CC BY 4.0

УДК 519.86
DOI: http://dx.doi.org/10.21686/2500-3925-2025-4-36-51

А.А. Брызгалов

Российский экономический университет им. Г.В. Плеханова, Москва, Россия

Экономико-математическое моделирование рисков в сервисной бизнес-модели сетевого предприятия

Целью *работы является разработка экономико-математической модели оценки рисков в сервисной бизнес-модели сетевого предприятия, способной формализовать влияние разнообразных факторов риска на устойчивость сетевой структуры и вырабатывать эффективные стратегии управления ими.*
Материалы и методы. *В работе применены стохастические методы, методы оптимизации, теория графов, системная динамика. Алгоритм моделирования включает этапы идентификации рисков, формализации параметров, анализа каскадных эффектов, оценки сетевой структуры и оптимизации стратегии управления. В качестве эмпирической базы использован пример IoT-платформы MindSphere и экосистемы её участников.*
Результаты. *Разработан комплексный подход к количественной оценке рисков в цифровых экосистемах на основе каскадного анализа, оценки центральности узлов экосистемы и моделирования ущерба. Комплексный подход к количественной оценке рисков предусматривает интеграцию методов, позволяющих не только измерить вероятность и потенциальный ущерб отдельных угроз, но и учесть их взаимосвязи, динамику развития и влияние на структуру сервисной бизнес-модели сетевого предприятия. Такой подход обеспечивает не только расчет ожидаемых потерь, но и выявление критических точек системы, разработку превентивных мер и визуализацию результатов для принятия обоснованных решений, что особенно важно для сложной экосистемы, где риски усиливаются за счет взаимозависимости ее участников.*
Заключение. *Разработанная модель позволяет количественно оценивать взаимосвязанные риски в сервисных бизнес-моделях, учитывать сетевую взаимосвязь рисков и структурные уязвимости экосистем. Это обеспечивает обоснованное принятие решений при управлении устойчивостью сетевой структуры. Результаты имеют практическое значение для промышленности, активно внедряющей IoT и облачные решения.*

Ключевые слова: *экономико-математическое моделирование; сервисные бизнес-модели; сетевые предприятия; управление рисками; каскадные эффекты; системная динамика; теория графов; центральность узлов; метод Монте-Карло; стохастическая оптимизация; устойчивость сети; цифровая экосистема; IoT-платформы*

Alexey A. Bryzgalov

Plekhanov Russian University of Economics, Moscow, Russia

Economic and Mathematical Modeling of Risks in the Service Business Model of a Network Enterprise

The aim *of the research is to develop an economic and mathematical model of risk assessment in the service business model of a network enterprise, capable of formalizing the impact of various risk factors on the stability of the network structure and developing effective strategies for managing them.*
Materials and methods. *The paper uses stochastic methods, optimization methods, graph theory, and system dynamics. The modeling algorithm includes the stages of risk identification, parameter formalization, cascade effects analysis, network structure assessment, and management strategy optimization. The example of the MindSphere IoT-platform and the ecosystem of its participants is used as an empirical base.*
Results. *A comprehensive approach to quantitative risk assessment in digital ecosystems has been developed based on cascade analysis, assessment of the centrality of ecosystem nodes, and damage modeling. A comprehensive approach to quantitative risk assessment involves the integration of methods that allow not only to measure the probability and potential damage of individual threats, but also consider their interrelationships, development dynamics and impact on the structure of the service business model of a network enterprise. This approach provides not only the calculation of expected losses, but also the identification of critical points of the system, the development of preventive measures and visualization of the results for informed decision-making, which is especially important for a complex ecosystem where risks are increased due to the interdependence of its participants.*
Conclusion. *The developed model allows quantifying interrelated risks in service business models, taking into account the network interconnection of risks and structural vulnerabilities of ecosystems. This ensures informed decision-making when managing the stability of the network structure. The results are of practical importance for the industry, which is actively implementing IoT and cloud solutions.*

Keywords: *economic and mathematical modeling; service business models; network enterprises; risk management; cascading effects; system dynamics; graph theory; node centrality; Monte Carlo method; stochastic optimization; network stability; digital ecosystem; IoT platforms.*

Введение

Современные сервисные бизнес-модели сетевых предприятий, особенно в условиях цифровой экономики, сталкиваются с беспрецедентным уровнем неопределённости и усложнённой природой рисков [1]. В отличие от традиционных линейных бизнес-структур, где угрозы зачастую локализованы и поддаются классическим методам управления, сервисные модели формируются на принципах сетевого взаимодействия, что радикально меняет характер и динамику рисков.

