характеристика

№ п/п	Угроза	Характеристика
1	Компрометации данных	Искажение, компрометация или подмена данных злоумышленниками, приводящая к ошибочным выводам и неверным управленческим решениям
2	Манипулирование ИИ-системами	Внешнее воздействие на ИИ, применяемый в компании для целенаправленного искажения анализа
3	Автоматизация и интеллектуализация кибератак	Повышение эффективности кибератак (автоматизированный поиск уязвимостей, постоянная адаптация) посредствам использование ИИ
4	Репутационный ущерб и информационные атаки	Создание и распространение дипфейков для распространения дезинформации, дискредитации компании, подрыва доверия к руководству или манипулирование партнерами и клиентами
5	Использование ИИ в социальной инженерии	Создание персонализированных сообщений, имитирующий стиль деловой переписки сотрудников и руководства
6	Риск ошибок и смещения в работе ИИ	Смещение данных и деградация ИИ в условиях изменяющейся цифровой среды способствует снижению точности анализа и выявления угроз
7.	Зависимость от интеллектуальных систем	Снижение роли экспертного контроля в связи с автоматизацией бизнес-процессов и принятие решений при помощи ИИ; уязвимость в силу утраты навыков ручного анализа и реагирования

Представленная таблица свидетельствует о том, что технология искусственного интеллекта одновременно усиливает и диверсифицирует существующие киберугрозы предприятия (автоматизация кибератак,

компрометация данных и пр.) и становится источником новых (манипулирование ИИ-системами, использование ИИ в социальной инженерии и пр.).

Наиболее важной внешней угрозой любого предприятия является кибератака. По итогам 2025 года выявлено, что главной целью для злоумышленников являются государственные учреждения и государственные компании. Так, на них приходятся атаки 13 APT групп. Группа APT, или Advanced Persistent Threat, – это группа киберпреступников, специализирующихся на сложных постоянных угрозах. Обычно это киберпреступники из государственных организаций или организаций, которые работают от имени государств. Всего за 2025 год выявлено в России и СНГ таких атак от 27 групп. На рис. 2 представлена подробная инфографика атак APT групп за 2025 год [4].

