

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2025, Том 17, № s3 / 2025, Vol. 17, Iss. s3 <https://esj.today/issue-s3-2025.html>

URL статьи: <https://esj.today/PDF/47FAVN325.pdf>

5.2.4. Финансы (экономические науки)

Ссылка для цитирования этой статьи:

Шушонов, И. А. Экономическая целесообразность внедрения технологий искусственного интеллекта в системы защиты финансовой информации / И. А. Шушонов // Вестник евразийской науки. — 2025. — Т. 17. — № s3. — URL: <https://esj.today/PDF/47FAVN325.pdf>.

For citation:

Shushokov I.A. Economic feasibility of implementing artificial intelligence technologies into financial information security systems. *The Eurasian Scientific Journal*. 2025;17(s3): 47FAVN325. Available at: <https://esj.today/PDF/47FAVN325.pdf>. (In Russ., abstract in Eng.).

УДК 336.7:004.89:338.012

Шушонов Ислам Асланович

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: prilipko1337@mail.ru

Экономическая целесообразность внедрения технологий искусственного интеллекта в системы защиты финансовой информации

Аннотация. Современные реалии цифровой экономики характеризуются экспоненциальным ростом объемов финансовых данных и усложнением киберугроз, требующих от финансовых организаций формирования инновационных подходов к обеспечению информационной безопасности. Данное исследование посвящено комплексному анализу экономической эффективности внедрения технологий искусственного интеллекта в системы защиты финансовой информации через призму теоретических концепций экономики информационной безопасности и эмпирических данных российского и зарубежного опыта. Рассматриваются возможности оптимизации соотношения затрат и выгод при использовании ИИ-технологий для предотвращения финансовых потерь от киберинцидентов, повышения эффективности процессов мониторинга и анализа угроз, автоматизации процедур аудита информационной безопасности. Анализируется эволюция научных подходов к экономической оценке инвестиций в информационную безопасность от классических моделей анализа рисков до современных интегративных концепций, учитывающих стратегические и репутационные факторы. Особое внимание уделяется теоретическому обоснованию методологических принципов расчета экономической эффективности ИИ-решений в контексте защиты финансовой информации, включая модели оценки возврата инвестиций, анализ совокупной стоимости владения и методы прогнозирования предотвращенного ущерба. Исследование демонстрирует, что экономическая целесообразность внедрения ИИ-технологий в финансовую кибербезопасность определяется комплексом факторов, включающих масштаб обрабатываемых данных, сложность угроз, регулятивные требования и стратегические цели организации. Полученные результаты свидетельствуют о необходимости развития интегрированных подходов к экономической оценке ИИ-проектов в области финансовой безопасности, учитывающих как прямые финансовые выгоды, так и косвенные эффекты в виде повышения операционной эффективности, укрепления репутации и соответствия регулятивным требованиям. Разработанная автором методологическая модель экономической оценки включает четыре основных компонента: анализ затрат на внедрение и эксплуатацию ИИ-систем, оценку прямых экономических выгод от предотвращения инцидентов, расчет

косвенных эффектов от повышения операционной эффективности и учет стратегических преимуществ конкурентоспособности. Научная новизна исследования заключается в создании теоретически обоснованной концепции экономической оценки ИИ-технологий в финансовой кибербезопасности, что открывает новые возможности для принятия обоснованных инвестиционных решений в сфере защиты финансовой информации и способствует развитию теории экономики информационной безопасности.

Ключевые слова: искусственный интеллект; финансовая информационная безопасность; экономическая эффективность; цифровая экономика; киберриски; возврат инвестиций; технологические инновации; финансовые технологии; экономика безопасности

Введение

Цифровая трансформация финансового сектора, ускорившаяся в период пандемии COVID-19 и получившая дополнительный импульс в условиях геополитической турбулентности 2022–2025 годов, привела к кардинальному изменению ландшафта информационной безопасности финансовых организаций.¹ Современные исследования в области экономики информационной безопасности демонстрируют возрастающую потребность в разработке эффективных методов экономической оценки инвестиций в технологии искусственного интеллекта для защиты финансовой информации.

