УДК 004.056

Павлов Анатолий Григорьевич, студент, Факультет Безопасности и таможни, Северо-Западный институт управления – филиал РАНХиГС, г. Санкт-Петербург

Олейник Наталья Михайловна, научный руководитель, доцент, кандидат экономических наук, доцент кафедры безопасности, Северо-Западный институт управления – филиал РАНХиГС, г. Санкт-Петербург

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПОВЫШЕНИЯ КИБЕРУСТОЙЧИВОСТИ: РОЛЬ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Аннотация

В статье рассматривается роль человеческого фактора в системе обеспечения киберустойчивости современных организаций. На основе анализа статистических данных ведущих международных и российских исследований в области кибербезопасности за период 2022–2024 годов установлено, что более 74% утечек данных обусловлены действиями персонала. Предложена классификация типичных ошибок пользователей информационных систем по трём категориям: технические, организационные и коммуникационные. Исследованы принципы концепции киберустойчивости как современной парадигмы управления информационными рисками. Выявлена статистически значимая отрицательная корреляция между уровнем культуры безопасности и частотой инцидентов информационной безопасности. По результатам исследования разработан комплекс организационных мер противодействия киберугрозам, включающий адаптивную систему обучения, симуляцию социотехнических атак, формализацию процедур реагирования на инциденты, интеграцию показателей киберкультуры в систему KPI руководителей и внедрение принципа «Security by Design». Для каждой меры определены

конкретные метрики эффективности. Результаты исследования представляют практический интерес для специалистов в области информационной безопасности и руководителей организаций.

Annotation

The article examines the role of the human factor in the cyber resilience system of modern organizations. Based on the analysis of statistical data from leading international and Russian cybersecurity studies for the period 2022–2024, it has been established that more than 74% of data breaches are caused by personnel actions. A classification of typical user errors in information systems into three categories — technical, organizational, and communication — is proposed. The principles of cyber resilience as a modern paradigm for information risk management are explored. A statistically significant negative correlation between an organization's security culture level and the frequency of information security incidents was identified. Based on the research findings, a set of five organizational measures to counter cyber threats was developed, including an adaptive training system, simulation of social engineering attacks, formalization of incident response procedures, integration of cybersecurity culture metrics into the KPI system for managers, and adoption of the "Security by Design" principle. Specific performance metrics (KPIs) are defined for each measure. The research results are of practical interest to information security professionals and organizational managers.

Ключевые слова: киберустойчивость, информационная безопасность, человеческий фактор, организационные меры, социальная инженерия, обучение персонала, культура безопасности

Keywords: cyber resilience, information security, human factor, organizational measures, social engineering, personnel training, security culture

В условиях цифровой трансформации экономики и общества проблема обеспечения киберустойчивости организаций приобретает критическое значение. Согласно данным международных исследований, более 85% [10] успешных кибератак связаны с эксплуатацией уязвимостей, обусловленных действиями или бездействием персонала организаций. Данное обстоятельство актуализирует необходимость комплексного изучения роли человеческого фактора в системе информационной безопасности. Под комплексным изучением в рамках данного исследования понимается системный анализ психологических, поведенческих и социальных аспектов взаимодействия сотрудников с информационными системами, а также оценка влияния корпоративной культуры на уровень киберустойчивости. Также необходима разработка эффективных организационных мер противодействия киберугрозам.

Несмотря на постоянное совершенствование технических средств защиты информации, злоумышленники всё чаще используют методы социальной инженерии для получения несанкционированного доступа к корпоративным данным. Фишинговые атаки, претекстинг, психологическое манипулирование сотрудниками становятся основными векторами реализации киберугроз. При этом традиционные технические решения оказываются недостаточно эффективными против угроз, эксплуатирующих психологические особенности и поведенческие паттерны пользователей.

Актуальность темы исследования обусловлена несколькими факторами. Во-первых, существует объективное противоречие между растущей сложностью информационных систем и ограниченными возможностями пользователей в понимании всех аспектов информационной безопасности. Во-вторых, динамичное развитие киберугроз требует постоянной адаптации организационных мер защиты под изменяющиеся тактики злоумышленников и новые векторы атак. В-третьих, отсутствие единой методологии формирования культуры информационной безопасности снижает

эффективность внедряемых решений и препятствует созданию комплексной системы управления киберрисками.