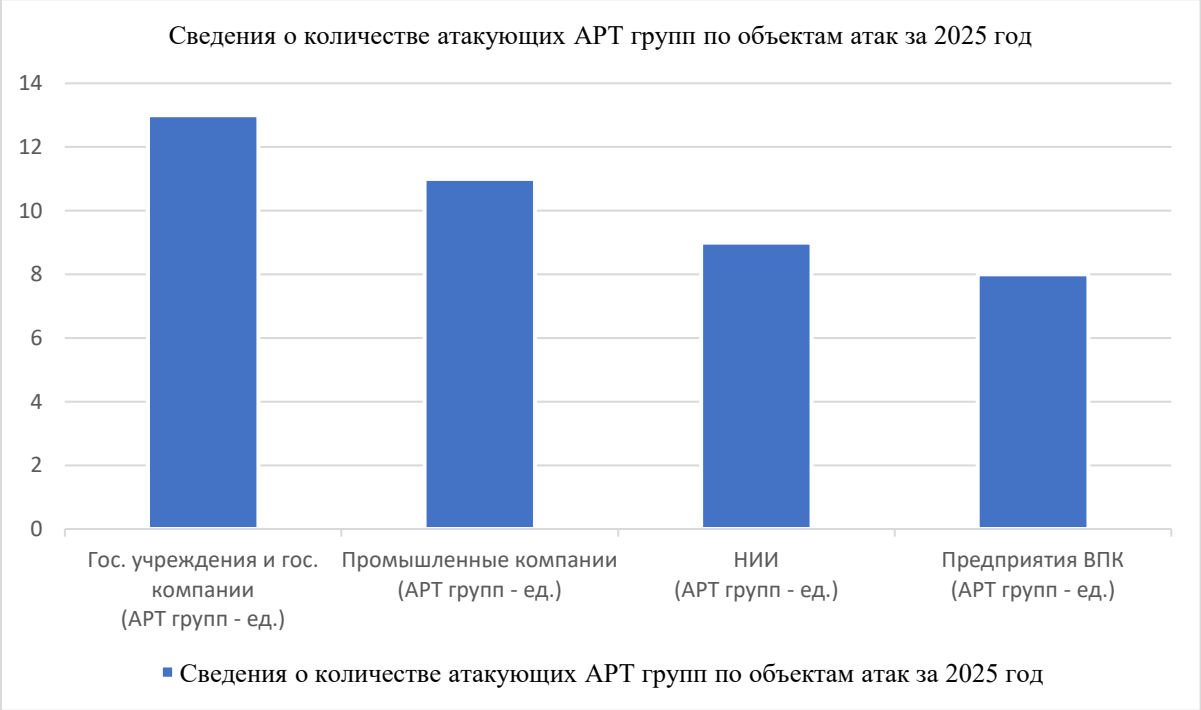

Рис. 2. Количество APT групп и объекты их атак за 2025 год

Также стоит отметить, что в 2025 году выросло на 15% количество атак, связанных с вымогательством. Главными целями таких атак стали средний и крупный бизнес. Чаще всего вымогатели атаковали производственные и инжиниринговые компании (17,1%), организации из сфер оптовой (14,3%) и розничной торговли (12,9%), информационных технологий (7,1%), транспорта и логистики (7,1%) [4].

Угроза компрометации данных особенно чувствительна на сегодняшний день в России и странах СНГ. Так в 2025 году было выявлено 230 новых публикаций баз данных российские компаний, еще 10 публикаций баз данных белорусских компаний и 10 публикаций данных компаний из стран СНГ. Суммарное количество записей, попавших в открытый доступ и содержащих данные россиян, составляет около 800 млн строк. Данные, затрагивающие белорусские компании, составляют 232 тыс. записей. Злоумышленники помимо публикации данных могут использовать их для последующего проведения каскадных атак на крупные организации коммерческого и государственного сектора [4].

Подводя итог вышеизложенному, можно с уверенностью заключить, что в современных реалиях для предприятия существует большое количество киберугроз, которые имеют различные формы, их количество постоянно растет и они непрерывно совершенствуются. В России в ближайшие годы ландшафт киберугроз во многом будет зависеть от политической ситуации. В условиях обострения геополитической ситуации ожидается усиление кибератак как со стороны политически мотивированных групп (хактивистов), так и упомянутых государственных APT-слоев, на российские предприятия. Количество атакующих групп и масштаб ущерба от их деятельности, скорее всего, будут увеличиваться. Для того чтобы комплексно оценить ситуацию с киберугрозами для предприятия, а на этом основании построить систему проактивного управления рисками по ним и тем самым их митигировать, необходимо разобраться в том числе в последствиях таких угроз.

Последствия киберугроз для предприятия

Главным последствием, но не единственным, любой кибератаки на предприятие как предпринимательскую структуру являются, конечно же, финансовые потери.

Наиболее распространенные последствия кибератак на отечественные предприятия — это утечка конфиденциальной информации и нарушение основной деятельности компаний. Эти два последствия часто взаимосвязаны. Например, злоумышленники могут сначала получить доступ к внутренним системам компании и незаметно извлечь ценные данные, после чего запустить шифровальщик, который парализует ключевые бизнес-процессы – от документооборота до работы сервисов, производственных систем и клиентских платформ.

Такая стратегия позволяет киберпреступникам добиться двойного эффекта: шантажировать организацию угрозой публикации или продажи украденных данных (так называемый double extortion) и одновременно требовать выкуп за восстановление доступа к системам. Такие инциденты ведут не только к финансовым потерям, но и существенно уменьшают доверие партнеров и клиентов. В условиях ужесточения законодательства по защите персональных данных, такие утечки становятся особенно опасными, поскольку могут повлечь крупные штрафы и серьезные репутационные риски.

Соответственно, важным последствием кибератак и утечки данных компаний является также репутационный ущерб. В отличие от прямых финансовых потерь, репутационный ущерб носит пролонгированный характер и выражается в снижении уровня доверия со стороны партнеров, потребителей и инвесторов. Важно отметить, что организации, функционирующие в сферах, связанных с обработкой персональных и финансовых данных, в наибольшей степени подвержены кибератакам, а следовательно, имеют наиболее суровые последствия таких атак. Данная характеристика обоснована тем, что последствия киберинцидентов усиливаются не только общественным резонансом, но и возможными регуляторными санкциями [6].

Говоря о репутационном ущербе для предприятий, нельзя не отметить складывающуюся в этом направлении тенденцию в части массового информирования о проведении в отношении предприятия кибератак. Мы можем с уверенностью констатировать, что в отличие от общемирового тренда, когда атакующие стараются без лишнего шума закрепиться в инфраструктуре, чтобы незаметно шпионить за жертвой или готовиться к будущей масштабной диверсии, проведенные в 2025 году атаки на российские транспортные компании и торговые сети, были очень громкими. Они сопровождались публикацией утечек данных, информационными вбросами и кампаниями по дискредитации пострадавших.