Согласно данным исследований, по состоянию на начало 2024 года лидером по внедрению технологий искусственного интеллекта в России является финансовый сектор, при чем около 90 % методов и инструментов ИИ, используемых российскими кредитными компаниями, основываются на методах машинного обучения.²

Крупнейшим рынком использования ИИ-решений в банковском секторе остается Северная Америка, где компании заработали 14,7 млрд на таких технологиях по итогам 2018 года, а к 2030 году экономический эффект от внедрения искусственного интеллекта в регионе прогнозируется до \$79 млрд.

Научная проблема заключается в отсутствии комплексной теоретической модели экономической оценки целесообразности внедрения ИИ-технологий в системы защиты финансовой информации, учитывающей специфику финансового сектора, многоуровневую структуру затрат и выгод, а также долгосрочные стратегические эффекты. Несмотря на наличие отдельных методик оценки экономической эффективности ИТ-инвестиций и информационной безопасности, в современной экономической науке недостаточно разработаны принципы интегральной оценки экономической целесообразности ИИ-проектов в контексте финансовой кибербезопасности.

Объектом исследования выступают экономические процессы формирования и оценки инвестиционных решений в области внедрения технологий искусственного интеллекта для защиты финансовой информации.

Предметом исследования являются теоретические основы и методологические принципы экономической оценки целесообразности инвестиций в ИИ-технологии информационной безопасности финансовых организаций в условиях цифровой экономики.

¹ Искусственный интеллект на финансовом рынке: регулирование и развитие. [Электронный ресурс]. — URL: <https://econs.online/articles/finansy/iskusstvennyy-intellekt-na-finansovom-rynke-regulirovanie-i-razvitie/> (дата обращения 02.07.2025).

² Искусственный интеллект в банках. [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках (дата обращения 02.07.2025).

Цель исследования — разработка теоретических основ и методических принципов экономической оценки целесообразности внедрения технологий искусственного интеллекта в системы защиты финансовой информации на основе анализа затрат, выгод и стратегических эффектов.

Задачи исследования:

1. Провести теоретический анализ эволюции научных подходов к экономической оценке инвестиций в информационную безопасность и ИИ-технологии в финансовом секторе.
2. Исследовать методологические основы расчета экономической эффективности ИИ-решений в области защиты финансовой информации.
3. Обосновать интегральную модель экономической оценки целесообразности внедрения ИИ-технологий в финансовую кибербезопасность.

Научная новизна исследования заключается в разработке комплексной методологической модели экономической оценки ИИ-технологий в финансовой информационной безопасности, объединяющей традиционные методы инвестиционного анализа с инновационными подходами к оценке стратегических и репутационных эффектов. Впервые предложено теоретическое обоснование четырехкомпонентной модели экономической оценки, включающей анализ затрат, прямых выгод, косвенных эффектов и стратегических преимуществ ИИ-внедрений в финансовую кибербезопасность.

Практическая значимость работы определяется возможностью применения разработанных методологических принципов в практике инвестиционного планирования финансовых организаций для повышения обоснованности решений о внедрении ИИ-технологий в системы защиты финансовой информации.

1. Методы и материалы

Методологическую основу исследования составляют принципы системного подхода в экономической науке, позволяющие рассматривать процессы внедрения ИИ-технологий в их взаимосвязи с общими стратегическими и операционными процессами финансовых организаций. Теоретической базой выступают концепции экономики информационной безопасности, разрабатываемые отечественными и зарубежными исследователями, принципы инвестиционного анализа, а также современные представления о механизмах экономической оценки технологических инноваций в финансовом секторе.

В качестве основного метода исследования использован теоретический анализ научной литературы, включающий систематизацию и обобщение результатов современных исследований в области экономики информационной безопасности, методов оценки экономической эффективности ИТ-инвестиций и анализа внедрения ИИ-технологий в финансовом секторе. Рассмотрены научные труды следующих авторов: В.И. Авдийский, В.М. Безденежных, В.Е. Лихтенштейн [1], Е.Д. Бутенко [2], ГМ. Бабукин [3], О.И. Ларина, С.С. Шкробтанова [4], А.Б. Живко, Н.А. Проданова [5], З.Р. Мазитова [6], А.С. Преображенская, М.М. Сорокина [7], О.С. Зиниша, Е.А. Волошина [8], И.А. Шабанов [9], А.А. Белоумцева, Т.Е. Даниловских [10], Ю.Ж. Юлдашев [11], М.М. Балог, А. В. Бабкин [12].