Сервисная бизнес-модель – это способ создания и доставки ценности, основанный преимущественно на услугах, предоставляемых цифровыми платформами. Она ориентирована не на владение активами, а на координацию их использования в рамках экосистемы. Классические работы Остервальдера А. и Пинье И. определили базовые компоненты бизнес-моделей, однако в контексте сетевых предприятий акцент смещается на взаимодействие множества участников и совместное создание ценности [2] Исследования *Li* и др. п.одчеркивают, что цифровые платформы трансформируют цепочки создания стоимости, формируя распределенные системы с высокой взаимозависимостью партнеров [3]. Её ключевыми характеристиками являются:

1. Центральная роль цифровой платформы, которая выступает инфраструктурной основой для обмена данными, услугами и ресурсами (например, IoT-платформа MindSphere).

2. Мультиагентность — участие разнородных субъектов (разработчики, поставщики оборудования, клиенты, интеграторы), каждый из которых вносит вклад в формирование конечной ценности.

3. Взаимозависимость участников сетевой структуры, в которой сбои или риски одного элемента сети могут вызвать каскадные последствия для всей системы.

Специфика сервисной ориентации сетевого предприятия проявляется в том, что ключевым продуктом выступают не материальные товары, а цифровые услуги и решения, такие как прогнозная аналитика, удаленный мониторинг оборудования или оптимизация производственных процессов.

Сервисные бизнес-модели сетевого предприятия функционируют в условиях высокой динамики, где ключевую роль играют нематериальные активы, распределённые взаимодействия и технологическая изменчивость. Работы Паркера и др. подробно рассматривают природу сетевых эффектов и стратегии монетизации платформенных моделей.[4] Успех подобных моделей, как показано в [5], зависит от интеграции оборудования, данных и приложений, что, в свою очередь, создаёт новые уязвимости, связанные с координацией и управлением взаимодействием. Проблемы организации цифровых платформ и технологической интеграции рассмотрены в отечественных источниках [6], [7], где подчёркивается значимость сочетания IoT-решений и облачных сервисов.

Ключевая особенность рисков в таких моделях — их системная взаимозависимость. Угрозы усиливаются за счёт сложной сетевой архитектуры взаимодействий: сбой одного компонента может вызвать каскадные эффекты [8]. Помимо технических аспектов, значимыми становятся регуляторные и поведенческие риски. В отличие от традиционных подходов (COSO ERM, ISO 31000) [9], которые фокусируются на внутренних угрозах, платформенные структуры сталкиваются с внешними факторами на стыке взаимодействий. Исследования Л.В. Санковой и Ф.И. Мирзабалаевой, предлагают классификацию рисков в платформенной экономике (технические, рыночные, регуляторные), а Радайкин А.Г. и др. выделяют «риски экосистем», включая зависимость от сторонних API и облачных решений [10], [11].

Для IoT-платформ работы [12], [13], [14] подчёркивают значимость киберрисков, особенно связанных с передачей данных между устройствами и облачными платформами. Однако вопросы синергии различных типов рисков – технических, регуляторных, операционных – остаются недостаточно изученными. В работе [15] анализируются финансовые и операционные угрозы, однако многие подходы рассматривают изолированные риски, игнорируя их каскадные последствия, например: как сбой облачного компонента приводит к кибератакам, а те – к штрафным санкциям за утечку персональных данных.

Кроме того, в такой среде риски обладают высокой латентностью: они скрыты в архитектуре платформы, зависимостях от поставщиков и пользовательском поведении. В условиях высокой скорости изменений классические модели оценки (например, VaR, [16]) теряют эффективность, поскольку не учитывают сетевые и нелинейные эффекты. Это усиливает потребность в современных методах анализа, способных отразить динамику, распределённость и неопределённость угроз.