Примером проявления манипулирования ИИ-системами и социальной инженерии может служить заражение устройств с операционной системой Android. Данная угроза хоть и косвенно затрагивает отнесенность компаний, но все равно является важным аспектом кибербезопасности. Так, на протяжении 2025 года эксперты фиксировали множественные случаи использования вредоносного программного обеспечения (далее также ПО), ориентированного на клиентов ведущих российских банков. В итоге, общий ущерб клиентов банков, подвергшихся только одной вредоносной программе «NFCGate», за 10 месяцев 2025 года составил не менее 1,6 млрд рублей [4].

К внутренним угрозам предприятия, связанным с использованием искусственного интеллекта, можно отнести риск ошибок и смещение в работе ИИ. Под этим следует понимать систематическое отклонение результатов моделей от объективной реальности вследствие не репрезентативности обучающих данных, алгоритмических ограничениях и пр. Реализация данного риска приводит к снижению точности моделей ошибочным решениям.

Также можно выделить риск зависимости предприятий от интеллектуальных систем. Искусственный интеллект самостоятельно генерирует паттерны поведения и выбирает решения без участия человека. Поэтому, если данные для тренировки и обучения нейросети были некорректными, то вероятность ошибочных решений будет высокой. Для предприятий это означает существенные потери денежных средств и риск банкротства [7].

В общем смысле, угрозы, представленные в таблице 1, обладают такими общими характеристиками как латентность и комплексность воздействия. Чаще всего они формируется постепенно, маскируясь под легитимную цифровую деятельность, но проявляются в тот момент, когда ущерб компании уже нанесен. Также ожидается увеличение атак с использованием ИИ как в части разработки ВПО, так и в части внедрения больших языковых моделей для его работы в момент зарождения.

Таким образом, актуальные угрозы кибербезопасности предприятия отличаются высокой скоростью распространения, возможностью масштабируемости и легкодоступны для злоумышленников. Следовательно, необходимо определить, насколько эффективно традиционные и проактивные методы управления способны идентифицировать и предупреждать данные угрозы.

Обеспечение кибербезопасности путем использования карты рисков как инструмента проактивного управления рисками предприятия

Принято выделать два базовых подхода к решению проблемы управления рисками – подход, основанный на традиционных методах, и подход, основанный на методах проактивного управления.

Традиционный подход к управлению рисками представляет собой систему управления, ориентированную на реагирования на уже реализовавшиеся угрозы и минимизацию последствий произошедших инцидентов [7]. Данный подход базируется на анализе прошлых событий, использует исторические данные и сигнатуры известных угроз, а его основная цель заключается в восстановлении работоспособности системы и снижении ущерба после наступления негативного события. Традиционный подход в контексте обеспечения кибербезопасности направлен на защиту технической инфраструктуры. Сущность данного подхода заключается в обнаружение и ликвидации последствий кибератак, в частности – в восстановлении работоспособности систем и минимизации ущерба. Иное название данного подхода – реактивный, связано с реализацией защитных механизмов после выявления последствий фактов нарушения безопасности. К основным средствам данного подхода можно отнести антивирусные программы, системы обнаружения и предотвращения вторжения. Указанные средства демонстрируют высокий уровень эффективности при противодействии известным угрозам, однако они неспособны противостоять современным угрозам кибербезопасности, характеризующиеся наличием способностью адаптироваться к разным видам защиты. Для реактивного подхода характерно наличие точных оценок последствий возникших инцидентов, а основной его целью является нейтрализация негативных последствий уже произошедших событий [8].