Применялись методы сравнительного анализа различных теоретических подходов, синтеза концептуальных положений и моделирования интегративных схем экономической оценки технологических инвестиций.

2. Результаты и обсуждения

Фундаментальные исследования в области экономики информационной безопасности и оценки технологических инвестиций имеют богатую историю развития, корни которой уходят к классическим работам по теории инвестиций и анализу рисков, заложивших основы понимания механизмов экономического обоснования защитных мероприятий в финансовой сфере. Эволюция научных подходов к изучению экономической эффективности инвестиций в информационную безопасность демонстрирует последовательное усложнение теоретических моделей и расширение методологического аппарата исследований, при чем каждая историческая эпоха привносила качественно новые концептуальные решения в понимание экономической природы технологических инвестиций в защиту информации.

Эволюция научных школ в изучении экономики информационной безопасности и технологических инвестиций представлена в таблице 1, отражающей ключевые этапы развития теоретических подходов к экономической оценке инвестиций в защиту информации.

Таблица 1

Эволюция научных школ в экономике информационной безопасности и технологических инвестиций

Исторический период	Научная школа	Основные представители	Ключевые концепции	Вклад в экономику ИБ
1960–1980 гг.	Классическая теория инвестиций	Г. Марковиц, У. Шарп, Дж. Тобин	Портфельная теория, CAPM, оптимизация риск-доходность	Основы количественного анализа рисков
1980–1995 гг.	Теория экономики информации	Дж. Стиглиц, М. Спенс, Дж. Акерлоф	Асимметрия информации, сигналинг, моральный риск	Понимание информации как экономического актива
1995–2005 гг.	Экономика информационной безопасности	Р. Андерсон, Б. Шнайер, Л. Гордон	Экономика безопасности, модели угроз, анализ затрат-выгод	Формирование базовых принципов экономики ИБ
2005–2015 гг.	Теория инвестиций в ИТ	Э. Бриньольфссон, Л. Хитт, П. Вейл	Парадокс производительности ИТ, цифровые опции, стратегическая ценность	Методы оценки ИТ-инвестиций
2015 — н.в.	Экономика цифровых технологий	К. Шваб, М. Кейси, В. Паркер	Цифровая трансформация, платформенная экономика, сетевые эффекты	Современные подходы к оценке цифровых технологий

Составлено автором на основе анализа материалов [13]³

Анализ представленной эволюции научных школ свидетельствует о постепенном формировании комплексного понимания экономических аспектов технологических инвестиций в информационную безопасность, при чем особенно значимым представляется переход от изолированного рассмотрения затрат на безопасность к интегральному анализу стратегической ценности технологических решений. Классическая теория инвестиций заложила фундаментальные основы количественного анализа рисков и методов оптимизации инвестиционных решений, при чем работы Г. Марковица по современной портфельной теории до сих пор сохраняют актуальность для современной практики управления технологическими рисками.

³ Финансовые кризисы искусственного интеллекта — 2: ответ регуляторов. [Электронный ресурс]. — URL: <https://econs.online/articles/opinions/finansovye-krizisy-iskusstvennogo-intellekta-2-otvet-regulyatorov/> (дата обращения 02.07.2025).

Теория экономики информации существенно расширила понимание информации как экономического актива, включив в сферу анализа проблемы асимметрии информации и стратегического поведения участников рынка, при чем работы Дж. Стиглица по экономике неопределенности и Дж. Акерлофа по проблеме неблагоприятного отбора продемонстрировали важность учета информационных факторов при экономической оценке технологических решений. Формирование экономики информационной безопасности как самостоятельного направления произошло благодаря работам Р. Андерсона и его коллег, которые впервые систематизировали экономические принципы анализа инвестиций в защиту информации и разработали базовые модели анализа затрат и выгод в области кибербезопасности.

Систематизация современных подходов к экономической оценке ИИ-технологий в финансовой информационной безопасности приведена в таблице 2, демонстрирующей разнообразие методологических подходов и их применимость к различным типам инвестиционных решений.

