DOI 10.37882/2223-2974.2026.02.23

ПРОБЛЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ СОВРЕМЕННЫХ ОРГАНИЗАЦИЙ

PROBLEMS OF INFORMATION SECURITY MANAGEMENT IN MODERN ORGANIZATIONS

Yu. Nozdrina

Summary. The article examines the main problems of information security management in modern organizations operating in the context of digital transformation and the increasing complexity of cyber threats. The relevance of the research is due to the fundamental transformation of the role of information security: from a highly technical function, it has become a strategic priority of corporate governance that requires attention at the board of director's level. Based on the systematization of scientific sources, three groups of interrelated problems have been identified: strategic, related to the gap between technical approaches and the needs of digital business; organizational, due to the human factor, including the phenomenon of «shadow security» and insufficient transparency of communications; technological, reflecting the complexity of implementing modern incident monitoring and management systems. An analysis of empirical studies demonstrates that 95 % of cyber-attacks are made possible by human error, and the average cost of data leakage reaches 4.45 million dollars [8]. Special attention is paid to the problems of security management in remote work, decentralized structures, and the increasing role of third-party vendors. The classification of risks into technical, personnel, process and third-party risks is proposed. The conclusion is substantiated that it is necessary to move from static protection models to adaptive, risk-oriented approaches that integrate technological, organizational, and human aspects. The scientific novelty of the research lies in a comprehensive analysis of information security management issues through the prism of three dimensions — strategic, organizational, and technological — considering current trends in digital transformation.

Keywords: information security, risk management, digital transformation, cyber threats, corporate governance.

Ноздрина Юлия Ивановна
кандидат экономических наук, Автономная некоммерческая организация высшего образования Московский международный университет
nojuiv@yandex.ru

Аннотация. В статье исследуются основные проблемы управления информационной безопасностью в современных организациях, функционирующих в условиях цифровой трансформации и возрастающей сложности киберугроз. Актуальность исследования обусловлена фундаментальной трансформацией роли информационной безопасности: из узкотехнической функции она превратилась в стратегический приоритет корпоративного управления, требующий внимания на уровне совета директоров. На основе систематизации научных источников выявлены три группы взаимосвязанных проблем: стратегические, связанные с разрывом между техническими подходами и потребностями цифрового бизнеса; организационные, обусловленные человеческим фактором, включая феномен «теневой безопасности» и недостаточную прозрачность коммуникаций; технологические, отражающие сложность внедрения современных систем мониторинга и управления инцидентами. Анализ эмпирических исследований демонстрирует, что 95 % кибератак становятся возможными из-за человеческих ошибок, а средняя стоимость утечки данных достигает 4,45 млн долларов [8]. Особое внимание уделяется проблемам управления безопасностью в условиях удаленной работы, децентрализованных структур и возрастающей роли сторонних поставщиков. Предложена классификация рисков на технические, кадровые, процессные и риски третьих сторон. Обоснован вывод о необходимости перехода от статических моделей защиты к адаптивным, риск-ориентированным подходам, интегрирующим технологические, организационные и человеческие аспекты. Научная новизна исследования заключается в комплексном анализе проблем управления информационной безопасностью через призму трех измерений — стратегического, организационного и технологического — с учетом современных тенденций цифровой трансформации.

Ключевые слова: информационная безопасность, управление рисками, цифровая трансформация, киберугрозы, корпоративное управление.

Введение

Ландшафт информационной безопасности претерпел фундаментальные изменения за последние десятилетия. Как отмечают исследователи, безопасность переместилась от узконаправленной технической проблемы к стратегическому вопросу бизнеса и приоритетному пункту повестки для высшего руководства организаций [10]. Эта трансформация обусловлена тотальным проникновением цифровых технологий во все аспекты деятельности современных компаний: облачные вычисления, искусственный интеллект, интернет вещей, большие данные, мобильные и социальные медиа технологии стали неотъемлемой частью бизнес-стратегий [3].

Однако цифровизация несет не только возможности, но и беспрецедентные риски. По данным IBM Cost of a Data Breach Report 2023, средняя стоимость утечки данных в мире достигла 4,45 миллиона долларов, увеличившись на 15 % за три года, при этом более 83 % организаций сталкивались с множественными утечками данных в те-

чение года [8]. Исследования показывают корреляцию между инцидентами безопасности и показателями деятельности компаний: объявление об утечке данных оказывает значительное негативное влияние на рыночную стоимость, варьирующееся от 1 до 2,1 процента [7, 10].