Проактивный подход к управлению рисками представляет собой систему управления, ориентированную на выявление и устранение источников и причин возникновения рисков до того, как они реализуются в негативное событие. В отличие от традиционного подхода, проактивное управление фокусируется не на содержании и видах рисков, а на их первопричинах и драйверах, используя прогнозные модели, анализ трендов и технологии искусственного интеллекта для предвиденья угроз. Развитию проактивного управления способствует использование цифровых технологий, в частности обработка больших данных, внедрение искусственного интеллекта, автоматизация процесса принятия управленческих решений. При проактивном управлении основной целью принимаемых решений является предупреждение возникновения различных неблагоприятных событий, приводящих к развитию рисков. Данный подход ориентирован на использование прогнозных оценок развития рисков и применяется для латентной части их жизненного цикла в условиях дефицита информации о величине возможных последствий развития негативных событий [8]. Таким образом, проактивное управление направлено на устранения причин негативных событий, поэтому вероятность их возникновения можно минимизировать, если своевременно выявлять и оценивать риск. Если говорить кратко, то по своей сути – это управление на опережение [9]. К основным средствам данного подхода можно отнести поиск уязвимостей, осуществление контроля за угрозами, регулярную проверку системы и защиты. Также необходимо отметить, что использование больших объемов данных, выявление скрытых закономерностей и прогнозирование рисковых сценариев позволяет повысить точность оценки рисков и снизить зависимость от субъективных факторов при обеспечении кибербезопасности [10].

Базовым и ключевым элементом проактивного подхода являются визуализация и систематизация рисков, позволяющая при выстраивании системы управления не только выявлять потенциальные угрозы, но и оперативно расставлять приоритеты в защите. Эффективным инструментом для реализации таких задач является карта рисков, которая предоставляет наглядное представление вероятности возникновения угроз и их потенциального воздействия. Карта рисков – это инструмент для наглядного представления важных для компании рисков, при формировании которого дается взвешенная оценка рискам и расставляется приоритетность и отношении мероприятий по их снижению [8]. Использование данного инструмента позволяет предприятиям фокусировать ресурсы на наиболее критичных направлениях защиты, выявлять «слепые зоны» безопасности и интегрировать превентивные меры в общую стратегию кибербезопасности [11]. Таким образом, карта рисков становится логическим продолжением проактивного подхода, обеспечивая переход от концепции опережающего управления угрозами к конкретной практической реализации мер защиты.

Как правило, карта рисков – это графическое и текстовое описание ограниченного числа рисков, расположенных в прямоугольной таблице, по одной «оси» которой указана сила воздействия или значимость риска, а по другой – вероятность или частота возникновения [12]. Также матрица имеет цветные ячейки, где зеленый цвет характеризует уровень угрозы как низкоприоритетный, оранжевый – значимый, красный – критический.

Для построения карты рисков были использованы данные табл. 1, распределение рисков в матрице будет осуществляться с учетом общепринятой методологии управления рискам в области кибербезопасности (ГОСТ Р ИСО/МЭК 27005-2010; ГОСТ Р ИСО 31000-2019) [13,14]. Кроме того, предложенная карта рисков учитывает

стремительное внедрение технологий искусственного интеллекта в управлении организациями, которое в результате трансформирует как операционные процессы, так и стратегическое планирование, но вместе с тем, имеет ошибки и, как следствие, негативные эффекты [15].

Диверсификация рисков проводилась следующим образом:

1. Риск компрометации данных отнесён в зону высокой вероятности и высокого ущерба, поскольку, по данным экспертов, в 2025 году было выявлено 230 новых публикаций баз данных российских компаний, а суммарное количество скомпрометированных записей достигло 800 млн строк.
2. Риск манипулирования ИИ-системами помещён в зону средней вероятности и среднего ущерба, так как подобные атаки требуют высокой квалификации и пока встречаются реже, но их последствия могут быть значительными.
3. Риск автоматизации кибератак и использования ИИ в социальной инженерии отнесены к зоне низкой вероятности, но высокого ущерба — это «слепые зоны», требующие мониторинга.
4. Риск ошибок и смещения в работе ИИ и риск зависимости от интеллектуальных систем расположены в зоне средней вероятности и среднего ущерба.
5. Репутационный ущерб отнесён в зону низкой вероятности, но высокого ущерба, поскольку громкие инциденты с дипфейками пока единичны, но их последствия могут быть катастрофическими.

Итоговое распределение рисков, перечисленных в табл. 1, наглядно представлено на рис. 2.

Высокая вероятность			Компрометация данных
Средняя вероятность	Зависимость от ИИ	Риск ошибок и смещения ИИ	Манипулирование ИИ-системами
Низкая вероятность		Репутационный ущерб	Автоматизация атак; Использование ИИ в социальной инженерии
	Низкий ущерб	Средний ущерб	Высокий ущерб

Рис. 2. Карта рисков угроз, связанных с использованием искусственного интеллекта

На основании карты рисков можно выстроить иерархию рисков, а также создать план по нейтрализации этих рисков [16]. Наиболее значимыми для предприятия при использовании ИИ являются риски компрометации данных и манипулирования ИИ-системами: зависимость от ИИ отнесена к зоне средних рисков (средняя вероятность при низком ущербе), а риск ошибок и смещений ИИ-моделей – к зоне повышенного внимания из-за сочетания средней вероятности и среднего ущерба.