Таблица 2

Методические подходы к экономической оценке ИИ-технологий в финансовой ИБ

Подход	Основные методы	Области применения	Преимущества	Ограничения
Традиционный ROI	NPV, IRR, Payback Period	Прямые финансовые выгоды	Простота расчета, понятность	Не учитывает стратегические эффекты
Реальные опционы	Биномиальная модель, Монте-Карло	Неопределенность и гибкость	Учет управленческой гибкости	Сложность моделирования
Сбалансированная система показателей	Финансовые и нефинансовые KPI	Комплексная оценка эффекта	Многоаспектность анализа	Субъективность весов
Экономика экосистемы	Сетевые эффекты, платформенная ценность	Интеграционные проекты	Учет синергетических эффектов	Сложность количественной оценки
Стоимостной инжиниринг	Activity-based costing, Value analysis	Операционная эффективность	Детализация процессов	Трудозатратность анализа

Составлено автором на основе анализа материалов⁴

Развитие теории инвестиций в информационные технологии внесло существенный вклад в понимание специфики экономической оценки технологических решений, при чем работы Э. Бриньолфссона по парадоксу производительности ИТ и исследования стратегической ценности информационных систем продемонстрировали важность учета косвенных и долгосрочных эффектов при оценке технологических инвестиций. Современный этап развития экономической науки характеризуется формированием комплексных подходов к оценке цифровых технологий, учитывающих сетевые эффекты, платформенную экономику и стратегические аспекты цифровой трансформации.

Рассматривая современное состояние исследований в области экономической оценки ИИ-технологий в финансовом секторе, следует отметить растущий интерес к разработке интегрированных методик, способных учитывать многоуровневую структуру затрат и выгод от внедрения искусственного интеллекта в системы защиты финансовой информации. Анализ

⁴ Как искусственный интеллект решает задачи бизнеса. [Электронный ресурс]. — URL: <https://www.rbc.ru/business/30/07/2024/66a7a35a9a79476982873df9> (дата обращения 02.07.2025).

Искусственный интеллект в банках: ТОП-10 эффективных кейсов. [Электронный ресурс]. — URL: https://smartgopro.com/novosti2/ai_banks/ (дата обращения 02.07.2025).

российского опыта показывает, что экономическая эффективность внедрения ИИ-решений в банковской сфере может достигать значительных масштабов: например, банк ВТБ благодаря использованию голосового робота в колл-центре экономит свыше Р30 млн в месяц, а чат-бот обрабатывает свыше 40 % клиентских обращений и экономит банку больше 200 млн руб. в месяц.⁵

Структура затрат на внедрение ИИ-технологий в финансовой информационной безопасности характеризуется многокомпонентностью и включает как прямые технологические инвестиции, так и сопутствующие организационные расходы. Компонентный анализ затрат на ИИ-проекты в финансовой кибербезопасности представлен в таблице 3.

Таблица 3

**Структура затрат на внедрение
ИИ-технологий в финансовой информационной безопасности**

Категория затрат	Доля в общих затратах	Основные компоненты	Особенности планирования
Технологическая инфраструктура	35–45 %	Аппаратное обеспечение, облачные сервисы, лицензии	Масштабируемость и производительность
Разработка и интеграция	25–35 %	Разработка моделей, интеграция с существующими системами	Кастомизация под бизнес-процессы
Данные и обучение	15–25 %	Сбор данных, разметка, обучение моделей	Качество и объем обучающих данных
Персонал и обучение	10–20 %	Найм специалистов, обучение сотрудников	Дефицит квалифицированных кадров
Сопровождение и развитие	5–15 %	Техническая поддержка, обновления, мониторинг	Непрерывное развитие моделей

Составлено автором на основе анализа материалов⁶

Анализ структуры затрат показывает, что наибольшую долю составляют инвестиции в технологическую инфраструктуру, что связано с высокими требованиями к вычислительным мощностям для обработки больших объемов финансовых данных и обучения сложных моделей машинного обучения. Особенностью проектов в области финансовой информационной безопасности является повышенное внимание к качеству и безопасности обучающих данных, что увеличивает долю затрат на подготовку данных по сравнению с другими применениями ИИ.

Экономические выгоды от внедрения ИИ-технологий в системы защиты финансовой информации можно классифицировать на прямые и косвенные эффекты, при чем прямые выгоды включают сокращение потерь от киберинцидентов, снижение операционных затрат на мониторинг и анализ угроз, автоматизацию процедур аудита и комплаенса. Косвенные эффекты охватывают повышение репутации организации, улучшение качества принятия решений благодаря более точной аналитике рисков, ускорение процессов внедрения новых финансовых продуктов за счет встроенных механизмов безопасности.