Актуальность темы исследования определяется тремя обстоятельствами. Во-первых, происходит стирание границ между физическим и цифровым миром: современные организации работают как цифровые цепочки поставок, где риски безопасности пересекают организационные границы и требуют межорганизационной координации [10]. Во-вторых, человеческий фактор остается наиболее уязвимым звеном: по оценкам специалистов, 95 % нарушений кибербезопасности вызваны человеческими ошибками, а развитие технологий искусственного интеллекта порождает новые, более изощренные угрозы социальной инженерии, включая дипфейки и фишинговые атаки [12]. В-третьих, регуляторная среда ужесточается: законы о защите данных, такие как Общий регламент по защите данных (GDPR), усиливают требования к организациям и повышают ответственность за утечки информации [10].

Цель настоящего исследования заключается в системном анализе проблем управления информационной безопасностью в современных организациях, выявлении их взаимосвязей и разработке направлений совершенствования подходов к управлению. Научная новизна исследования состоит в комплексном подходе к анализу проблем управления информационной безопасностью, интегрирующем стратегическое, организационное и технологическое измерения с учетом современных тенденций цифровой трансформации. В работе впервые систематизируются количественные оценки значимости различных проблем и факторов на основе актуальных эмпирических исследований, что позволяет перейти от качественного описания к обоснованным рекомендациям.

Материалы и методы исследования

Теоретико-методологическую основу исследования составляют фундаментальные положения теории управления информационной безопасностью, концепции управления рисками, а также современные разработки в области поведенческих аспектов безопасности и цифровой трансформации. Информационную базу работы образуют научные публикации российских и зарубежных авторов по проблемам управления информационной безопасностью. В процессе исследования применялись следующие методы: системный анализ, сравнительный анализ, метод классификации, контент-анализ научных источников для, метод теоретического обобщения и синтеза.

Результаты и обсуждения

Управление информационной безопасностью прошло значительную эволюцию за последние десятилетия. Как отмечается в литературе, первоначально безопасность рассматривалась как узкотехническая функция, сосредоточенная на защите периметра информационных систем и реализации технических контролей [1, 10]. Однако с развитием цифровых технологий и их тотальным проникновением в бизнес-процессы произошло смещение парадигмы: безопасность стала стратегическим вопросом бизнеса, требующим внимания на уровне совета директоров [2].

Исследователи выделяют три главных фактора, определяющих необходимость трансформации подходов к управлению информационной безопасностью [3, 10]. Во-первых, цифровой бизнес требует полного встраивания безопасности в бизнес-процессы. Организации стремительно внедряют цифровые бизнес-стратегии с высоким уровнем технологического развертывания, что приводит к устранению разрыва между традиционным физическим миром и новым цифровым миром. Примеры таких компаний, как Airbnb, Uber и Alibaba, демонстрируют, что современная бизнес-среда больше не оставляет места для дистанции между технологиями и бизнесом, а следовательно, и между безопасностью и бизнесом.

Во-вторых, вследствие тотального встраивания технологий в бизнес инциденты и нарушения безопасности теперь напрямую влияют на бизнес и могут серьезно затрагивать организацию. Успешные кибератаки могут приводить к потере клиентов, партнеров, финансовым и репутационным потерям, а также к судебным искам и государственным санкциям, ограничивая производительность фирмы, инновационный потенциал и конкурентные преимущества [4, 10].

В-третьих, цифровизация требует от организаций принятия межорганизационной перспективы в отношении безопасности. В цифровой среде организации функционируют как цифровые цепочки поставок, а не как отдельные бизнесы. Риски безопасности существуют через границы, и организации становятся зависимыми от экспертизы своих партнеров в создании безопасности, ожидая от них прозрачности в этом вопросе [4, 10].

Несмотря на признание этих факторов, исследователи констатируют, что существующие подходы к управлению информационной безопасностью остаются неадекватными новым реалиям. Основной акцент по-прежнему делается на контролях и общепринятых практиках, которые либо универсальны по охвату, либо статичны, что хорошо работает в относительно стабильной технической среде, но недостаточно в быстрой, гибкой и постоянно меняющейся цифровой среде [3].

Анализ научной литературы позволяет выделить ряд стратегических проблем, препятствующих эффективному управлению информационной безопасностью в современных организациях.