Проблема исследования заключается в необходимости выявления наиболее эффективных организационных мер, направленных на минимизацию рисков, связанных с человеческим фактором, и формирование устойчивой системы киберзащиты организации. Для решения данной проблемы в рамках настоящей работы проводится анализ роли человеческого фактора в обеспечении киберустойчивости и разрабатываются соответствующие практические рекомендации. При этом система информационной безопасности рассматривается как комплексный объект, объединяющий технические средства, нормативную базу и образовательные процессы, а предметом детального изучения выступают конкретные организационные меры защиты информации от социотехнических угроз.

Киберустойчивость представляет собой способность организации предвидеть, противостоять, адаптироваться и восстанавливаться после киберугроз и инцидентов информационной безопасности с минимальным ущербом [7] для бизнес-процессов. В отличие от традиционной концепции информационной безопасности, ориентированной преимущественно на предотвращение инцидентов, киберустойчивость подразумевает признание невозможности абсолютной защиты и акцентирует внимание на способности организации функционировать в условиях реализации угроз.

Концепция киберустойчивости базируется на нескольких фундаментальных принципах. Принцип превентивности [7] предполагает проактивное выявление потенциальных уязвимостей и угроз до их реализации. Принцип адаптивности означает способность системы безопасности динамически изменяться в ответ на эволюцию ландшафта киберугроз. Принцип непрерывности обеспечивает постоянный мониторинг и оценку состояния защищённости информационных активов. Принцип комплексности требует интеграции технических, организационных и правовых мер защиты информации.

Человеческий фактор в контексте информационной безопасности представляет собой совокупность психологических, поведенческих и социальных характеристик пользователей информационных систем, способных оказывать влияние на уровень защищённости информационных активов организации [4]. Исследования демонстрируют, что данный фактор является одновременно наиболее уязвимым звеном системы безопасности и потенциально мощным ресурсом её укрепления.

Влияние человеческого фактора на информационную безопасность может быть классифицировано по нескольким основаниям. По степени осознанности [4] выделяют непреднамеренные действия, обусловленные недостатком знаний или невнимательностью, и преднамеренные действия, направленные на нарушение требований безопасности. По характеру воздействия различают активные действия пользователей и пассивное бездействие при наличии признаков инцидентов безопасности. По масштабу последствий дифференцируют локальные нарушения, затрагивающие отдельные информационные ресурсы, и системные инциденты, способные парализовать деятельность организации.

Ошибки пользователей информационных систем представляют собой один из наиболее распространённых источников инцидентов информационной безопасности. Системный анализ позволяет выделить несколько категорий типичных пользовательских ошибок, различающихся по механизму возникновения и потенциальным последствиям [1].

Технические ошибки связаны с неправильным использованием функционала информационных систем и средств защиты информации. К данной категории относятся неверная конфигурация параметров безопасности, некорректное применение криптографических средств, ошибки при управлении правами доступа. Последствия таких ошибок могут варьироваться от временного нарушения доступности сервисов до создания критических уязвимостей, эксплуатация которых позволяет получить несанкционированный доступ к конфиденциальной информации [1].

Организационные ошибки обусловлены несоблюдением установленных политик и процедур безопасности. Наиболее распространёнными проявлениями являются использование слабых паролей или их передача третьим лицам, игнорирование процедур верификации корреспондентов при обмене конфиденциальной информацией, нарушение правил работы с мобильными устройствами и съёмными носителями [5]. Такие ошибки часто становятся возможными из-за недостаточной осведомлённости персонала о существующих угрозах или восприятия требований безопасности как излишне обременительных.