⁵ Искусственный интеллект в финансах: как банки используют нейросети. [Электронный ресурс]. — URL: <https://trends.rbc.ru/trends/industry/61e924349a7947761b46f2d8> (дата обращения 02.07.2025).

⁶ Как рассчитать эффективность внедрения ИИ-решений для проверки документов. [Электронный ресурс]. — URL: <https://www.advgazeta.ru/mneniya/kak-rasschitat-effektivnost-vnedreniya-ii-resheniy-dlya-proverki-dokumentov/> (дата обращения 02.07.2025)

Искусственный интеллект (мировой рынок). [Электронный ресурс]. — URL: [https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_\(мировой_рынок\)](https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_(мировой_рынок)) (дата обращения 02.07.2025).

Количественная оценка экономических выгод от ИИ-технологий в финансовой кибербезопасности представлена в таблице 4, демонстрирующей потенциальные источники экономической ценности и методы их измерения.

Таблица 4

Экономические выгоды от ИИ-технологий в финансовой информационной безопасности

Тип выгод	Источники стоимости	Методы оценки	Временной горизонт
Прямые операционные	Предотвращение потерь от инцидентов	Анализ исторических данных, стресс-тестирование	1–3 года
Снижение затрат	Автоматизация процессов мониторинга	Сравнение до/после, бенчмаркинг	6 месяцев — 2 года
Повышение эффективности	Ускорение выявления угроз	Метрики производительности SOC	3–12 месяцев
Соответствие требованиям	Снижение штрафов и санкций	Анализ регулятивных рисков	1–5 лет
Стратегические	Конкурентные преимущества	Анализ рыночной позиции	2–7 лет

Составлено автором на основе анализа материалов⁷

Особую важность приобретает анализ долгосрочных стратегических эффектов от внедрения ИИ-технологий, которые могут превышать прямые операционные выгоды. Согласно международным исследованиям, к 2030 году экономический эффект от внедрения искусственного интеллекта в финансовом секторе Северной Америки может достигнуть 79 млрд, а в Азиатско-Тихоокеанском регионе — 50,6 млрд.⁸



Рисунок 1. Компонентная структура интегральной модели экономической оценки ИИ-технологий в финансовой информационной безопасности (составлено автором на основе [14])

⁷ Искусственный интеллект может повысить эффективность рынков и их волатильность. [Электронный ресурс]. — URL: <https://www.imf.org/ru/Blogs/Articles/2024/10/15/artificial-intelligence-can-make-markets-more-efficient-and-more-volatile> (дата обращения 02.07.2025).

Отзвук ИИ в сфере финансов. [Электронный ресурс]. — URL: <https://www.imf.org/ru/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns> (дата обращения 02.07.2025).

⁸ Искусственный интеллект в банках. [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках (дата обращения 02.07.2025).

Разработанная автором интегральная модель экономической оценки ИИ-технологий в финансовой информационной безопасности основывается на четырехкомпонентном подходе, учитывающем различные аспекты создания стоимости. Компонентная структура интегральной модели экономической оценки представлена на рисунке 1.

Первый компонент модели включает комплексный анализ затрат, охватывающий капитальные инвестиции в технологическую инфраструктуру, операционные расходы на поддержание и развитие ИИ-систем, а также альтернативные издержки, связанные с отвлечением ресурсов от других проектов. Второй компонент фокусируется на количественной оценке прямых экономических выгод, включая предотвращенные потери от киберинцидентов, сокращение операционных затрат благодаря автоматизации процессов и повышение эффективности работы служб информационной безопасности.

Третий компонент модели учитывает косвенные эффекты, которые часто недооцениваются при традиционном анализе ROI, включая репутационные эффекты от повышения уровня защищенности, улучшение качества бизнес-процессов благодаря встроенным механизмам безопасности и ускорение инновационных процессов за счет снижения рисков. Четвертый компонент охватывает стратегические преимущества, включая формирование конкурентных преимуществ на рынке финансовых услуг, создание технологического задела для будущих инноваций и опционную стоимость от возможности масштабирования решений на другие области деятельности.

