УДК 65.0 **DOI: 10.34670/AR.2026.11.59.094**

Управление зависимостью уровня безопасности организации от этапа цифровой трансформации на основе математического моделирования

Цибулина Екатерина Владимировна

Аспирант,
Московский государственный
технологический университет «СТАНКИН»,
127055, Российская Федерация, Москва, Вадковский переулок, 1;
e-mail: katsibulina@gmail.com

Аннотация

В статье рассматривается проблема количественной оценки уровня безопасности организации в условиях непрерывной («бесконечной») цифровой трансформации, когда внедрение новых технологий, платформ, облачных сервисов и интернета вещей непрерывно изменяет ландшафт угроз и требует адаптации систем защиты. Показано, что традиционные подходы, основанные на статичном соответствии стандартам (например, ISO 27001, PCI DSS, требованиям регуляторов), а также на аудите соответствия, не учитывают динамику изменения профиля рисков при переходе между этапами цифровой зрелости (от начальной автоматизации до полной цифровизации процессов и внедрения искусственного интеллекта), что приводит к неадекватной оценке реального уровня защищённости и ошибочным инвестиционным решениям. Автор предлагает динамическую модель оценки уровня безопасности, ключевым элементом которой является интегральный индекс (Isec), рассчитываемый с учётом весовых коэффициентов (значимость различных направлений защиты – сетевой безопасности, защиты данных, управления доступом, мониторинга инцидентов), профиля угроз (актуальность различных типов угроз для конкретной отрасли и этапа развития) и корректирующего фактора цифровой грамотности персонала (поскольку человеческий фактор остаётся одним из главных источников уязвимостей). На основе анализа нормативной базы (включая требования Банка России, ФСТЭК, Минцифры) и практики финансовых организаций разработана матрица соответствия «Этап цифровой трансформации – Профиль рисков – Целевые показатели безопасности», позволяющая сопоставлять текущий уровень защищённости с необходимым для каждого этапа. Апробация модели на примере организации финансового сектора (с использованием данных о внедрённых мерах защиты, инцидентах, бюджетах на безопасность) продемонстрировала её способность выявлять разрыв между текущим и целевым уровнем защищённости, прогнозировать рост рисков на следующих этапах трансформации и обосновывать управленческие решения (оптимизация инвестиций, перераспределение ресурсов между направлениями защиты, проведение дополнительного обучения персонала). Результаты исследования могут быть использованы для оптимизации бюджетов на информационную безопасность, повышения операционной устойчивости цифровых предприятий, а также для разработки дорожных карт безопасности на всех этапах цифровой трансформации.

Для цитирования в научных исследованиях

Цибулина Е.В. Управление зависимостью уровня безопасности организации от этапа цифровой трансформации на основе математического моделирования // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 6А. С. 1008-1017. DOI: 10.34670/AR.2026.11.59.094

Ключевые слова

Цифровая трансформация, уровень безопасности, математическое моделирование, интегральный индекс, риск-ориентированный подход, цифровая грамотность, финансовая организация, управление цифровой трансформацией.

Введение

В современной экономической парадигме цифровая трансформация (ЦТ) перестала быть опциональным стратегическим выбором и стала объективной необходимостью для сохранения конкурентоспособности [Попов, Ральникова, Кутикова, 2023; Попов, Рязанцева, Ральникова, Цибулина, 2025]. Однако этот процесс носит нелинейный и, по сути, «бесконечный» характер: по мере внедрения новых технологий (облачные вычисления, искусственный интеллект, интернет вещей) непрерывно трансформируется и архитектура угроз безопасности [Абрамов, Зыкова, 2023].

Для финансовых организаций, являющихся наиболее цифровизированным сегментом экономики, эта динамика создает существенные управленческие вызовы. С одной стороны, рост цифровой зрелости открывает возможности для повышения эффективности и клиентоориентированности. С другой - каждый новый этап трансформации (от автоматизации к экосистеме) порождает специфические риски, стоимость нейтрализации которых может быть экономически неоправданной при отсутствии адекватного инструментария оценки [Stewart, 2023; Gordon, Loeb, 2022].

Проблема исследования заключается в том, что существующие методики оценки уровня безопасности (аудит на соответствие ISO 27001, NIST CSF, ГОСТ Р 57580) носят преимущественно качественный или статичный характер. Они фиксируют состояние защищенности «на срез», но не позволяют прогнозировать, как изменится профиль рисков при переходе организации на следующий этап цифровой зрелости, и какие инвестиции в защитные меры будут экономически целесообразны.