Коммуникационные ошибки возникают при взаимодействии с внешними контрагентами и обработке входящей информации. Переход по подозрительным ссылкам в электронных сообщениях, открытие вложений неизвестного происхождения, предоставление служебной информации без должной авторизации запрашивающей стороны -- типичные примеры данной категории ошибок [4]. Эксплуатация коммуникационных ошибок является основой большинства современных фишинговых атак и методов социальной инженерии. Психологические механизмы данного явления детально рассмотрены в работах исследователей, изучающих когнитивные уязвимости персонала и методы их нейтрализации в корпоративной среде [8].

Последствия пользовательских ошибок могут быть чрезвычайно серьёзными. Финансовые потери включают прямой ущерб от утечки информации, расходы на расследование инцидентов и восстановление систем, штрафы регуляторов за нарушение требований защиты персональных данных. Репутационные риски связаны с потерей доверия клиентов и партнёров, негативным освещением инцидентов в средствах массовой информации. Операционные последствия выражаются в нарушении бизнес-процессов, снижении производительности, необходимости дополнительных затрат на усиление системы безопасности.

Особая роль в этом процессе принадлежит руководству компании. Когда топ-менеджеры демонстрируют свою приверженность принципам

безопасности, это создаёт условия для того, чтобы соответствующие ценности распространялись на все уровни организации.

Механизмы защиты информационных активов должны проектироваться с учётом реальных рабочих процессов, обеспечивая необходимый уровень безопасности без создания излишних препятствий для выполнения функциональных обязанностей. Вовлечение конечных пользователей в процесс разработки политик повышает их приемлемость и эффективность применения.

Однако, даже самые совершенные политики будут бесполезны без должной подготовки сотрудников. Именно поэтому ключевым элементом организационных мер является регулярная образовательная деятельность. Система обучения персонала в области информационной безопасности должна быть построена на принципах непрерывности, релевантности и практической ориентированности [6]. Однократное вводное обучение не обеспечивает формирования устойчивых компетенций и не учитывает динамичную эволюцию ландшафта киберугроз. Эффективная программа обучения предполагает сочетание различных форматов и методов передачи знаний.

Базовое обучение для всех категорий персонала должно охватывать фундаментальные принципы информационной безопасности, типичные угрозы и методы их реализации, основные требования корпоративных политик безопасности. Содержание обучения необходимо адаптировать к специфике деятельности различных групп сотрудников, акцентируя внимание на рисках и мерах защиты, наиболее релевантных для их рабочих функций.

Информационные кампании по повышению осведомлённости дополняют формальное обучение регулярными напоминаниями о текущих угрозах и правилах безопасного поведения. Использование разнообразных каналов коммуникации – корпоративной почты, внутренних порталов, информационных стендов – обеспечивает охват всего персонала. Актуализация содержания информационных материалов в соответствии с

текущей обстановкой в сфере киберугроз поддерживает актуальность и релевантность информации.

Оценка эффективности обучения должна основываться не только на формальных показателях прохождения курсов, но и на измерении изменений в реальном поведении сотрудников. Мониторинг соблюдения политик безопасности, анализ результатов учебных фишинговых атак, обратная связь от службы информационной безопасности позволяют оценить практическое воздействие образовательных программ и внести необходимые коррективы.

Система политик и процедур информационной безопасности образует нормативную основу управления киберрисками в организации. Эффективность данной системы определяется не только полнотой охвата потенциальных угроз, но и практической применимостью документов, их понятностью для персонала и соответствием реальным бизнес-процессам.

Политика информационной безопасности верхнего уровня определяет стратегические цели и принципы обеспечения защиты информации, распределение ответственности между подразделениями, общие требования к персоналу. Документ должен быть утверждён высшим руководством организации и регулярно пересматриваться для обеспечения соответствия изменяющимся условиям деятельности и угрозам. Нормативным ориентиром при формировании политик безопасности выступают требования регуляторов, в частности ФСТЭК России [3], устанавливающих базовый состав мер защиты информации.

Специализированные политики конкретизируют требования безопасности для отдельных областей: управления доступом, работы с мобильными устройствами, использования электронной почты и интернета, обработки конфиденциальной информации. В каждой политике должны быть прописаны чёткие правила поведения, объяснение, почему эти требования необходимы, и описание того, к чему может привести их нарушение. При этом важно, чтобы все сотрудники имели доступ к этим документам и регулярно с ними знакомились.