В качестве ответа на эти вызовы используется адаптированный подход системной динамики [17], позволяющие смоделировать развитие рисков во времени и учитывать обратные связи между событиями. Сетевой анализ, базирующийся на теории графов [18], применяется для выявления узлов с наибольшей уязвимо-

стью и оценки устойчивости платформ. В частности, работа [19] предлагает модель анализа цифровой платформы на основе центральности узлов, однако её применимость к многоагентным сервисным моделям, где задействованы интеграторы, провайдеры и заказчики, требует дополнительного изучения [20].

Российские исследования [21], [22] предлагают использовать многокритериальный анализ для оценки и выбора стратегий управления рисками. Однако их адаптация к реальности IoT-экосистем, где технические сбои сочетаются с нормативными ограничениями, пока остаётся открытым направлением для исследований.

Проведенный анализ исследований обуславливает потребность в разработке комплексного подхода моделирования оценки рисков в сервисной бизнес-модели сетевого предприятия, учитывающего: сетевые взаимосвязи между участниками; эволюцию и динамику рисков; стохастическую природу цифровых экосистем; интеграцию различных типов угроз в рамках единой модели.

Исследование автора направлено на экономико-математическом моделировании оценки рисков, адаптированной к условиям сервисных бизнес-моделей сетевых предприятий. Она основывается на причинно-следственном анализе рисков и применяет набор взаимодополняющих методов: сетевой анализ для выявления структурных уязвимостей, системную динамику для оценки развития рисков во времени и вероятностные методы для анализа неопределённости. Такой подход позволит перейти от реактивного управления к проактивной стратегии, обеспечивающей устойчивость и адаптивность бизнеса в цифровой среде.

Обоснование выбора методов и последовательности алгоритма экономико-математического моделирования рисков

Пусть сервисное сетевое предприятие функционирует в условиях неопределенности, где различные виды рисков могут проявляться с определенной вероятностью и вызывать ущерб различной степени. Требуется:

1. Разработать систему количественной оценки рисков.

2. Определить зависимость между различными видами рисков.

3. Разработать оптимизационную модель управления рисками, минимизирующую суммарные потери.

Модель должна учитывать как отдельные риски, так и их совокупное влияние на устойчивость сервисной бизнес-модели.

Для количественной оценки рисков сервисной бизнес-модели сетевого предприятия необходим выбор адекватного математического аппарата, который позволит учитывать вероятностную природу рисков, их взаимосвязь, а также прогнозировать возможные последствия их реализации.

Экономико-математическое моделирование рисков в сетевых бизнес-моделях требует системного подхода, учитывающего их распределенную природу, взаимозависимость участников и нелинейность во времени возникающих угроз. Предлагаемый алгоритм объединяет методы, которые последовательно решают задачи моделирования оценки рисков, обеспечивая комплексный анализ даже в условиях высокой неопределенности. Ниже представлена методика моделирования оценки рисков, которая отражает естественный путь анализа, включая логику перехода от идентификации угроз к их количественной оценке и практическому управлению:

1. Идентификация ключевых рисков → Без нее модель не имеет предмета анализа.

2. Формализация параметров рисков → Превращает качественные угрозы в количественные параметры, делая их пригодными для математического анализа.

3. Построение матрицы влияния → Определяет причинно-следственные связи между рисками, что необходимо для последующего анализа каскадных эффектов.

4. Расчет каскадных эффектов → Ядро модели, объясняющее механизм усиления ущерба в сетевых структурах.

5. Динамическое моделирование роста ущерба → Дополняет анализ каскадов временным измерением, показывая, как ущерб накапливается и распространяется в системе.

6. Анализ центральности узлов → Выявляет ключевые узлы сети, где управление рисками дает максимальный эффект.

7. Вероятностная оценка ущерба методом Монте-Карло → Добавляет в анализ стохастичность, отражающую реальную неопределенность.

8. Оптимизация управления рисками → Превращает результаты анализа в практические управленческие решения.