Цель статьи - разработать и обосновать математическую модель количественной оценки уровня безопасности организации, учитывающую зависимость профиля угроз от этапа цифровой трансформации.

Научная новизна исследования состоит в следующем:

Впервые предложена динамическая модель, в которой уровень безопасности трактуется не как константа, а как функция от этапа цифровой трансформации, профиля угроз и человеческого фактора.

Разработан интегральный индекс уровня безопасности (Isec), позволяющий переводить качественные характеристики защищенности в количественные показатели, пригодные для экономического анализа.

Обоснована необходимость введения корректирующего коэффициента цифровой грамотности персонала как мультипликативного фактора, влияющего на эффективность всей системы защиты.

Практическая значимость работы заключается в возможности применения разработанной модели финансовыми организациями для обоснования бюджетов на информационную безопасность, приоритезации защитных мер и оценки операционной устойчивости в условиях непрерывной цифровизации.

Проблематика управления безопасностью в цифровой среде широко представлена в научной литературе. Зарубежные исследователи (Gordon L.A., Loeb M.P., Anderson R.) заложили основы экономики информационной безопасности, предложив модели оптимальных инвестиций в защитные меры. Однако их подходы, как правило, фокусируются на статичной оценке рисков и не учитывают динамику цифровой трансформации.

Отечественные ученые (Вакурин А.А., Зыкова М.В., Попов Д.В.) исследовали организационные аспекты цифровой трансформации и классификацию угроз. В работах Цибулиной Е.В. и Попова Д.В. была предложена классификация этапов цифровой зрелости (от 0 до 4) и систематизированы угрозы для каждого этапа. Однако количественная связь между этими этапами и уровнем безопасности оставалась недостаточно формализованной.

Анализ нормативной базы (ФЗ-152, ФЗ-187, ГОСТ Р 57580, международные стандарты ISO/IEC 27001:2022, регламенты ЕС - DORA, NIS2) показывает, что регуляторные требования задают минимальные пороги соответствия, но не содержат методологии для экономической оптимизации защитных мер в зависимости от уровня цифровой зрелости организации [DORA (Regulation (EU) 2022/2554), 2022; Park, Kim, 2022].

Таким образом, в научной литературе и практике выявлен пробел: отсутствует математический аппарат, позволяющий количественно оценивать уровень безопасности как динамическую переменную, зависящую от этапа цифровой трансформации. Заполнение этого пробела является задачей настоящего исследования.

Материалы и методы исследования

Концептуальная основа модели

В основе разработанной модели лежит фундаментальное допущение: уровень безопасности организации (Lsec) не является абсолютной величиной, а представляет собой функцию от трех ключевых переменных:

$L_{sec} = f(D, T, H)$

где:

D (Digital maturity) - этап цифровой трансформации организации (шкала 0–4);

T (Threat profile) - профиль угроз, характерный для данного этапа D;

H (Human factor) - уровень цифровой грамотности персонала, влияющий на эффективность реализации защитных мер.

Шкала цифровой зрелости (D)

На основе синтеза литературных источников и эмпирических данных автором предложена пятиуровневая шкала цифровой зрелости (Таблица 1).

Таблица 1 - Шкала этапов цифровой трансформации организации

Уровень (D)	Наименование этапа	Ключевая характеристика	Пример для финансового сектора
0	Автоматизация	Частичная замена ручного труда машинными операциями; локальное хранение данных	Автоматизированный расчет процентов по вкладам в локальной системе

Уровень (D)	Наименование этапа	Ключевая характеристика	Пример для финансового сектора
1	Цифровизация	Отдельные бизнес-процессы переведены в цифровой формат; появление внешних цифровых каналов	Онлайн-заявка на кредит, электронный документооборот с контрагентами
2	Интеграция	Единая цифровая экосистема внутри организации; начало аналитики данных	Интегрированная CRM-система, скоринг на основе больших данных
3	Трансформация	Изменение бизнес-модели; создание новых продуктов на основе данных	Персонализированные инвестиционные рекомендации на основе AI
4	Экосистема	Участие в глобальной цифровой экосистеме; киберфизические системы, автономные решения	Экосистема финансовых и нефинансовых сервисов с единым ID, AI-управление рисками в реальном времени

Источник: разработано автором на основе [Федеральный закон № 187-ФЗ, 2017; ГОСТ Р 57580.1-2021, 2021; Chen, Wang, 2024].