Что касается процедур, они подробно описывают последовательность действий в различных ситуациях. Например, процедуры реагирования на инциденты объясняют, что делать при обнаружении признаков нарушения безопасности: кто за что отвечает, как распределяются роли, по каким каналам идёт коммуникация. Есть также процедуры управления изменениями -- они регулируют, как вносить модификации в информационные системы, не нарушая требований безопасности. А процедуры управления уязвимостями помогают находить, оценивать и устранять слабые места в защите.

Отдельно стоит сказать о том, насколько важно встраивать требования безопасности в сам процесс разработки и эксплуатации информационных систем. Когда критерии безопасности учитываются уже на этапах проектирования, тестирования и внедрения, это даёт гораздо лучший результат, чем попытки «залатать дыры» в уже работающей системе.

Для подтверждения теоретических положений о роли человеческого фактора в обеспечении киберустойчивости организаций было проведено комплексное исследование, включающее анализ вторичных статистических данных международных и российских источников, а также изучение отчётов о киберинцидентах за период 2022-2024 годов. Методологическую основу исследования составили методы статистического анализа, сравнительного анализа, систематизации и обобщения эмпирических данных.

Информационная база исследования включала отчёты специализированных организаций в области кибербезопасности (Verizon Data Breach Investigations Report, IBM Security Cost of Data Breach Report, Positive Technologies), данные аналитических центров международных консалтинговых компаний, материалы исследований Национального координационного центра по компьютерным инцидентам [2], публикации научных и отраслевых изданий по проблематике информационной безопасности.

Систематизация статистических данных позволяет количественно оценить масштаб влияния человеческого фактора на состояние

информационной безопасности организаций. Согласно глобальному исследованию компании Verizon, проведённому на основе анализа более восьмидесяти двух тысяч инцидентов безопасности в 2024 году, доля утечек данных, обусловленных действиями сотрудников организаций, составила семьдесят четыре процента от общего числа подтверждённых нарушений [15]. При этом шестьдесят восемь процентов инцидентов были связаны с непреднамеренными действиями персонала, тогда как тридцать два процента представляли собой результат умышленных злоупотреблений [7].

Анализ отчёта компании IBM Security о стоимости утечек данных за 2024 год выявил существенную дифференциацию экономического ущерба в зависимости от причин инцидента. Средняя стоимость утечки данных, обусловленной ошибками персонала, составила четыре целых двадцать восемь сотых миллиона долларов США, тогда как утечки вследствие технических уязвимостей оценивались в три целых шестьдесят две сотых миллиона долларов. Наиболее затратными оказались инциденты, связанные с целенаправленной эксплуатацией человеческого фактора методами социальной инженерии, средняя стоимость которых достигла пяти целых тринадцати сотых миллиона долларов [10].

Количественная оценка результативности организационных мер защиты базируется на анализе корреляции между внедрением определённых практик и частотой инцидентов безопасности. Исследование компании Proofpoint, охватившее более семи тысяч организаций в 2024 году, продемонстрировало, что внедрение комплексных программ обучения персонала в области информационной безопасности коррелирует со снижением успешности фишинговых атак на шестьдесят три процента по сравнению с организациями, не реализующими систематическое обучение [13].

Внедрение системы контроля соблюдения политик безопасности с применением автоматизированных механизмов мониторинга показало существенное влияние на снижение числа организационных ошибок персонала. По данным исследования Gartner, организации, использующие

технологии предотвращения потери данных в сочетании с обучением пользователей, зафиксировали сокращение инцидентов утечки конфиденциальной информации на сорок девять процентов в течение двенадцати месяцев после внедрения [9].

Результаты анализа продемонстрировали статистически значимую отрицательную корреляцию между интегральным показателем культуры безопасности и частотой инцидентов информационной безопасности. Организации с высоким уровнем культуры безопасности (верхний квартиль распределения) фиксировали в среднем четыре целых две десятых инцидента на тысячу сотрудников в год, тогда как организации с низким уровнем культуры (нижний квартиль) регистрировали восемнадцать целых семь десятых инцидента на тысячу сотрудников. Коэффициент корреляции Пирсона составил минус ноль целых семьдесят три сотых, что свидетельствует о сильной обратной связи между изучаемыми показателями [12].

