МЕНЕДЖМЕНТ

Управление рисками кибербезопасности в организациях малого и среднего бизнеса

Cybersecurity Risk Management in Small and Medium-Sized Businesses

DOI: 10.12737/2587-9111-2026-14-2-67-73 Получено: 11 февраля 2026 г. / Одобрено: 18 февраля 2026 г. / Опубликовано: 25 апреля 2026 г.

Цой В.В.

Преподаватель кафедры цифровой экономики, Университет «Синергия»,
Россия, 129090, г. Москва, ул. Мещанская, д. 9/14, стр. 1,
e-mail: cttrgais@gmail.com

Кикоть А.В.

Преподаватель цифровой экономики, Университет «Синергия»,
Россия, 129090, г. Москва, ул. Мещанская, д. 9/14, стр. 1,
e-mail: Kav270602@mail.ru

Кочеткова Е.А.

Старший преподаватель кафедры цифровой экономики,
Университет «Синергия»,
Россия, 129090, г. Москва, ул. Мещанская, д. 9/14, стр. 1.
e-mail: alyona191296@ya.ru

Водолаженко Р.А.

Канд. техн. наук, доцент кафедры прикладной математики,
Университет «Синергия»,
Россия, 129090, г. Москва, ул. Мещанская, д. 9/14, стр. 1,
e-mail: vra35977@gmail.com

Tsoi V.V.

Lecturer, Department of Digital Economics,
Synergy University,
9/14, bld. 1, Meshchanskaya St., Moscow, 129090, Russia,
e-mail: cttrgais@gmail.com

Kikot A.V.

Lecturer, Department of Digital Economics,
Synergy University,
9/14, bld. 1, Meshchanskaya St., Moscow, 129090, Russia,
e-mail: Kav270602@mail.ru

Kochetkova E.A.

Senior Lecturer, Department of Digital Economics,
Synergy University,
9/14, bld. 1, Meshchanskaya St., Moscow, 129090, Russia,
e-mail: alyona191296@ya.ru

Vodolazhenko R.A.

Candidate of Technical Sciences, Associate Professor, Department of Applied Mathematics, Synergy University,
9/14, bld. 1, Meshchanskaya St., Moscow, 129090, Russia,
e-mail: vra35977@gmail.com

Аннотация

В статье решается научная проблема анализа подходов к решению проблемы управления рисками кибербезопасности в организациях малого и среднего бизнеса (МСП). Наличие значительного проблемного поля исследования, несмотря на наличие значительного количества инцидентов нарушения кибербезопасности, актуализирует вопрос расширения исследовательских практик и поиска направлений дальнейшей работы по выработке решений по реагированию на наступление рисковых событий. Целью статьи является моделирование процесса управления рисками кибербезопасности в контакте достижения стратегических целей и обеспечения достижения ключевых показателей деятельности организаций малого и среднего бизнеса (МСП). Обозначенная цель декомпозирована на следующие задачи: исследование подходов к управлению рисками кибербезопасности, анализ эмпирических и практических данных о киберрисках, выявление актуальных мероприятий по управлению киберрисками для МСП, разработка рекомендаций по повышению эффективности управления рисками для МСП и направлений для проработки различных аспектов анализа их эффективности и инвестирования в системы управления такими рисками. Авторский вклад состоит в том, что с помощью эмпирического анализа управления киберрисками в МСП на материалах исследования, а также анализа тенденций, охарактеризованных учеными и исследователями в области киберрисков, были сформированы выводы о перечне актуальных направлений формирования систем управления киберрисками. Статья будет интересна всем, кто на практике занимается управлением киберрисками рисками в малых и средних организациях.

Ключевые слова: киберриски, МСП, малые предприятия, управление рисками, риски кибербезопасности.

Abstract

The article solves the scientific problem of analyzing approaches to solving the problem of cybersecurity risk management in small and medium-sized businesses (SMEs). The presence of a significant problem field of research, despite the presence of a significant number of cybersecurity incidents, raises the issue of expanding research practices and finding areas for further work on developing solutions to respond to the onset of risky events. The purpose of the article is to model the cybersecurity risk management process in order to achieve strategic goals and ensure the achievement of key performance indicators for small and medium-sized businesses (SMEs). The designated goal is decomposed into the following tasks: research of approaches to cybersecurity risk management, analysis of empirical and practical data on cyber risks, identification of relevant measures for managing cyber risks for SMEs, development of recommendations for improving the effectiveness of risk management for SMEs and directions for studying various aspects of analyzing their effectiveness and investing in such risk management systems. The author's contribution consists in the fact that with the help of an empirical analysis of cyber risk management in SMEs based on research materials, as well as an analysis of trends characterized by scientists and researchers in the field of cyber risks, conclusions were drawn about the list of relevant areas for the formation of cyber risk management systems. The article will be of interest to anyone who is engaged in cyber risk management in small and medium-sized organizations in practice.