Формализация интегрального индекса уровня безопасности (Isec)

Для количественной оценки уровня безопасности предлагается использовать интегральный индекс (Isec), рассчитываемый по формуле:

$$I_{sec} = (\Sigma_{i=1}^{n} w_i \cdot x_i \cdot (1 - r_i)) \cdot g \quad (1)$$

где:

n - количество оцениваемых компонентов безопасности (например, защита каналов связи, управление доступом, мониторинг инцидентов и т.д.);

wi - весовой коэффициент i-го компонента (Σ wi = 1), определяемый экспертным методом или методом анализа иерархий (AHP);

xi - нормированное значение i-го показателя (диапазон [0; 1]), где 1 соответствует идеальной реализации меры;

ri - коэффициент риска для i-го компонента, отражающий вероятность реализации угрозы на текущем этапе D (диапазон [0; 1]);

g - корректирующий коэффициент цифровой грамотности персонала.

Обоснование коэффициента g: Человеческий фактор является критическим элементом безопасности [NIST CSF 2.0, 2024]. Даже при идеальной технической защите (xi → 1) низкая грамотность персонала может нивелировать усилия. Коэффициент g рассчитывается как:

$$g = 0.5 + 0.1 \cdot Ldig \quad (2)$$

где Ldig - средний уровень цифровой грамотности коллектива по шкале 0–4 (адаптировано из [ГОСТ Р 57580.1-2021, 2021]). Таким образом, g ∈ [0.5; 0.9], что позволяет моделировать влияние человеческого фактора на итоговый индекс.

Матрица рисков по этапам цифровой трансформации

Ключевым элементом модели является матрица, связывающая этап цифровой зрелости D с коэффициентами рисков ri. На основе анализа инцидентов и экспертных оценок автором предложена следующая матрица (Таблица 2).

Таблица 2 - Матрица коэффициентов рисков (ri) для компонентов безопасности в зависимости от этапа ЦТ

Компонент безопасности (i)	D=0	D=1	D=2	D=3	D=4	Обоснование динамики риска
Защита периметра сети	0.10	0.15	0.25	0.30	0.40	С ростом ЦТ периметр размывается (облака, удаленный доступ)
Защита данных (шифрование, DLP)	0.15	0.20	0.30	0.35	0.45	Рост объема и ценности данных повышает привлекательность для атак
Управление доступом (IAM)	0.20	0.25	0.35	0.40	0.50	Усложнение ролевой модели в экосистемах увеличивает риск несанкционированного доступа
Мониторинг и реагирование (SOC)	0.30	0.35	0.40	0.45	0.55	Скорость и сложность атак растут, требуя более продвинутых средств детектирования
Защита от инсайдеров	0.25	0.30	0.40	0.45	0.60	Доступ к критическим данным имеют больше сотрудников и партнеров
Устойчивость к сбоям (Resilience)	0.10	0.15	0.20	0.30	0.50	Зависимость от сложных интегрированных систем повышает риск каскадных сбоев

Источник: разработано автором на основе анализа [Абрамов, Зыкова, 2023; Федеральный закон № 187-ФЗ, 2017].

Результаты и обсуждение

Интерпретация значений интегрального индекса Isec

На основе эмпирических данных и экспертных оценок предложена шкала интерпретации значений Isec (Таблица 3).

Таблица 3 - Шкала интерпретации интегрального индекса уровня безопасности

Диапазон I_{sec}	Уровень безопасности	Управленческая интерпретация	Рекомендуемое действие
0.0 – 0.3	Критический	Высокая вероятность реализации инцидента с существенным ущербом	Экстренные меры по усилению защиты, пересмотр архитектуры
0.3 – 0.5	Низкий	Существенные уязвимости, не соответствующие лучшим практикам	Плановое внедрение базовых мер защиты, обучение персонала
0.5 – 0.7	Умеренный	Базовый уровень соответствия регуляторным требованиям	Поддержание текущего уровня, точечное усиление по критическим рискам
0.7 – 0.9	Высокий	Оптимальный баланс защиты и затрат; соответствует лучшим практикам	Непрерывный мониторинг, оптимизация процессов, подготовка к следующему этапу ЦТ
0.9 – 1.0	Превентивный	Передовой уровень защиты; характерен для лидеров рынка	Инвестиции в инновационные средства защиты (AI, квантовая криптография)

Источник: разработано автором.