Детальный анализ компонентов культуры безопасности выявил, что наибольшее влияние на снижение числа инцидентов оказывает фактор вовлечённости высшего руководства в процессы обеспечения информационной безопасности. Организации, в которых топ-менеджмент демонстрирует активную поддержку инициатив в области кибербезопасности и личным примером следует установленным политикам, показывали на сорок два процента меньше инцидентов по сравнению с организациями, где руководство дистанцируется от вопросов информационной безопасности [6].

Временной анализ динамики инцидентов демонстрирует устойчивую тенденцию роста числа атак, ориентированных на эксплуатацию человеческого фактора. По данным Microsoft Digital Defense Report 2024, за последние два года количество фишинговых атак на корпоративных пользователей возросло более чем на сто процентов, при этом атаки с использованием методов социальной инженерии занимают лидирующее место среди векторов компрометации корпоративных сетей [11].

Комплексный анализ статистических данных и эмпирических исследований позволяет сформулировать несколько принципиальных выводов относительно роли человеческого фактора в обеспечении киберустойчивости организаций. При этом динамика последних лет демонстрирует устойчивую тенденцию роста доли атак, ориентированных на человеческий фактор, что обусловлено повышением технической защищённости информационных систем и смещением фокуса злоумышленников на более уязвимое звено – пользователей [4].

Эмпирические данные подтверждают, что внедрение программ обучения персонала, формирование культуры информационной безопасности, регулярное проведение симуляций атак способны обеспечить значительное снижение числа инцидентов безопасности. Однако эффективность данных мер напрямую зависит от непрерывности их реализации и адаптации к эволюции ландшафта киберугроз [14].

Результаты исследований показывают, что универсальные программы обучения демонстрируют ограниченную эффективность по сравнению с целевыми программами, учитывающими специфику рабочих функций и уровень технической компетентности сотрудников.

Анализ показал: концепция киберустойчивости идёт дальше традиционного понимания информационной безопасности. Она фокусируется не только на предотвращении угроз, но и на том, как организация может продолжать работать даже при реализации этих угроз, как минимизировать последствия инцидентов.

Человеческий фактор занимает центральное место в системе киберустойчивости, выступая одновременно как источник рисков и как ключевой ресурс обеспечения защиты информации.

Исследование угроз информационной безопасности, связанных с действиями пользователей, выявило многообразие проявлений человеческого фактора: от непреднамеренных технических ошибок до целенаправленной эксплуатации психологических особенностей персонала методами

социальной инженерии. Значительная часть успешных кибератак базируется на использовании уязвимостей, обусловленных недостаточной осведомлённостью или невнимательностью пользователей, что подчёркивает критическую важность организационных мер защиты.

Анализ организационных мер повышения киберустойчивости продемонстрировал необходимость комплексного подхода, сочетающего формирование культуры информационной безопасности, систематическое обучение персонала и разработку эффективных политик и процедур [5, 13]. Формирование культуры безопасности требует долгосрочных системных усилий и активного вовлечения высшего руководства. Система обучения должна основываться на принципах непрерывности, релевантности и практической ориентированности, адаптируясь к специфике деятельности различных категорий персонала.

На основе проведенного анализа и выявленных уязвимостей, был разработан комплекс организационных мер, направленных на минимизацию влияния человеческого фактора. Данные меры систематизированы и представлены в Таблице 1.