Keywords: cyber risks, SMEs, small enterprises, risk management, cybersecurity risks.

Введение

Кибербезопасность представляет собой комплекс мер, технологий и практик, созданных и используемых для защиты компьютерных систем, сетей, программ и данных от цифровых вмешательств третьих лиц, в том числе несанкционированного доступа к информации [1]. В настоящее время кибербезопасность является важнейшим стратегическим вектором повышения устойчивости организаций и оказывает значительное влияние на показатели эффективности, прибыльности и устойчивости компаний.

Актуальность настоящей статьи определяется наличием в правовом и информационном поле резонансных киберинцидентов, оказавших влияние на

показатели деятельности компаний, в контакте которых эти инциденты происходили. Вместе с тем очевидно, что использование набора методов управления рисками в стратегическом ключе дает организациям возможность эффективно распределять ресурсы, расставлять приоритеты в части обеспечения безопасности и поддерживать общий уровень рисков организаций на приемлемом уровне.

Данные аналитических отчетов, исследований, проведенных учеными и практиками, а также анализ информации в открытых источниках, реализованный автором настоящей статьи, позволил заключить, что в крупных организациях использование систем управления рисками является общеупотребительной практикой [2; 3]. Вместе с тем малые и средние предприятия (далее — МСП) испытывают определенный дефицит в этом отношении, а их сотрудники не имеют достаточной грамотности в области обеспечения безопасности [4]. Анализ показал, что организации, имеющие стратегические документы по управлению рисками и программы управления рисками, имеют более устойчивые бизнес-модели, нежели те, кто рассматривает обеспечение кибербезопасности исключительно как затратную статью в бюджетах. Полученные результаты позволяют сделать вывод, что управление рисками должно представлять собой фундаментальную стратегическую возможность для организаций принимать решение об инвестировании в кибербезопасность на основе анализа влияния систем управления рисками на показатели бизнеса, интегрировав риск-ориентированные решения в бизнес-планирование, бизнес-моделирование и методическое обеспечение операционных процессов.

Актуальность настоящей статьи заключается в разработке методических подходов к реализации инвестиционных инициатив в отношении обеспечения кибербезопасности. Целью исследования является моделирование процесса управления рисками кибербезопасности в контакте достижения стратегических целей и обеспечения достижения показателей деятельности организаций малого и среднего бизнеса (МСП) [5].

В соответствии с заявленной целью исследования были поставлены и решены следующие задачи: анализ современных исследований в отношении процессов управления рисками кибербезопасности, моделирование эффективности управления рисками в контексте обеспечения безопасности организаций. Кроме того, были выявлены барьеры внедрения процессов управления рисками кибербезопасности для МСП, и предложены практические подходы к управлению такими рискамии.

Методика исследования

Традиционные подходы к обеспечению кибербезопасности на основе традиционных «низких» технологий в условиях высоких темпов развития облачных технологий, роста количества удаленных сотрудников, внедрения Интернета вещей (*IoT*) и большого количества инициатив цифровой трансформации оказываются все более несостоятельными. В то же время растет количество инцидентов, произошедших на базе новых, высоких, облачных технологий.

Краткий обзор научных публикаций по тематике управления рисками кибербезопасности позволил сделать вывод о том, что исследования подобных вопросов, во-первых, незначительно по количеству, во-вторых, охватывает не все аспекты управления, не учитывает отраслевую динамику. В целом в исследовательском поле наблюдается дефицит глубоких качественных и количественных работ в этом отношении.

Среди зарубежных авторов следует выделить Т. Олзака, рассматривавшего интеграцию управления рисками кибербезопасности в системы управления в целом [6], В. Серней, исследовавшего основы управления рисками кибербезопасности в целом, в том числе их страновую специфику [7], А. Осама, О. Эзекиель [8], Д. Вейвер, А. Редди, проводивших исследования в отношении кибербезопасности в *IT*-инфраструктуре на основе разработанной ими платформы [9].