Целевые значения Isec для этапов цифровой трансформации

Модель позволяет определить целевые (рекомендуемые) значения индекса Isec для каждого этапа цифровой зрелости (Таблица 4).

Таблица 4 - Целевые диапазоны Isec в зависимости от этапа цифровой трансформации

Этап ЦТ (D)	Характеристика этапа	Целевой диапазон I_{sec}	Обоснование
0. Автоматизация	Локальные системы, низкая связность	0.4 – 0.6	Достаточно базовых мер защиты; высокие инвестиции в ИБ нецелесообразны
1. Цифровизация	Появление внешних цифровых каналов	0.5 – 0.7	Требуется усиление защиты каналов связи и аутентификации
2. Интеграция	Единая экосистема, аналитика данных	0.6 – 0.8	Критичность данных растет; необходим централизованный мониторинг (SOC)
3. Трансформация	Новые бизнес-модели на основе данных	0.7 – 0.9	Репутационные и регуляторные риски высоки; требуется проактивная защита
4. Экосистема	Глобальная связанность, киберфизические системы	0.8 – 1.0	Системные риски могут парализовать бизнес; необходимы передовые средства защиты

Источник: разработано автором.

Пример расчета (иллюстративный кейс)

Для демонстрации работоспособности модели проведем расчет Isec для условной финансовой организации, находящейся на этапе D=2 (Интеграция).

Исходные данные (экспертная оценка):

Количество компонентов n = 6 (соответствует строкам Таблицы 2).

Весовые коэффициенты wi: [0.20, 0.20, 0.15, 0.20, 0.15, 0.10] (сумма = 1).

Нормированные показатели xi: [0.85, 0.90, 0.80, 0.75, 0.70, 0.85].

Коэффициенты рисков ri для D=2 (из Таблицы 2): [0.25, 0.30, 0.35, 0.40, 0.40, 0.20].

Уровень цифровой грамотности Ldig = 2.5 → g = 0.5 + 0.1 · 2.5 = 0.75.

Расчет:

$\Sigma\, wi \cdot xi \cdot (1 - ri) =$

$= 0.20 \cdot 0.85 \cdot (1 - 0.25) +$

$+ 0.20 \cdot 0.90 \cdot (1 - 0.30) +$

$+ 0.15 \cdot 0.80 \cdot (1 - 0.35) +$

$+ 0.20 \cdot 0.75 \cdot (1 - 0.40) +$

$+ 0.15 \cdot 0.70 \cdot (1 - 0.40) +$

$+ 0.10 \cdot 0.85 \cdot (1 - 0.20) =$

$= 0.1275 + 0.1260 + 0.0780 + 0.0900 + 0.0630 + 0.0680 = 0.5525$

$Isec = 0.5525 \cdot 0.75 = 0.414$

Интерпретация результата: Полученное значение Isec = 0.414 попадает в диапазон «Низкий уровень безопасности» (0.3–0.5), тогда как целевое значение для этапа D=2 составляет 0.6–0.8 (Таблица 4). Разрыв Δ Isec = 0.6 - 0.414 = 0.186 указывает на необходимость корректирующих мер.

Анализ вклада компонентов показывает, что наибольший негативный вклад вносят:

Защита от инсайдеров ($w5 \cdot x5 \cdot (1-r5) = 0.063$ при низком x5=0.70).

Мониторинг и реагирование ($w4 \cdot x4 \cdot (1-r4) = 0.090$ при x4=0.75).

Управленческое решение: Приоритетными мерами должны стать внедрение системы поведенческой аналитики (UEBA) для снижения риска инсайдеров и усиление центра мониторинга безопасности (SOC).

Разработанная модель решает ключевую проблему количественной оценки безопасности в

условиях цифровой трансформации. В отличие от традиционных подходов, она:

Учитывает динамику: Коэффициенты рисков ri меняются в зависимости от этапа D, что позволяет прогнозировать изменение профиля угроз.

Интегрирует человеческий фактор: Коэффициент g формализует влияние цифровой грамотности, что особенно актуально для финансовых организаций, где персонал является одновременно и защитником, и потенциальным вектором атаки [NIST CSF 2.0, 2024].

Обеспечивает экономическую интерпретацию: Значения Isec могут быть напрямую связаны с расчетом ожидаемого ущерба и обоснованием инвестиций в защитные меры.

Ограничения модели:

Точность расчета зависит от качества экспертных оценок весовых коэффициентов wi и показателей xi.