Во-первых, следует отметить разрыв между техническими подходами и потребностями бизнеса. Исследователи отмечают, что управление информационной безопасностью исторически развивалось как техническая дисциплина, что привело к доминированию технических специалистов в принятии решений и недостаточному вниманию к бизнес-аспектам [12]. Этот разрыв проявляется в том, что меры безопасности часто внедряются без должного понимания бизнес-процессов и потребностей пользователей, что приводит к сопротивлению со стороны сотрудников и поиску обходных путей.

Также следует отметить отсутствие целостного стратегического видения. Многие организации подходят к безопасности фрагментированно, внедряя отдельные решения для защиты от конкретных угроз без формирования комплексной стратегии. Исследование, проведенное на основе TOI-фреймворка (технологические, организационные, индивидуальные аспекты), показало, что организации часто упускают из виду важные факторы, такие как привычки сотрудников, организационная культура и ценности, которые не охватываются широко используемыми стандартами управления безопасностью, например серией ISO/IEC 27000 [12].

Немаловажную роль играет такая проблема как недостаточная вовлеченность высшего руководства. Несмотря на признание важности безопасности, исследователи фиксируют сохраняющиеся проблемы с привлечением внимания высшего руководства к вопросам безопасности [4, 10]. Без активной поддержки топ-менеджмента и совета директоров инициативы в области безопасности остаются недофинансированными и не получают необходимого организационного веса.

Человеческий фактор признается критическим элементом в управлении информационной безопасностью. По оценкам специалистов, 95 % нарушений кибербезопасности вызваны человеческими ошибками. При этом развитие технологий искусственного интеллекта создает новые угрозы: сотрудники могут непреднамеренно раскрывать конфиденциальные данные при использовании AI-инструментов, как в случае с тремя сотрудниками, допустившими утечку корпоративных данных в ChatGPT [12].

Одним из наиболее значимых феноменов, выявленных в современных исследованиях, является «теневая безопасность» — несанкционированные практики обеспечения безопасности, создаваемые и применяемые сотрудниками, особенно когда они воспринимают официальные практики как обременительные. Исследование с участием 433 офисных работников показало, что информационная перегрузка в области безопасности и психологическая расширенность прав и возможностей увеличивают намерения сотрудников прибегать к мерам теневой безопасности, тогда как воспринимаемая прозрачность организационной безопасности снижает это намерение [6].

Важно понимать двойственную природу теневой безопасности. С одной стороны, такие практики могут открывать уязвимости и создавать коллективное ложное чувство безопасности в компании. С другой стороны, существование теневых практик представляет возможность для обучения: организации могут анализировать причины, побуждающие сотрудников искать обходные пути, и совершенствовать свои официальные практики [6].

Также следует отметить проблемы коммуникаций. Исследование управления уязвимостью Log4Shell в крупной сложной организации выявило три основные проблемы в поддержании ситуационной осведомленности о киберугрозах: обмен информацией между сотрудниками не был легким; не была установлена общеорганизационная единая операционная картина; распространялась неточная информация [5]. Эти проблемы коммуникации критичны, поскольку в условиях быстро развивающейся угрозы сотрудники разных подразделений нуждаются в согласованном понимании ситуации для принятия эффективных мер.

Кроме того, исследования показывают, что национальная культура влияет на поведение сотрудников в области безопасности. В коллективистских культурах групповое неподчинение политикам безопасности встречается чаще, и сотрудники больше подвержены влиянию отношения руководителей к практикам безопасности [12]. В более индивидуалистических культурах влияние коллег и лидеров менее выражено. Этот культурный контекст должен учитываться при разработке программ обучения и повышения осведомленности.

Технологический аспект управления информационной безопасностью также сопряжен с существенными проблемами, особенно в контексте цифровой трансформации.

Системы управления информацией и событиями безопасности являются существенными для специалистов по безопасности в различных повседневных задачах: мониторинге, обнаружении аномалий, расследованиях, выявлении индикаторов компрометации, охоте за угрозами и обработке инцидентов. Исследование с использованием метода Дельфи и двумя раундами интервью с двенадцатью экспертами по безопасности в крупных организациях выявило тринадцать категорий проблем

SIEM-систем. Наиболее значимые проблемы связаны с использованием, за которыми следуют удобство использования и пользовательские компоненты [11]. Это указывает на то, что даже передовые технологические решения сталкиваются с проблемами человеко-центрированного характера.

Исследование реакции на уязвимость Log4Shell демонстрирует сложность управления уязвимостями в современных организациях. Количество публикуемых уязвимостей стремительно растет: в 2024 году было зарегистрировано 40 257 уязвимостей, что почти вдвое больше, чем в 2021 году [5]. Это требует от организаций разработки методологий приоритизации и поддержания высокого уровня операционной эффективности.