Практическое применение интегральной модели требует адаптации к специфике конкретной финансовой организации и учета отраслевых особенностей. Для крупных банков с обширной клиентской базой и сложной ИТ-инфраструктурой экономическая эффективность ИИ-технологий может быть особенно высокой благодаря эффекту масштаба. Согласно исследованиям, чем больше договоров и операций в организации, тем выше экономическая эффективность внедрения ИИ-систем, при чем окупаемость может составлять менее двух лет при правильном планировании проекта.⁹

Важным аспектом экономической оценки является учет регулятивных требований и их влияния на экономическую эффективность ИИ-проектов. Банк России активно развивает нормативную базу в области информационной безопасности, при чем за 2024 год было инициировано делегирование 1 335 фишинговых доменов, направлено на блокировку более 170 тысяч мошеннических телефонных номеров, что свидетельствует о масштабах киберугроз и необходимости инвестиций в современные системы защиты.¹⁰

Современные тенденции развития экономической оценки ИИ-технологий характеризуются переходом от изолированного анализа отдельных проектов к интегрированному подходу, учитывающему синергетические эффекты от комплексного внедрения ИИ-решений в различных областях деятельности финансовых организаций. Согласно прогнозам, глобальные затраты банков на системы генеративного ИИ составят около 6 млрд в 2024 году и могут достигнуть 85 млрд к 2030 году, что представляет рост более чем в 1 300 %.¹¹

⁹ Как рассчитать эффективность внедрения ИИ-решений для проверки документов. [Электронный ресурс]. — URL: <https://www.advgazeta.ru/mneniya/kak-rasschitat-effektivnost-vnedreniya-ii-resheniy-dlya-proverki-dokumentov/> (дата обращения 02.07.2025).

¹⁰ Информационная безопасность. [Электронный ресурс]. — URL: https://cbr.ru/information_security/ (дата обращения 02.07.2025).

¹¹ Искусственный интеллект в банках. [Электронный ресурс]. — URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках (дата обращения 02.07.2025).

Многофакторная модель экономической эффективности ИИ-технологий в финансовой кибербезопасности представлена в таблице 5, демонстрирующей взаимосвязи между ключевыми факторами и экономическими результатами.

Таблица 5

**Факторы экономической эффективности
ИИ-технологий в финансовой кибербезопасности**

Группа факторов	Ключевые переменные	Влияние на эффективность	Метрики оценки
Масштабные	Объем обрабатываемых данных, количество пользователей	Положительное (эффект масштаба)	ROI, NPV на единицу данных
Технологические	Уровень зрелости ИИ-алгоритмов, качество интеграции	Сильное положительное	Точность моделей, время отклика
Организационные	Готовность персонала, культура инноваций	Критическое для успеха	Скорость внедрения, пользовательская адаптация
Регулятивные	Требования надзорных органов, стандарты отрасли	Положительное через снижение рисков	Соответствие требованиям, избежание штрафов
Рыночные	Конкурентная среда, ожидания клиентов	Стратегическое влияние	Рыночная доля, клиентская лояльность

Составлено автором на основе анализа материалов¹²

Анализ факторов показывает, что экономическая эффективность ИИ-технологий в финансовой информационной безопасности определяется комплексным взаимодействием технологических, организационных и рыночных факторов. Особенно важным является фактор готовности организации к изменениям, поскольку даже самые передовые технологические решения могут не принести ожидаемого экономического эффекта при недостаточной подготовке персонала и организационных процессов.

Современные исследования подтверждают высокую экономическую эффективность внедрения ИИ в различных отраслях российской экономики. Согласно данным, экономический эффект от внедрения искусственного интеллекта в компании «Норникель» достиг \$100 млн по итогам 2023 года, а в Магнитогорском металлургическом комбинате экономический эффект превысил 4,5 млрд рублей.¹³ Данные примеры демонстрируют потенциал ИИ-технологий для создания значительной экономической стоимости при правильном планировании и реализации проектов.

Выводы

Теоретический анализ эволюции научных подходов к экономической оценке инвестиций в информационную безопасность и ИИ-технологии выявил последовательное развитие методологических принципов от классических моделей анализа рисков до современных интегративных концепций. Установлена трансформация понимания экономической ценности технологических инвестиций от узкого фокуса на прямые затраты и выгоды к комплексному анализу стратегических и репутационных эффектов. Определена ведущая роль теории экономики информации в формировании современных подходов к оценке ИИ-технологий, классических методов инвестиционного анализа в развитии количественных

¹² Искусственный интеллект завоевывает бизнес. [Электронный ресурс]. — URL: <https://cipr.ru/izdanie-2025/iskusstvennyj-intellekt-zavoevyvaet-biznes/> (дата обращения 02.07.2025).