Среди российских ученых можно выделить исследования А.И. Згобы, Д.В. Маркелова, П.И. Смирнова в части угроз, вызовов, решений кибербезопасности [10], К.К. Казарян в отношении управления рисками кибербезопасности в целом [4], В. Г. Халина и Г.В. Черновой в части влияния цифровизации на киберриски [11], А.А. Аванесова о проблеме страхования киберрисков [12], О.А. Ждановой, Е.А. Максимовой, которые рассматривали проблемы совершения сделок с цифровыми финансовыми активами как инструментами финансирования [13]. Управление киберрисками с учетом принципов функционирования системы цифровой безопасности рассмотрел А.Р. Маргамов [14], а вызовы и стратегии защиты в цифровую эпоху — Э.А. Абдуллаев [15]. Угрозы и методы защиты кибербезопасности в современном мире стали предметом рассмотрения Я.А. Гранкиной и С.Д. Баймедетова [16]. Однако представленные работы не учитывают множества аспектов. И, что важнее всего, ни одна работа не посвящена анализу киберрисков для предприятий малого и среднего бизнеса. Вместе с тем очевидна их специфика, связанная, прежде всего, с уровнем развития технологий (которые, например, в крупных

компаниях представляют собой структурированные *IT*-системы, дающие высокие степени контроля и защиты).

Однако количество таких работ позволяет сделать вывод о наличии исследовательского интереса к проблеме управления рисками. Требуется вместе с тем расширение предметного поля (акцент на малый и средний бизнес) и апробация уже имеющихся на сегодняшний день положений на материалах малых и средних организаций.

Статья, таким образом, базируется на теоретических концепциях и методологических положениях исследователей и практиков в сфере управления рисками кибербезопасности. Методологическую основу исследования составляют аналитический и системный подходы.

Результаты и выводы

Практика последних лет показала, что инциденты, связанные с наступлением риска кибербезопасности, приводят к катастрофическим последствиям для бизнеса, зачастую превышающим затраты на техническое устранение собственно риска: например, имеют следствием затраты на восстановление систем, а в качестве каскадного следствия — перебои в поставках, долгосрочный репутационный ущерб и пр. [17–19]. Подобная ситуация наблюдается в различных секторах: медицинские организации сталкиваются с перебоями в обслуживании пациентов вследствие рисков кибербезопасности, финансовые учреждения — с санкциями регулирующих органов, производители — с простоями производственных процессов. В этой связи решения по обеспечению кибербезопасности представляют собой инициативы уровня совета директоров и руководства.

Эмпирические доказательства важности управления рисками кибербезопасности для бизнеса были представлены в отчете о состоянии управления киберрисками за 2025 г. [20]. 847 организаций из разных секторов экономики стали целевой аудиторией для получения экспертных мнений. По мнению представителей организаций-респондентов, наличие программ страхования киберрисков повышает устойчивость бизнеса, что выражается в снижении частоты инцидентов, сокращении времени восстановления после наступления рискового события и снижении финансовых последствий в случае возникновения инцидентов [20].

Также очевидными стали дифференциации между организациями, имеющими и не имеющими методологии управления рисками, по показателям эффективности. В частности:

1) организации, использующие количественные методы оценки рисков, продемонстрировали на 37% более эффективное распределение бюджетных средств на кибербезопасность по сравнению с теми, кто использует качественные подходы;
2) организации, имеющие методологии управления рисками, продемонстрировали более высокую устойчивость к рисковым воздействиям: на 28% меньше оказалась частота серьезных инцидентов в сфере безопасности, на 41% меньше — среднее время обнаружения инцидентов, на 35% быстрее происходило восстановление нормальной работы после инцидентов, на 52% ниже оказывался финансовый ущерб от инцидентов. По оценкам, представленным в том же отчете, ежегодные затраты на кибератаки в организациях, имеющих методологии управления рисками, ниже порядка на 2,3 млн долл. по сравнению с организациями, не имеющих таких документов;
3) организации, имеющие бизнес-процессы оценки рисков, имеют возможность быстро оценить последствия новых бизнес-инициатив, приобретений или внедрения технологий с точки зрения рисков кибербезопасности. Например, организации, рассматривающие возможность перехода на облачные технологии, могут систематически оценивать риски, связанные с различными моделями облачных сервисов, и определять меры контроля.