Также были определены «слепые зоны», то есть риски с низкой вероятностью возникновения, но высоким потенциальным ущербом, которые могут быть недооценены без системного анализа. К таким рискам отнесены автоматизация кибератак и использование искусственного интеллекта в социальной инженерии (зона средних рисков) и репутационный ущерб (зона низких рисков).

Таким образом, приоритизация защитных мер должна быть направлена прежде всего на обеспечение целостности и защищённости данных, повышение устойчивости ИИ-систем к манипулированию и снижение зависимости критичных бизнес-процессов от автономных интеллектуальных решений.

Заключение

В ходе исследования установлено, что традиционный подход к управлению рисками предприятия не способен ответить в полной мере на актуальные угрозы кибербезопасности. Применение инструментов проактивного подхода к управлению рисками, основанного на системном анализе и прогнозировании, обеспечивает более высокий уровень защищённости и устойчивости хозяйствующих субъектов.

Показано, что карта рисков является эффективным инструментом проактивного управления, позволяющим визуализировать угрозы, оценивать их вероятность и потенциальный ущерб, а также рационально распределять ресурсы на защиту наиболее критичных направлений. Использование данного инструмента способствует снижению финансовых и репутационных потерь, а также повышению качества управленческих решений в сфере кибербезопасности.

Научно-практическая значимость результатов данной работы заключается в том, что построенная карта рисков может быть использована предприятиями разной специализации в целях приоритизации мер защиты и условиях развития информационных технологий и повсеместного внедрения технологий искусственного интеллекта. Также результаты исследования наглядно демонстрируют важность выявления «слепых зон» в системе защиты, связанных с низкой вероятностью возникновения, но высоким потенциальным ущербом. Предложенная методика оценки рисков может быть адаптирована под конкретное предприятие с учетом отраслевой принадлежности и размеров организации. Так, данная методика может являться ориентиром при составлении расходов на обеспечение кибербезопаности с учетом реальных угроз и формировать план мероприятий по нейтрализации наиболее критических рисков.

Вместе с тем, перспективным направлением развития системы защиты предприятий является и интеграция искусственного интеллекта, обеспечивающая автоматическое обнаружение вторжений, формирование адаптивных систем реагирования. Одновременно с этим, возрастает значимость формирования риск-культуры в организации, включающей подготовку персонала, развитие цифровой грамотности и управление человеческим фактором, что позволяет минимизировать уязвимости, связанные с использованием интеллектуальных технологий.

Литература

1. *Буевич А.П.* Киберугрозы как современный вызов безопасности банковского сектора в России // Национальная безопасность. 2025. №. 4. С. 46-54.
2. *Друзенко А.В.* Проактивная парадигма управления рисками инвестиционно-строительного проекта // Фундаментальные исследования. 2016. № 5-3.
3. *Жирков Г.С., Готовцева О.Г.* Основные тренды кибербезопасности: обзор современных трендов и вызовов // Вестник науки. 2025. №. 8(89). С. 317-324.
4. Киберугрозы в России и Беларуси. Аналитика и прогнозы 2025/26 // F6 — ведущий поставщик решений в области кибербезопасности. URL: https://cdn.f6.ru/main/media/69807825816f6_cybercrime-trends-annual-report-2025-2026.pdf (дата обращения: 07.04.2026).
5. *Балашов А.А.* Развитие искусственного интеллекта: угрозы и возможности для экономической безопасности России // Международный научно-исследовательский журнал. 2023. №. 10(136). С. 1-6.
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Справ.-правовая система «КонсультантПлюс».
7. *Синявская Е.Е.* Искусственный интеллект в финансовой сфере // Вестник Академии знаний. 2025. №3 (68).
8. *Скатков А.В., Воронин Д.Ю., Шевченко В.И., Ключарев А.А.* Проактивный и реактивный риск-менеджмент IT-сервисов облачных сред // Информационно-управляющие системы. 2017. №3 (88).
9. *Бочанов М.А.* От реактивного к проактивному государственному управлению в эпоху цифровой трансформации // Ars Administrandi. 2024. №. 4(16). С. 555-569.
10. *Безденежных В.М., Родионов А.С.* Проактивный риск-ориентированный подход в сценарном планировании деятельности хозяйствующих субъектов // Экономика. Налоги. Право. 2017. № 6.
11. *Мартыненко О.В., Полещук С.М., Печеневская М.А.* Проактивное управление рисками бюджетным и автономным учреждениями при осуществлении деятельности, финансируемой за счет субсидий на выполнение государственного (муниципального) задания // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2026. № 1. С. 82-93.
12. Гайдаенко Э.В. Карта рисков как инструмент управления рисками сельскохозяйственного производства // Современные тенденции в экономике и управлении: новый взгляд. 2012. С. 1-9.
13. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введ. 2011-12-01. – Москва: Стандартинформ, 2011. 36 с.
14. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. Введ. 2020-03-01. – Москва: Стандартинформ, 2020. 14 с.
15. *Макарова О.Н., Мартыненко О.В., Полещук С.М., Шалыгина Е.В.* Использование технологий искусственного интеллекта в управлении организации // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2025. № 3. С. 66-75.
16. *Касливцева Е.Е., Сбродова Н.В.* Риски деятельности предприятия сферы производства строительных материалов (на примере ООО "Акерман цемент") // Экономика и социум. 2022. №. 11(112). С. 633-637.