Как искусственный интеллект меняет рынок финансовых услуг. [Электронный ресурс]. — URL: <https://www.vedomosti.ru/partner/articles/2024/10/16/1068013-iskusstvennii-intellekt-menyaet> (дата обращения 02.07.2025).

¹³ Искусственный интеллект завоевывает бизнес. [Электронный ресурс]. — URL: <https://cipr.ru/izdanie-2025/iskusstvennyj-intellekt-zavoevyvaet-biznes/> (дата обращения 02.07.2025).

методов оценки, современной теории цифровых технологий в понимании сетевых эффектов и платформенной экономики.

Исследование методологических основ расчета экономической эффективности ИИ-решений в области защиты финансовой информации выявило многокомпонентную структуру затрат и выгод, требующую применения комплексных методов оценки. Обоснована необходимость учета не только прямых финансовых эффектов, но и косвенных влияний на операционную эффективность, репутацию и стратегическое позиционирование организации. Определены ключевые факторы экономической эффективности, включающие масштабные, технологические, организационные, регулятивные и рыночные переменные, влияющие на успешность ИИ-проектов в финансовой кибербезопасности.

Разработанная интегральная модель экономической оценки целесообразности внедрения ИИ-технологий в финансовую кибербезопасность представляет собой четырехкомпонентную систему, включающую анализ затрат, оценку прямых выгод, расчет косвенных эффектов и учет стратегических преимуществ. Обоснованы методологические принципы применения модели для различных типов финансовых организаций с учетом их специфики и стратегических целей. Установлена критическая важность учета эффекта масштаба, качества технологической интеграции и организационной готовности для достижения высокой экономической эффективности ИИ-проектов.

Проведенное исследование свидетельствует о высокой экономической целесообразности внедрения ИИ-технологий в системы защиты финансовой информации при условии комплексного подхода к планированию и реализации проектов. Разработанная методологическая модель представляет собой теоретически обоснованную систему, позволяющую финансовым организациям принимать обоснованные инвестиционные решения в области ИИ-технологий для информационной безопасности.

ЛИТЕРАТУРА

1. Авдийский, В.И. Финансово-экономическая безопасность экономических агентов / В.И. Авдийский, В.М. Безденежных, В.Е. Лихтенштейн [и др.] // Вестник Финансового университета. — 2015. — № 5(89). — С. 40–50. — EDN VBGRPT.
2. Бутенко, Е.Д. Искусственный интеллект в банках сегодня: опыт и перспективы / Е.Д. Бутенко — DOI 10.24891/df.25.2.230. // Дайджест-финансы. — 2020. — Т. 25, № 2(254). — С. 230–242 — EDN UUQUJV.
3. Бабукин, Г.М. Цифровизация и искусственный интеллект в банках: шаг в будущее / Г.М. Бабукин // Chronos: экономические науки. — 2021. — Т. 6, № 1(29). — С. 6–9. — EDN JNOJZE.
4. Ларина, О.И. Искусственный интеллект в банках: первые результаты, препятствия и риски / О.И. Ларина, С.С. Шкретанова — DOI 10.15688/re.volsu.2023.4.8. // Региональная экономика. Юг России. — 2023. — Т. 11, № 4. — С. 88–98 — EDN RDHKBG.
5. Живко, А.Б. Анализ российского и зарубежного опыта управления рисками в коммерческом банке / А.Б. Живко, Н.А. Проданова // Финансовые рынки и банки. — 2024. — № 9. — С. 114–120. — EDN KBXGDA.
6. Мазитова, З.Р. искусственный интеллект в банковской сфере / З.Р. Мазитова // Политика, экономика и инновации. — 2024. — № 1(54). — EDN TDLSGF.