В стандарте ГОСТ Р ИСО/МЭК 27005, идентичном международному документу ISO 27005, содержатся дополнительные рекомендации в части управления рисками информационной безопасности [21]. Стандарт определяет подходы к выявлению, оценке, устранению и мониторингу рисков. Его ключевые принципы включают порядок оценки рисков, требования к разработке решений по управлению рисками, мероприятия по нивелированию угроз и уязвимостей, ответственность за показатели управления рисками и др. Вместе с тем подчеркивается, что управление рисками представляет собой непрерывный процесс и требует постоянной оценки и верификации.

Далее в ряде исследований формулируется вывод о том, что, помимо организационных факторов (культура информационной безопасности, доступность инвестиционных ресурсов и пр.), на эффективность внедрения системы управления рисками оказывают влияние и такие факторы, как:

- ***ограниченность ресурсов***. Особенно это касается МСП, для которых инвестиции в обеспечение безопасности воспринимаются как непроизводительные затраты, снижающие прибыль. Эта проблема обостряется для организаций, имеющих

низкую рентабельность, и работающих в соответствующих отраслях. Найм персонала для служб кибербезопасности, закупка и внедрение инструментов мониторинга требует затрат, которые зачастую воспринимаются как менее важные, чем более актуальные задачи организаций;

- сложность интеграции информационных систем и сервисов. Зачастую сервисы, мобильные устройства, сторонняя интеграция и существующие системы реализованы в различных системах. Средства контроля безопасности, например, многофакторная аутентификация, усложняют процессы входа в систему, в то время как сегментация сети усложняет доступ к ресурсам. Необходимо соблюдение баланса между требованиями безопасности и операционной эффективностью, что требует привлечения заинтересованных сторон и обеспечения контроля информационных систем и сервисов.

Вместе с тем важность управления рисками заключается в том, что оно фактически является связующим звеном между «технической» кибербезопасностью и достижением ключевых показателей деятельности организаций. Так, управление рисками позволяет:

- во-первых, приоритизировать активы, предлагая методологию оценки активов для приоритетной защиты. Например, в организациях здравоохранения приоритетными активами являются электронные медицинские карты;
- во-вторых, обосновывать эффективность инвестиций, формулировать инвестиционные потребности в терминах, понятных лицам, принимающим решения, и членам совета директоров. Более того, методологии количественной оценки рисков (например, факторный анализ информационных рисков) позволяют структурировано подходить к оценке потенциальных потерь от киберинцидентов. Анализ целесообразности инвестирования в обеспечение кибербезопасности на основе ожидаемого снижения рисков проводится использованием этих оценок.

Что касается малых и средних предприятий, то для них имеют место следующие дополнительные проблемы:

- *недостаточная осведомленность руководства*.

Исследование, проведенное в отношении 312 руководителей малого и среднего бизнеса в 2025 г. [22], показало, что 67% из них значительно недооценивают киберриски своих организаций, и это связано с их низкой осведомленностью руководителей в области кибербезопасности. Данные опроса также показали, что 71% руководителей организаций малого и среднего бизнеса оценивают киберриск своей организации как «низкий» или «очень низкий», несмотря на то, что 58% организаций сталкивались с инцидентами безопасности за предыдущие 12 месяцев. При этом лишь 34% опрошенных руководителей малых и средних предприятий провели комплексную инвентаризацию активов в 2024 г. Однако в том случае, если руководители не идентифицируют как значимые потенциальные последствия кибератак для бизнеса, инвестиции в обеспечение безопасности воспринимаются как расходы, которые необходимо минимизировать, а не как стратегические возможности развития бизнеса;

- *недостаточный кадровый потенциал*.

МСП зачастую полагаются на ИТ-специалистов широкого профиля. Однако такой подход неэффективен для внедрения системы управления рисками. Небольшие команды часто не ориентируются на специалистов для решения широкого круга задач в области безопасности (сетевая безопасность, безопасность приложений, реагирование на инциденты и пр.).

Вместе с тем существуют новые тенденции, которые для малых и средних предприятий могут быть достаточно ресурсными. Так, например, внедрение технологий генеративного искусственного интеллекта в области кибербезопасности позволяет расширить возможности обнаружения угроз, анализировать системы безопасности, сопоставлять показатели из нескольких источников данных, создавать сводки аналитической информации об угрозах и пр. Вместе с тем искусственный интеллект создает дополнительные уязвимости, требующие оценки рисков, например, риск манипулирования обучающими или входными данными, утечки данных через системы искусственного интеллекта, масштабирования и усиления атак (например, посредством фишинговых электронных писем).