Кроме того, переход к удаленной работе, ускоренный пандемией COVID-19, создал новые вызовы для управления безопасностью. Исследователи выделяют пять основных проблем в управлении безопасностью удаленной работы: управление безопасностью конечных точек, размывание границ сетевой безопасности, распространение теневых IT-практик, сложности проверки соответствия требованиям и поддержание культуры безопасности [9].

Обзор литературы по управлению рисками кибербезопасности позволил выделить четыре основные категории рисков. Прежде всего это технические риски, которые связаны с уязвимостями программного и аппаратного обеспечения, недостатками архитектуры информационных систем, ошибками конфигурации. Эти риски традиционно находятся в фокусе внимания специалистов по безопасности и хорошо обеспечены методологиями оценки и смягчения.

Кадровые риски обусловлены действиями или бездействием сотрудников: ошибками, небрежностью, недостаточной осведомленностью, а также злонамеренными действиями инсайдеров. Несмотря на признание критической важности человеческого фактора, исследования показывают, что организации недостаточно системно подходят к управлению этими рисками [12].

Процессные риски связаны с недостатками процедур и регламентов: нечеткостью распределения ответственности, отсутствием регулярных аудитов, неэффективностью процессов реагирования на инциденты. Исследование реагирования на Log4Shell показало, что процессные проблемы, такие как отсутствие единой операционной картины, существенно затрудняют эффективное управление инцидентами [5].

Риски третьих сторон возникают в связи с использованием услуг внешних поставщиков, включая облачных провайдеров, аутсорсинговые компании, партнеров по цепочке поставок. В цифровой среде организации становятся зависимыми от безопасности своих партнеров, что требует развития механизмов межорганизационного управления рисками [10].

Проведенный анализ позволяет сформулировать ряд направлений совершенствования управления информационной безопасностью в современных организациях.

Первоначально рекомендуется переход к адаптивным моделям управления. Исследователи предлагают концепцию цифрового управления безопасностью как новую исследовательскую территорию, которая адресует ограничения и пробелы традиционных подходов к управлению информационной безопасностью в цифровом контексте [10]. В отличие от статических моделей, основанных на контролях, адаптивные модели предполагают непрерывную оценку рисков, гибкое реагирование на изменения и интеграцию безопасности во все бизнес-процессы.

Также предлагается развитие человеко-центрированного подхода. TOI-фреймворк предлагает рассматривать управление безопасностью через три измерения: технологическое, организационное и индивидуальное. Это позволяет организациям системно подходить к формированию поведения сотрудников в области безопасности, учитывая не только технические контроли, но и факторы мотивации, восприятия, организационной культуры. Рекомендуется использовать фреймворк как дорожную карту для проектирования и внедрения практик управления безопасностью, мотивирующих сотрудников к формированию безопасного поведения, как на рабочем месте, так и при удаленной работе [12].

Повышение прозрачности и качества коммуникаций. Исследование теневой безопасности показывает, что воспринимаемая прозрачность организационной безопасности снижает намерения сотрудников прибегать к небезопасным обходным путям [6]. Это подчеркивает важность эффективной коммуникации о целях, требованиях и обосновании мер безопасности. Организациям рекомендуется развивать механизмы обратной связи, позволяющие сотрудникам сообщать о сложностях в соблюдении политик безопасности и предлагать улучшения.

Удаленная работа требует адаптации подходов к управлению безопасностью. Рекомендуется применять многоуровневые подходы к управлению, балансирующие технические контроли с человеко-центрированными мерами безопасности, и использовать риск-ориентированные фреймворки, адаптирующиеся к распределенному характеру удаленной работы.

Также в условиях, когда организации функционируют как часть цифровых цепочек поставок, управление

безопасностью должно выходить за организационные границы. Это требует развития механизмов обмена информацией об угрозах, согласования стандартов безопасности с партнерами, проведения совместных аудитов и учений.