7. Преображенская, А.С. Современное состояние и тенденции развития банковского сектора РФ в условиях цифровизации / А.С. Преображенская, М.М. Сорокина — DOI 10.51691/2500-3666_2022_5_2. // Вектор экономики. — 2022. — № 5(71) — EDN KASNUV.
8. Зиниша, О.С. Информационная безопасность в финансовой сфере / О.С. Зиниша, Е.А. Волошина — DOI 10.18411/trnio-07-2022-137. // Тенденции развития науки и образования. — 2022. — № 87-4. — С. 60–64 — EDN VUEXVB.
9. Шабанов, И.А. Информационная безопасность в финансовом секторе: вызовы, решения и влияние на качество финансовой отчетности / И.А. Шабанов — DOI 10.46845/2541-8254-2024-5(47)-7-7. // Вестник молодежной науки. — 2024. — № 5(47). — С. 7 — EDN RNRMIA.
10. Белоумцева, А.А. Финансовая безопасность: сущность и место в системе экономической безопасности предприятия / А.А. Белоумцева, Т.Е. Даниловских — DOI 10.17513/fr.43277. // Фундаментальные исследования. — 2022. — № 7. — С. 20–24 — EDN VPNYEE.
11. Юлдашев, Ю.Ж. Информационная безопасность в системе защиты национальных интересов Российской Федерации / Ю.Ж. Юлдашев // Коммуникология: электронный научный журнал. — 2020. — Т. 5, № 2. — С. 72–83. — EDN XHERWJ.
12. Балог, М.М. Защищённость информационного пространства как фактор экономической безопасности региона: инструментарий оценки / М.М. Балог, А.В. Бабкин — DOI 10.18721/IE.16304. // π-Economy. — 2023. — Т. 16, № 3. — С. 63–79 — EDN HSJQHG.
13. Полякова, Т.А. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) / Т.А. Полякова, А.В. Минбалева, Н.В. Кроткова — DOI 10.31857/S102694520017761-8. // Государство и право. — 2021. — № 12. — С. 97–108 — EDN MXNVHZ.
14. Ивановский, Б.Г. Экономические эффекты от внедрения технологий «искусственного интеллекта» / Б.Г. Ивановский — DOI 10.31249/snsn/2021.02.01. / Социальные новации и социальные науки. — 2021. — № 2(4). — С. 8–25 — EDN VISNBS.

Shushokov Islam Aslanovich

Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: prilipko1337@mail.ru

Economic feasibility of implementing artificial intelligence technologies into financial information security systems

Abstract. Modern realities of the digital economy are characterized by exponential growth in financial data volumes and increasing complexity of cyber threats, requiring financial organizations to develop innovative approaches to ensuring information security. This study is devoted to a comprehensive analysis of the economic efficiency of implementing artificial intelligence technologies into financial information security systems through the prism of theoretical concepts of information security economics and empirical data from Russian and foreign experience. The article considers the possibilities of optimizing the cost-benefit ratio when using AI technologies to prevent financial losses from cyber incidents, improve the efficiency of threat monitoring and analysis processes, and automate information security audit procedures. The article analyzes the evolution of scientific approaches to the economic evaluation of investments in information security from classical risk analysis models to modern integrative concepts that take into account strategic and reputational factors. Particular attention is paid to the theoretical substantiation of the methodological principles for calculating the economic efficiency of AI solutions in the context of financial information protection, including return on investment assessment models, total cost of ownership analysis, and methods for predicting prevented damage. The study demonstrates that the economic feasibility of implementing AI technologies in financial cybersecurity is determined by a set of factors, including the scale of the data processed, the complexity of threats, regulatory requirements, and the strategic goals of the organization. The results indicate the need to develop integrated approaches to the economic evaluation of AI projects in the field of financial security, taking into account both direct financial benefits and indirect effects in the form of increased operational efficiency, stronger reputation, and compliance with regulatory requirements. The methodological model of economic evaluation developed by the author includes four main components: analysis of the costs of implementing and operating AI systems, assessment of direct economic benefits from incident prevention, calculation of indirect effects from increased operational efficiency, and consideration of strategic competitive advantages. The scientific novelty of the study lies in the creation of a theoretically sound concept for the economic evaluation of AI technologies in financial cybersecurity, which opens up new opportunities for making informed investment decisions in the field of financial information protection and contributes to the development of the theory of information security economics.

Keywords: artificial intelligence; financial information security; economic efficiency; digital economy; cyber risks; return on investment; technological innovation; financial technologies; security economics