Базируясь на изложенных выше выводах с учетом результатов исследования [22] и данных, полученных в ходе анализа методической литературы, для МСП могут быть целесообразными следующие принципы управления рисками кибербезопасности:

- упрощенная оценка рисков, акцент на критически важных бизнес-активах и наиболее вероятных угрозах с целью экономии ресурсов на первых этапах и недопущения разброса сил;
- идентификация важнейших активов (систем документооборота, данных и процессов), которые могут быть использованы при проектировании системы управления рисками кибербезопасности;
- разработка сценариев реагирования на риски (5–10 наиболее актуальных угроз);

- оценка потенциального воздействия для каждого сценария угрозы на организацию в конкретных показателях эффективности (дни простоя, потеря доходов, штрафные санкции);
- определение порядка внедрения средств контроля киберрисков.

Разработка упрощенных моделей управления киберрисками позволяет оценить средние затраты за день простоя операционной системы; предполагаемую вероятность наступления крупного инцидента как следствия киберрисков на основе отраслевой статистики; ожидаемый годовой риск убытков кибербезопасности (вероятность × воздействие); стоимость внедрения базовых элементов управления киберрисками.

В качестве рекомендации для управления киберрисками МСП может быть представлено внедрение интегрированной архитектуры кибербезопасности (табл. 1).

Таблица 1

Рекомендации для управления киберрисками МСП (интегрированная архитектура кибербезопасности)

Компонент структуры управления киберрисками	Процессы	Мероприятия
Управленческая стратегия организации	Формулирование миссии, определение ключевых активов, документирование бизнес-процессов	Характеристика основных бизнес-процессов и ценностных предложений, требований, ключевых показателей
Процесс оценки рисков	Идентификация угроз, оценка уязвимостей, оценка вероятности рисков, анализ воздействия	документирование сценариев угроз, выявление технических и процедурных уязвимостей, оценка последствий успешных мероприятий
Обработка рисков и выбор средств контроля	Снижение рисков, их передача и предотвращение	Внедрение мер безопасности, снижающих вероятность или воздействие выявленных рисков, исключение высокорискованных видов деятельности или технологий и пр.
Внедрение и эксплуатация средств контроля	Разработка дорожной карты, управление изменениями, оперативный мониторинг	Разработка плана внедрения средств контроля с учетом зависимостей и доступности ресурсов
Постоянное совершенствование	Метрики, ключевые показатели эффективности, повышение уровня зрелости	Регулярные обзоры, учитывающие изменения в бизнесе, новые угрозы и развитие технологий

Источник: составлено автором на основе [22].

Для МСП, внедряющих системы управления рисками, актуальны следующие рекомендации.

1. Необходимость повышения квалификации руководителей в части управления рисками, проведение семинаров, брифингов для совета директоров, коучинга для руководителей.
2. Использование упрощенных количественных моделей, анализа затрат и выгод на обеспечение безопасности от киберрисков.
3. Первоначальные инвестиции необходимо сосредоточить на несложных технически элементах контроля: многофакторной аутентификации, автоматизированном управлении исправлениями, регулярном резервном копировании и пр.
4. Необходимо установить реалистичные сроки разработки и внедрения систем управления киберрисками, разработать соответствующие внутренние нормативные документы, дорожные карты.
5. Необходимо разработать показатели безопасности, которые будут связаны с результатами деятельности организации. Например, это могут быть влияние рисков на клиентов, соответствие нормативным требованиям, количество случаев наступления рисковых событий в отношении к количеству их нивелирования.
6. Целесообразно планировать сценарии управления рисками и осуществлять их тестирование в реальных условиях.
7. Необходимо создание механизмов использования практики работы с киберрисками (как внутренними, так и внешними) с целью повышения эффективности их контроля.
8. Следует внедрять процессы оценки поставщиков, основанные на оценке рисков, при этом внимание должно быть направлено на поставщиков, которые потенциально являются более склонными к инициированию рискового события.