Выводы

Проведенное исследование позволяет сформулировать следующие основные выводы. Управление информационной безопасностью в современных организациях сталкивается с комплексом взаимосвязанных проблем, которые не могут быть решены в рамках традиционных подходов, ориентированных преимущественно на технические контроли и статические модели защиты. Фундаментальная трансформация роли безопасности — от узкотехнической функции к стратегическому приоритету корпоративного управления — требует переосмысления сложившихся практик и разработки новых концептуальных подходов. Стратегические проблемы включают разрыв между техническими подходами и потребностями бизнеса, отсутствие целостного стратегического видения и недостаточную вовлеченность высшего руководства. Организационные проблемы концентрируются вокруг человеческого фактора, включая феномен теневой безопасности, проблемы коммуникации и прозрачности, а также культурные аспекты, влияющие на восприятие и соблюдение политик безопасности сотрудниками. Технологические проблемы отражают сложность внедрения современных систем мониторинга и управления инцидентами, а также вызовы, связанные с удаленной работой и управлением уязвимостями в условиях экспоненциального роста их количества. Классификация рисков на технические, человеческие, процессные и риски третьих сторон позволяет организациям более системно подходить к идентификации и управлению угрозами. При этом критически важно признание взаимосвязи этих категорий: технологические решения неэффективны без учета человеческого фактора, а процессные меры бесполезны без вовлеченности сотрудников и поддержки руководства. Перспективными направлениями совершенствования управления информационной безопасностью являются: переход от статических моделей к адаптивным, риск-ориентированным подходам; развитие человекоцентрированных практик, учитывающих мотивацию, восприятие и потребности сотрудников; повышение прозрачности и качества коммуникаций о безопасности; адаптация подходов к условиям удаленной работы; развитие механизмов межорганизационной координации в цифровых цепочках поставок.

ЛИТЕРАТУРА

1. Бучаев М.А. Задачи обеспечения информационной безопасности промышленного предприятия / М.А. Бучаев, Г.И. Голиков, О.Д. Старченкова // Вестник Академии знаний. — 2025. — № 1(66). — С. 91–94.
2. Бучаев М.А. Подходы к определению информационной безопасности промышленного предприятия закрытого типа / М.А. Бучаев, Г.И. Голиков, Е.А. Конников // Вестник Академии знаний. — 2025. — № 4(69). — С. 101–107.
3. Райлян Д.А. Влияние цифровизации транспортной инфраструктуры на информационную безопасность малых и средних предприятий / Д.А. Райлян // Экономика и социум. — 2025. — № 10–2(137). — С. 879–885.
4. Сеник А.Я. Информационная безопасность на промышленных предприятиях и в бюджетных организациях / А.Я. Сеник, Н.Н. Кочерженко // Управление качеством. — 2025. — № 1(251). — С. 42–46. — DOI 10.33920/pro-01-2501-06.
5. Andreasson A., Artman H., Brynielsson J. et al. Cyber situation awareness during an emerging cyberthreat: a case study // International Journal of Information Security. — 2025. — № 24, № 217. https://doi.org/10.1007/s10207-025-01106-z/.
6. Dang-Pham D., Thompson N., Ahmad A., Maynard S. Shadow information security practices in organizations: The role of information security transparency, overload, and psychological empowerment // Computers & Security. — 2025. — Vol. 156. — pp. 104538. https://doi.org/10.1016/j.cose.2025.104538.
7. Franke U., Brynielsson J. Cyber situation awareness — A systematic review of the literature // Information Security Technical Report. — 2014. — Vol. 19. — pp. 18–31.
8. Haque G.M.M., Akula D.K., Mohammed Y.S., Syed A., Arafat Y. Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review // The American Journal of Engineering and Technology. — 2025. — Vol. 7, № 8. — pp. 126–150. — DOI: 10.37547/tajet/Volume07Issue08-14.
9. Mahimalur R.K. Implementing security governance for remote work: challenges and best practices // Information and Computer Security. — 2025. — Vol. 33. — № 5. — pp. 860–870. doi: https://doi.org/10.1108/ICS-03-2025-0101.
10. Schinagl S., Shahim A. What do we know about information security governance? // Information and Computer Security. — 2020. — Vol. 28, № 2. — pp. 261–292. doi: https://doi.org/10.1108/ICS-02-2019-0033.
11. Shirazi P., Padyab A. Discerning Challenges of Security Information and Event Management (SIEM) Systems in Large Organizations // 18th International Symposium on Human Aspects of Information Security and Assurance (HAISA). — Skövde, Sweden, 2024. — pp. 339–354. — DOI: 10.1007/978-3-031-72559-3_23.
12. Topa I-A., Karyda M. Addressing organisational, individual, and technological aspects and challenges in information security management: applying a framework in workplace and teleworking // Organizational Cybersecurity Journal: Practice, Process and People. — 2025. — Vol. 5, № 1. — pp. 26–59. — DOI: 10.1108/OCJ-03-2023-0006.

Журнал «Современная наука: актуальные проблемы теории и практики»