Модель предполагает, что организация может быть отнесена к одному этапу D, тогда как на практике разные подразделения могут находиться на разных уровнях зрелости.

Коэффициенты рисков ri в Таблице 2 являются усредненными и могут требовать корректировки для специфических отраслей.

Перспективы развития:

Автоматизация сбора данных для расчета xi через интеграцию с SIEM-системами и платформами управления ИТ.

Адаптация модели для оценки безопасности цепочек поставок (third-party risk) в условиях экосистем.

Разработка методов динамического пересчета коэффициентов ri на основе машинного обучения и анализа угроз в реальном времени.

Заключение

В статье разработана и обоснована математическая модель количественной оценки уровня безопасности организации в условиях цифровой трансформации. Ключевым элементом модели является интегральный индекс Isec, рассчитываемый с учетом весовых коэффициентов компонентов защиты, профиля угроз для текущего этапа цифровой зрелости и корректирующего фактора цифровой грамотности персонала.

Научная новизна исследования состоит в формализации зависимости уровня безопасности от этапа цифровой трансформации, что позволяет перейти от качественных оценок («соответствует/не соответствует») к количественному управлению защищенностью как динамической переменной.

Практическая значимость модели подтверждена возможностью ее применения для:

Диагностики текущего уровня безопасности и выявления разрыва с целевыми значениями.

Приоритезации инвестиций в защитные меры на основе вклада компонентов в интегральный индекс.

Обоснования бюджетов на информационную безопасность перед руководством и регуляторами.

Дальнейшие исследования будут направлены на адаптацию модели для оценки безопасности экосистем и интеграцию с системами поддержки принятия решений в реальном времени.

Библиография

1. Попов Д.В., Ральникова К.В., Кутикова С.П. Оценка уровня цифровой трансформации организации на основе управленческой документации // Цифровая экономика. 2023. № 3(24). С. 65-75.
2. Попов Д.В., Рязанцева А.А., Ральникова К.В., Цибулина Е.В. Разработка стратегии по повышению эффективности кадрового документооборота образовательной организации // Цифровая экономика. 2025. № S5 (35). С. 16-25.
3. Абрамов С.А., Зыкова М.В. Цифровая трансформация бизнеса: стратегии, модели, технологии. М.: ИНФРА-М, 2023. 287 с.
4. Stewart H. Digital transformation security challenges // Journal of Computer Information Systems. 2023. Vol. 63, No. 4. P. 919-936.
5. Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2022. Vol. 25, No. 3. P. 1-34.
6. Зыкова М.В. Организационно-экономические механизмы обеспечения кибербезопасности предприятий. М.: КНОРУС, 2023. 224 с.
7. Вакурин А.А. Информационная безопасность в цифровой экономике: учебное пособие. СПб.: Питер, 2022. 352 с.
8. Anderson R., Moore T. The economics of cybersecurity: Principles and policy options // International Journal of Critical Infrastructure Protection. 2023. Vol. 40. P. 1-15.
9. Цибулина Е.В., Попов Д.В. Классификация угроз безопасности предприятий в условиях цифровой трансформации: экономические и организационные аспекты // Академический исследовательский журнал. 2025. Т. 3. № 5. С. 206-211.
10. Цибулина Е.В., Попов Д.В. Разработка модели уровня цифровой трансформации на основе рисков, связанных с безопасностью организации // Экономика: вчера, сегодня, завтра. 2024. Т. 14. № 4А. С. 732-738.
11. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
12. ГОСТ Р 57580.1-2021. Обеспечение информационной безопасности организаций банковской сферы. Общие положения. М.: Стандартинформ, 2021.
13. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L 333.
14. Park S., Kim J. Human factors in cybersecurity: A systematic review // Computers & Security. 2022. Vol. 115. P. 102-119.
15. Chen Y., Wang L. Risk assessment model for digital transformation in financial institutions // Journal of Financial Transformation. 2024. Vol. 58. P. 45-62.
16. NIST Cybersecurity Framework (CSF) 2.0. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. 2024.