Дальнейшего изучения требуют, как представляется, следующие вопросы. Во-первых, количественные аспекты воздействия управления киберрисками на показатели деятельности организаций (рентабельность инвестиций в управление киберрисками, соотношение эффекта от нивелирования рисков с ростом выручки, прибыли, оптимальное распределение ресурсов). Во-вторых, создание и апробация методологий управления киберрисками для малого и среднего бизнеса, предполагающих упрощенные инструменты оценки рисков, эффективные системы контроля, использование различных подходов к повышению грамотности руководителей в области кибербезопасности. В-третьих, оценка рисков внедрения новых технологий (искусственный интеллект, квантовые вычисления, интернет вещей и др.). В-четвертых, когнитивные и организацион-

ные факторы, влияющие на эффективность управления рисками (влияние когнитивных искажений на восприятие риска и инвестиционные решения, влияние организационной структуры и культуры на зрелость управления рисками и пр.). Наконец, анализ цепочек поставок и экосистем, и в этой связи методологии оценки киберрисков и управления ими в сложных цепочках поставок, оптимальное распределение ответственности, модели страхования киберрисков в цепочках поставок и пр.

Результаты анализа, представленного в статье, позволили сделать следующие выводы.

К внедрению кибербезопасности для МСП необходим структурированный подход, предполагающий несколько ключевых принципов: систематическую оценку рисков, их количественную оценку, компромисс между безопасностью, удобством использования, стоимостью и производительностью, постоянная адаптация управление рисками под изменения задач организации.

Авторский вклад состоит в том, что с помощью эмпирического анализа управления киберрисками в МСП на материалах исследования, а также анализа тенденций, охарактеризованных учеными и исследователями в области киберрисков, были сформированы выводы о перечне актуальных направлений формирования систем управления киберрисками.

В материалах статьи представлены наиболее значимые предпосылки необходимости разработки систем управления рисками кибербезопасности. Актуален вывод, что по мере ускорения цифровой трансформации стратегическая значимость управления рисками в области кибербезопасности будет только возрастать. В этой связи необходимо, чтобы организации, особенно МСП, рассматривали управление рисками кибербезопасности не с точки зрения соблюдения требований законодательства, а как стратегическую возможность, обеспечивающую достижение ключевых показателей организации.

Литература

1. *Белослудцев Н.В.* Что такое кибербезопасность и почему это важно? [Текст] / Н.В. Белослудцев, Л.В. Гаев // Инновационная наука. — 2025. — № 4-2. — URL: https://cyberleninka.ru/article/n/chto-takoe-kiberbezopasnost-i-pochemu-eto-vazhno
2. *Мартынюк М.С.* Организационно-управленческие механизмы обеспечения кибербезопасности российскаих компаний [Текст] / М.С. Мартынюк // Финансовые рынки и банки. — 2023. — № 6. — URL: https://cyberleninka.ru/article/n/organizatsionno-upravlencheskie-mehanizmy-obespecheniya-kiberbezopasnosti-rossiyskih-kompaniy
3. *Бойченко О.В.* Система управления рисками кибербезопасности кредитно-финансовой деятельности [Текст] / О.В. Бойченко // Научный вестник: финансы, банки, инвестиции. — 2024. — № 3. — URL: https://cyberleninka.ru/article/n/sistema-upravleniya-riskami-kiberbezopasnosti-kreditno-finansovoy-deyatelnosti
4. *Казарян К.К.* Управление рисками кибербезопасности [Текст] / К.К. Казарян // StudNet. — 2022. — № 1. — URL: https://cyberleninka.ru/article/n/upravlenie-riskami-kiberbezopasnosti
5. *Шувалова М.* Три кита цифровой трансформации субъектов МСП: перевод бизнеса в онлайн-формат, финансовая поддержка, обучение цифровым навыкам [Электронный ресурс]. — URL: https://www.garant.ru/article/1467601/?ysclid=miimpo272n578660081
6. Olzak T. (2025). Cybersecurity Risk Analysis and Management. 10.13140/RG.2.2.32254.91208
7. Ohrimenco Serghei & Valeriu Cernei. (2024). Cybersecurity risk. 145–154. 10.53486/escst2023.17
8. Ezekiel O. Risk Management as a Strategic Bridge: Aligning Cybersecurity Architecture with Business Objectives in Modern Organizations. IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, vol. XX, no. X, month 2025.
9. Aljumaiah Osama & Jiang, Weiwei & Addula, Santosh Reddy & Almaiah Mohammed. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing. 2025. 12–26. 10.63180/jcsra.thestap.2025.2.2.
10. *Згоба А.И.* Кибербезопасность: угрозы, вызовы, решения [Текст] / А.И. Згоба, Д.В. Маркелов, П.И. Смирнов // Вопросы кибербезопасности. — 2014. — № 5. — URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya
11. *Халин В.Г.* Цифровизация и киберриски [Текст] / В.Г. Халин, Г.В. Чернова // Управленческое консультирование. — 2023. — № 7. — URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-kiberriski
12. *Аванесов А.А.* Проблемы страхования киберрисков [Текст] / А.А. Аванесов // Экономическое развитие России. — 2025. — № 6. — URL: https://cyberleninka.ru/article/n/problemy-strahovaniya-kiberriskov
13. *Жданова О.А.* Киберриски совершения сделок с цифровыми финансовыми активами как инструментами финансирования [Текст] / О.А. Жданова, Е.А. Максимова // Инновации и инвестиции. — 2023. — № 10. — URL: https://cyberleninka.ru/article/n/kiberriski-sovershheniya-sdelok-s-tsifrovymi-finansovymi-aktivami-kak-instrumentami-finansirovaniya
14. *Маргамов А.Р.* Управление киберрисками с учетом принципов функционирования системы цифровой безопасности [Текст] / А.Р. Маргамов // Индустриальная экономика. — 2023. — № 5. — URL: https://cyberleninka.ru/article/n/upravlenie-kiberriskami-s-uchetom-printsipov-funktsionirovaniya-sistemy-tsifrovoy-bezopasnosti
15. *Абдуллаев Э.А.* Кибербезопасность: вызовы и стратегии защиты в цифровую эпоху [Текст] / Э.А. Абдуллаев // Молодой ученый. — 2023. — № 33. — С. 8–9. — URL: https://moluch.ru/archive/480/105493
16. *Гранкина Я.А.* Кибербезопасность в современном мире: угрозы и методы защиты [Текст] / Я.А. Гранкина, С.Д. Баймедетов // Вестник науки. — 2024. — № 11. — URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-sovremennom-mire-aktualnye-ugrozy-i-metody-zaschity
17. *Жирков Г.С.* Основные угрозы кибербезопасности: обзор современных трендов и вызовов [Текст] / Г.С. Жирков, О.Г. Готовцева // Вестник науки. — 2025. — № 8. — URL:

https://cyberleninka.ru/article/n/osnovnye-ugrozy-kiberbezopasnosti-obzor-sovremennyh-trendov-i-vyzovov
18. *Камбулов Д.А*. Угрозы кибербезопасности [Текст] / Д.А. Камбулов // StudNet. — 2021. — № 7. — URL: https://cyberleninka.ru/article/n/ugrozy-kiberbezopasnosti
19. *Менлиева А*. Угроза и анализ рисков: выбор эффективных мероприятий кибербезопасности для организаций [Текст] / А. Менлиева, Н. Баллыева, К. Гарягдыева // Вестник науки. 2024. № 10. — URL: https://cyberleninka.ru/article/n/ugroza-i-analiz-riskov-vybor-effektivnyh-meropriyatiy-kiberbezopasnosti-dlya-organizatsii
20. Глобальный отчет J.S. Held 2025: Эффективное управление киберрисками [Электронный ресурс]. — 2025. — 26 марта. — URL: https://www.appercase.ru/news/59006/?ysclid=minqptnefo81185279
21. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management. ГОСТ Р ИСО/МЭК 27005-2010. ОКС 35.040. — URL: https://normativ.kontur.ru/document?moduleId=9&documentId=225742&ysclid=minqxlqg9e946376626
22. В 2025 году бизнес подвергался кибератакам на 38% чаще [Электронный ресурс]. — URL: https://allo.tochka.com/news/kiberataki-2025?ysclid=mip87so44c684934570.