References

1. Buevich A.P. Cyber threats as a modern challenge to the security of the banking sector in Russia // *National Security*. 2025. No. 4. pp. 46-54.
2. Druzenko A.V. Proactive risk management paradigm of an investment and construction project // *Fundamental Research.* 2016. No. 5-3.
3. Zhirkov G.S., Gotovtseva O.G. The main trends in cybersecurity: an overview of current trends and challenges // *Bulletin of Science*. 2025. No. 8(89). pp. 317-324.
4. Cyber threats in Russia and Belarus. Analytics and Forecasts 2025/26 // F6 is a leading provider of cybersecurity solutions. URL: https://cdn.f6.ru/main/media/69807825816f6_cybercrime-trends-annual-report-2025-2026.pdf (date of access: 04/07/2026).
5. Balashov A.A. Development of artificial intelligence: threats and opportunities for Russia's economic security // *International Scientific Research Journal.* 2023. No. 10(136). pp. 1-6.
6. Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" // Reference.- the legal system "ConsultantPlus".
7. Sinyavskaya E.E. Artificial intelligence in the financial sphere // *Bulletin of the Academy of Knowledge.* 2025. №3 (68).
8. Skatkov A.V., Voronin D.Yu., Shevchenko V.I., Klyucharev A.A. Proactive and reactive risk management of IT services in cloud environments // *Information Management Systems.* 2017. №3 (88).
9. Bochanov M.A. From reactive to proactive public administration in the era of digital transformation // *Ars Administrandi*. 2024. №. 4(16). Pp. 555-569.
10. Bezdenezhnykh V.M., Rodionov A.S. Proactive risk-oriented approach in scenario planning of business entities // *Economy. Taxes. Right*. 2017. No. 6.
11. Martynenko O.V., Poleshchuk S.M., Pechenevskaya M.A. Proactive risk management by budgetary and autonomous institutions in carrying out activities funded by subsidies for the performance of state (municipal) tasks // *Scientific Journal of the National Research University of ITMO. The series "Economics and Environmental Management*". 2026. No. 1. pp. 82-93.
12. Gaidaenko E.V. Risk map as a risk management tool for agricultural production // *Modern trends in economics and management: a new perspective*. 2012. pp. 1-9.
13. GOST R ISO/IEC 27005-2010. Information technology. Methods and means of ensuring security. Information security risk management. Introduction. 2011-12-01. Moscow: Standartinform, 2011. 36 p.
14. GOST R ISO 31000-2019. Risk management. Principles and guidelines. Introduction. 2020-03-01. Moscow: Standartinform, 2020. 14 p.
15. Makarova O.N., Martynenko O.V., Poleshchuk S.M., Shalygina E.V. The use of artificial intelligence technologies in the management of an organization // *Scientific Journal of the National Research University of ITMO. The series "Economics and Environmental Management"*. 2025. No. 3. pp. 66-75.
16. Kaslivtseva E.E., Sbrodova N.V. Risks of activity of the enterprise in the sphere of production of building materials (on the example of Akerman Cement LLC) // *Economics and society.* 2022. №. 11(112). Pp. 633-637.

Статья поступила в редакцию 12.03.2026 *Received 12.03.2026*
Принята к публикации 29.05.2026 *Accepted for publication 29.05.2026*