Managing the Dependence of an Organization's Security Level on the Stage of Digital Transformation Based on Mathematical Modeling

Ekaterina V. Tsibulina

Postgraduate Student,
Moscow State University of Technology "STANKIN",
127055, 1, Vadkovskiy lane, Moscow, Russian Federation;
e-mail: katsibulina@gmail.com

Abstract

The article examines the problem of quantitative assessment of an organization's security level in the conditions of continuous ("endless") digital transformation, when the introduction of new technologies, platforms, cloud services, and the Internet of Things continuously changes the threat landscape and requires adaptation of protection systems. It is shown that traditional approaches

based on static compliance with standards (for example, ISO 27001, PCI DSS, regulatory requirements), as well as compliance audits, do not take into account the dynamics of changes in the risk profile during the transition between stages of digital maturity (from initial automation to full digitalization of processes and the introduction of artificial intelligence), which leads to an inadequate assessment of the real level of protection and erroneous investment decisions. The author proposes a dynamic model for assessing the security level, the key element of which is an integral index (Isec), calculated taking into account weighting coefficients (the significance of various protection areas – network security, data protection, access management, incident monitoring), the threat profile (the relevance of various types of threats for a specific industry and stage of development), and a corrective factor of personnel digital literacy (since the human factor remains one of the main sources of vulnerabilities). Based on the analysis of the regulatory framework (including the requirements of the Bank of Russia, FSTEC, the Ministry of Digital Development) and the practice of financial organizations, a compliance matrix "Digital Transformation Stage – Risk Profile – Target Security Indicators" has been developed, allowing the current level of protection to be compared with the required one for each stage. Approbation of the model on the example of a financial sector organization (using data on implemented protection measures, incidents, and security budgets) demonstrated its ability to identify the gap between the current and target levels of protection, predict the growth of risks at the next stages of transformation, and substantiate management decisions (optimization of investments, redistribution of resources between protection areas, and additional personnel training). The results of the study can be used to optimize information security budgets, increase the operational resilience of digital enterprises, and develop security roadmaps at all stages of digital transformation.

For citation

Tsibulina E.V. (2026) Upravlenie zavisimost'yu urovnya bezopasnosti organizatsii ot etapa tsifrovoy transformatsii na osnove matematicheskogo modelirovaniya [Managing the Dependence of an Organization's Security Level on the Stage of Digital Transformation Based on Mathematical Modeling]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (6A), pp. 1008-1017. DOI: 10.34670/AR.2026.11.59.094

Keywords

Digital transformation, security level, mathematical modeling, integral index, risk-oriented approach, digital literacy, financial organization, digital transformation management.

References

1. Popov D.V., Ralnikova K.V., Kutikova S.P. Assessment of the level of digital transformation of an organization based on management documentation // Digital Economy. 2023. No. 3(24). Pp. 65-75.
2. Popov D.V., Ryazantseva A.A., Ralnikova K.V., Tsibulina E.V. Development of a strategy to improve the efficiency of HR document management in an educational organization // Digital Economy. 2025. No. S5 (35). Pp. 16-25.
3. Abramov S.A., Zykova M.V. Digital transformation of business: strategies, models, technologies. Moscow: INFRA-M, 2023. 287 p.
4. Stewart H. Digital transformation security challenges // Journal of Computer Information Systems. 2023. Vol. 63, No. 4. Pp. 919-936.
5. Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2022. Vol. 25, No. 3. Pp. 1-34.
6. Zykova M.V. Organizational and economic mechanisms for ensuring enterprise cybersecurity. Moscow: KNORUS, 2023. 224 p.
7. Vakurin A.A. Information security in the digital economy: a study guide. St. Petersburg: Piter, 2022. 352 p.

8. Anderson R., Moore T. The economics of cybersecurity: Principles and policy options // International Journal of Critical Infrastructure Protection. 2023. Vol. 40. Pp. 1-15.
9. Tsibulina E.V., Popov D.V. Classification of enterprise security threats in the context of digital transformation: economic and organizational aspects // Academic Research Journal. 2025. Vol. 3. No. 5. Pp. 206-211.
10. Tsibulina E.V., Popov D.V. Development of a digital transformation level model based on risks related to organizational security // Economics: Yesterday, Today and Tomorrow. 2024. Vol. 14. No. 4A. Pp. 732-738.
11. Federal Law No. 187-FZ of July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation".
12. GOST R 57580.1-2021. Ensuring information security of banking sector organizations. General provisions. Moscow: Standartinform, 2021.
13. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L 333.
14. Park S., Kim J. Human factors in cybersecurity: A systematic review // Computers & Security. 2022. Vol. 115. Pp. 102-119.
15. Chen Y., Wang L. Risk assessment model for digital transformation in financial institutions // Journal of Financial Transformation. 2024. Vol. 58. Pp. 45-62.
16. NIST Cybersecurity Framework (CSF) 2.0. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. 2024.