References

1. Belosludtsev N.V., Gaev L.V. What is cybersecurity and why is it important? // Innovative science. 2025. № 4-2. URL: https://cyberleninka.ru/article/n/chto-takoe-kiberbezopasnost-i-pochemu-eto-vazhno
2. Martynyuk M.S. Organizational and managerial mechanisms for ensuring cybersecurity of Russian companies // Financial markets and banks. 2023. № 6. URL: https://cyberleninka.ru/article/n/organizatsionno-upravlencheskie-mehanizmy-obespecheniya-kiberbezopasnosti-rossiyskih-kompaniy
3. Boychenko O.V. Cybersecurity risk management system for credit and financial activities // Scientific Bulletin: Finance, banks, investments. 2024. № 3. URL: https://cyberleninka.ru/article/n/sistema-upravleniya-riskami-kiberbezopasnosti-kreditno-finansovoy-deyatelnosti
4. Kazaryan K.K. Cybersecurity risk management // StudNet. 2022. No. 1. URL: https://cyberleninka.ru/article/n/upravlenie-riskami-kiberbezopasnosti
5. Shuvalova M. The three pillars of the digital transformation of SMEs are: the transfer of business to an online format, financial support, and digital skills training. URL: https://www.garant.ru/article/1467601/?ysclid=miimpo272n578660081
6. Olzak T. (2025). Cybersecurity Risk Analysis and Management. 10.13140/RG.2.2.32254.91208
7. Ohrimenco Serghei & Valeriu Cernei. (2024). Cybersecurity risk. 145–154. 10.53486/escst2023.17
8. Ezekiel O. Risk Management as a Strategic Bridge: Aligning Cybersecurity Architecture with Business Objectives in Modern Organizations. IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, VOL. XX, NO. X, MONTH 2025.
9. Aljumaiah, Osama & Jiang, Weiwei & Addula, Santosh Reddy & Almaiah, Mohammed. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing. 2025. 12–26. 10.63180/jcsra.thestap.2025.2.2
10. Zgoba A.I., Markelov D.V., Smirnov P.I. Cybersecurity: threats, challenges, solutions // Cybersecurity issues. 2014, no. 5. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya
11. Khalin V.G., Chernova G.V. Digitalization and cyber risks // Management consulting. 2023, no. 7. URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-i-kiberriski
12. Avanesov A.A. Problems of cyber risk insurance // Economic development of Russia. 2025, no. 6. URL: https://cyberleninka.ru/article/n/problemy-strahovaniya-kiberriskov
13. Zhdanova O.A., Maksimova E.A. Cyber risks of making transactions with digital financial assets as financing instruments // Innovation and investment. 2023, no. 10. URL: https://cyberleninka.ru/article/n/kiberriski-sovershеniya-sdelok-s-tsifrovymi-finansovymi-aktivami-kak-instrumentami-finansirovaniya
14. Margamov A.R. Cyber risk management based on the principles of functioning of the digital security system // Industrial Economy. 2023, no. 5. URL: https://cyberleninka.ru/article/n/upravlenie-kiberriskami-s-uchetom-printsipov-funktsionirovaniya-sistemy-tsifrovoy-bezopasnosti
15. Abdullaev E.A. Cybersecurity: Challenges and protection strategies in the digital age // Young scientist. 2023, no. 33, pp. 8–9. URL: https://moluch.ru/archive/480/105493
16. Grankina Ya.A., Baymedetov S.D. Cybersecurity in the modern world: threats and methods of protection // Bulletin of Science. 2024, no. 11. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-sovremennom-mire-aktualnye-ugrozy-i-metody-zaschity
17. Zhirkov G.S., Gotovtseva O.G. The main threats to cybersecurity: an overview of current trends and challenges // Bulletin of Science. 2025, no. 8. URL: https://cyberleninka.ru/article/n/osnovnye-ugrozy-kiberbezopasnosti-obzor-sovremennyh-trendov-i-vyzovov
18. Kambulov D.A. Threats to cybersecurity // StudNet. 2021, no. 7. URL: https://cyberleninka.ru/article/n/ugrozy-kiberbezopasnosti
19. Menlieva A., Ballyeva N., Garyagdieva K. Threat and risk analysis: choosing effective cybersecurity measures for organizations // Bulletin of Science. 2024, no. 10. URL: https://cyberleninka.ru/article/n/ugroza-i-analiz-riskov-vybor-effektivnyh-meropriyatiy-kiberbezopasnosti-dlya-organizatsii
20. Global Report J.S. Held 2025: Effective Cyber Risk Management. March 26, 2025. URL: https://www.appercase.ru/news/59006 /?ysclid=minqptnefo81185279
21. Information security risk management. Information technology. Security techniques. Information security risk management. GOST R ISO/IEC 27005-2010. OKS 35.040. URL: https://normativ.kontur.ru/document?moduleId=9&documentId=225742&ysclid=minqxlqg9e946376626
22. In 2025, businesses were exposed to cyber attacks 38% more often. URL: https://allo.tochka.com/news/kiberataki-2025?ysclid=mip87so44c684934570