Таблица 1 — Предлагаемый комплекс организационных мер

Наименование меры	Содержание мероприятия	Ожидаемый результат и метрики (KPI)
1. Внедрение адаптивной системы обучения	Переход от разовых инструктажей к непрерывному циклу подготовки. Включает входное тестирование знаний, специализированные модули для разных ролей (IT, бухгалтерия, HR) и регулярное микро-обучение (microlearning) по актуальным угрозам.	Формирование устойчивых знаний. KPI: Охват персонала обучением > 95%; средний балл тестирования не ниже 80%.
2. Регулярная симуляция	Проведение учебных фишинговых кампаний (email,	Выработка практического навыка распознавания

социотехнических атак	мессенджеры) не реже 1 раза в квартал. Обязательный разбор ошибок (debriefing) с сотрудниками, не распознавшими атаку.	угроз. KPI: Снижение доли переходов по фишинговым ссылкам (Click Rate) на 10-15% ежеквартально.
3. Формализация процедур реагирования	Разработка алгоритмов действий (playbooks) для сотрудников при подозрении на инцидент. Внедрение упрощенных каналов информирования (например, кнопка «Сообщить о фишинге» в почтовом клиенте).	Ускорение обнаружения инцидентов. KPI: Сокращение времени от начала атаки до сообщения пользователя (Mean Time to Detect via User).
4. Интеграция показателей киберкультуры в KPI	Включение метрик соблюдения требований ИБ подчиненными (например, отсутствие инцидентов, прохождение обучения) в систему оценки эффективности руководителей подразделений.	Повышение вовлеченности менеджмента в вопросы ИБ. KPI: Процент подразделений без повторных нарушений политик безопасности.
5. Внедрение принципа «Security by Design»	Обязательная экспертиза безопасности при изменении бизнес-процессов, закупке или внедрении нового ПО на этапе планирования (до начала эксплуатации).	Снижение стоимости устранения уязвимостей. KPI: Количество рисков, выявленных и устраненных на этапе проектирования системы.

Реализация представленных в Таблице 1 мер позволит не только снизить вероятность возникновения инцидентов, но и создать измеримую систему контроля состояния киберкультуры в организации.

Практическая значимость исследования заключается в выработке рекомендаций по построению эффективной системы управления киберрисками с учётом роли человеческого фактора. Ключевыми элементами такой системы являются: создание культуры ответственного отношения к

вопросам безопасности, реализация программ обучения и повышения осведомлённости, разработка понятных и практически применимых политик и процедур, установление механизмов мониторинга и постоянного совершенствования организационных мер защиты.

Список использованных источников

1. Баранова Е. К. Управление рисками информационной безопасности в условиях цифровой трансформации / Е. К. Баранова, А. В. Бабаш // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 2–13.
2. Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Доклад об инцидентах в сфере информационной безопасности за 2024 год [Электронный ресурс]. – URL: https://ncircc.ru (дата обращения: 10.02.2026).
3. Приказ ФСТЭК России от 22.03.2023 № 61 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации» [Электронный ресурс]. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/2500 (дата обращения: 10.02.2026).
4. Суворова Г. М. Социальная инженерия как угроза корпоративной информационной безопасности: методы противодействия / Г. М. Суворова, Р. О. Дмитриев // Вопросы кибербезопасности. – 2024. – № 2(60). – С. 14–26.
5. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (в редакции 2024 года) [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/47851 (дата обращения: 10.02.2026).
6. Федотова Е. Л. Формирование культуры информационной безопасности в организации: поведенческий подход / Е. Л. Федотова // Вестник

Российского экономического университета имени Г. В. Плеханова. – 2024. – № 3. – С. 118–127.

7. Чекулаев М. В. Киберустойчивость организаций: концептуальные основы и практические механизмы обеспечения / М. В. Чекулаев, С. А. Петренко // Вопросы кибербезопасности. – 2025. – № 1(63). – С. 32–45.
8. Шилов Н. Е. Психологические аспекты противодействия атакам социальной инженерии в корпоративной среде / Н. Е. Шилов, Д. А. Коробейников // Безопасность информационных технологий. – 2024. – № 4. – С. 55–67.
9. Gartner Research. Security Awareness Training Market Guide 2024 [Electronic resource]. – URL: https://www.gartner.com/en/documents/security-awareness-training (accessed: 10.02.2026).
10. IBM Security. Cost of a Data Breach Report 2024 [Электронный ресурс]. -- URL: https://www.ibm.com/security/data-breach (дата обращения: 10.02.2026).
11. Microsoft. Digital Defense Report 2024 [Электронный ресурс]. -- URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024 (дата обращения: 10.02.2026).
12. Positive Technologies. Актуальные киберугрозы: итоги 2024 года [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 10.02.2026).
13. Proofpoint. State of the Phish Report 2024 [Electronic resource]. – URL: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (accessed: 10.02.2026).
14. SANS Institute. Security Awareness Report 2024 [Electronic resource]. – URL: https://www.sans.org/security-awareness-training/resources/reports/ssar-2024 (accessed: 10.02.2026).

15. Verizon Business. Data Breach Investigations Report 2024 [Electronic resource]. – URL: https://www.verizon.com/business/resources/reports/dbir/ (accessed: 10.02.2026).

References

1. Baranova E. K., Babash A. V. Upravlenie riskami informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii [Information security risk management in the context of digital transformation] // Voprosy kiberbezopasnosti. – 2024. – No. 1(59). – P. 2–13.
2. Natsional'nyy koordinatsionnyy tsentr po komp'yuternym intsidentam (NKTsKI). Doklad ob intsidentakh v sfere informatsionnoy bezopasnosti za 2024 god [Report on information security incidents in 2024]. – URL: https://ncircc.ru (accessed: 10.02.2026).
3. Prikaz FSTEK Rossii ot 22.03.2023 No. 61 «Ob utverzhdenii Trebovaniy po bezopasnosti informatsii» [Order of FSTEC Russia No. 61 "On Approval of Information Security Requirements"]. – URL: https://fstec.ru (accessed: 10.02.2026).
4. Suvorova G. M., Dmitriev R. O. Sotsial'naya inzheneriya kak ugroza korporativnoy informatsionnoy bezopasnosti [Social engineering as a threat to corporate information security] // Voprosy kiberbezopasnosti. – 2024. – No. 2(60). – P. 14–26.
5. Ukaz Prezidenta RF ot 01.05.2022 No. 250 «O dopolnitel'nykh merakh po obespecheniyu informatsionnoy bezopasnosti Rossiyskoy Federatsii» [Decree of the President of the Russian Federation No. 250 "On Additional Measures to Ensure Information Security"]. – URL: http://www.kremlin.ru/acts/bank/47851 (accessed: 10.02.2026).
6. Fedotova E. L. Formirovanie kul'tury informatsionnoy bezopasnosti v organizatsii: povedencheskiy podkhod [Forming an information security

culture: a behavioral approach] // Vestnik Rossiyskogo ekonomicheskogo universiteta imeni G. V. Plekhanova. – 2024. – No. 3. – P. 118–127.

7. Chekulaev M. V., Petrenko S. A. Kiberustoychivost' organizatsiy: kontseptual'nye osnovy i prakticheskie mekhanizmy [Cyber resilience of organizations: conceptual foundations and practical mechanisms] // Voprosy kiberbezopasnosti. – 2025. – No. 1(63). – P. 32–45.
8. Shilov N. E., Korobeynikov D. A. Psikhologicheskie aspekty protivodeystviya atakam sotsial'noy inzhenerii [Psychological aspects of countering social engineering attacks] // Bezopasnost' informatsionnykh tekhnologiy. – 2024. – No. 4. – P. 55–67.
9. Gartner Research. Security Awareness Training Market Guide 2024. – URL: https://www.gartner.com (accessed: 10.02.2026).
10. IBM Security. Cost of a Data Breach Report 2024. – URL: https://www.ibm.com/security/data-breach (accessed: 10.02.2026).
11. Microsoft. Digital Defense Report 2024. – URL: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024 (accessed: 10.02.2026).
12. Positive Technologies. Aktual'nye kibeugrozy: itogi 2024 goda [Current cyber threats: 2024 results]. – URL: https://www.ptsecurity.com (accessed: 10.02.2026).
13. Proofpoint. State of the Phish Report 2024. – URL: https://www.proofpoint.com (accessed: 10.02.2026).
14. SANS Institute. Security Awareness Report 2024. – URL: https://www.sans.org (accessed: 10.02.2026).
15. Verizon Business. Data Breach Investigations Report 2024. – URL: https://www.verizon.com/business/resources/reports/dbir/ (accessed: 10.02.2026).