Каждый метод дополняет предыдущий: матрица влияния питает графы каскадов, системная динамика уточняет расчеты Монте-Карло, а теория графов задает приоритеты для оптимизации. Такой синтез методов позволяет преодолеть ограничения классических подходов и предложить решение, адекватное сложности сетевых сервисных бизнес-моделей.

Первый этап - Последовательность начинается с идентификации ключевых рисков, поскольку без четкого понимания угроз, специфичных для

сетевой структуры, дальнейшее моделирование теряет смысл. В данном случае важно выделить не просто отдельные риски, а те из них, которые способны инициировать цепные реакции [23]. Например, в экосистеме могут быть критичны риски сбоев облачных провайдеров и кибератак, так как они затрагивают всех участников. Этот этап опирается на экспертные интервью, исторические данные и мозговые штурмы, что позволяет избежать субъективности и сосредоточиться на реально значимых угрозах. В результате идентификации ключевых рисков формируется список рисков $R = \{r_1, r_2, ..., r_n\}$.

Второй этап — Формализация параметров рисков – переводит качественные оценки в количественные метрики: вероятность, ущерб, время восстановления. Каждый идентифицированный риск описывается кортежем – $r_j = \langle P_j, U_j, T_j \rangle$. Для того, чтобы получить значение элементов по каждому риску необходимо определить источники данных, а также рассчитать по формуле значение показателя. Без этого невозможно перейти к математическому моделированию. Предложенные варианты источников данных и формула расчета параметров рисков представлены в таблице 1 [14].

Третий этап – Построение матрицы влияния. Для оценки взаимосвязей между рисками в сетевой сервисной бизнес-модели применяется матрица влияния, элементы которой представляют собой коэффициенты c_{jk}, отражающие степень воздействия риска r_j на риск r_k. Например, сбой облачного провайдера может повысить вероятность кибератаки на API платформы. Таким образом, этап становится ключевым для анализа каскадных эффектов. Коэффициенты c_{jk} принимают значения в диапазоне [0,1], где: $c_{jk} = 0$ означает отсутствие влияния (риски независимы), $c_{jk} = 1$ соответствует полной зависимости (реализация r_j с необходимостью влечёт наступление r_k).

Таблица 1 / Table 1

Источники данных и формулы для количественной оценки

Data sources and formulas for quantification

Параметр	Источник данных
P_j – вероятность осуществления риска	○ Статистика прошлых инцидентов. ○ Экспертные оценки. ○ Отраслевые отчеты (Gartner, McKinsey и др.).
U_j – ущерб от осуществления риска	○ Финансовая отчетность компаний (потери клиентов, штрафы). ○ Оценка операционных потерь. ○ Репутационные издержки.
T_j – время воздействия риска	○ Среднее время восстановления (MTTR) из отчетов инцидентов. ○ SLA участников сетевого предприятия. ○ Экспертные оценки интеграторов.

При наличии достаточного объема наблюдений коэффициенты c_{jk} могут интерпретироваться как эмпирические оценки условных вероятностей $P(r_k|r_j)$. Это приближает модель к формализму байесовских сетей, в которых узлы представляют вероятностные события (риски), а направленные связи отражают условные зависимости между ними. Таким образом, даже в условиях ограниченной информации модель использует байесовскую логику, в рамках которой априорная вероятность одного события корректируется с учётом наступления другого [24].

Коэффициенты c_{jk} могут быть определены одним из следующих способов:

1. На основе исторических данных как отношение Qs — число зафиксированных случаев наступления риска r_k после риска r_j, к Qv — общее количество случаев реализации риска r_j. Такой подход обеспечивает наибольшую объективность, но требует обширной базы наблюдаемых инцидентов.

2. С использованием статистического анализа применяя регрессионные или корреляционные модели, выявляющих статистически значимые связи между рисками. Это позволяет учесть скрытые зависимости и уточнить оценки влияния.

3. Экспертная оценка, где итоговое значение определяется как среднее арифметическое оценок всех экспертов:

Включение матрицы влияния в модель принципиально важно, поскольку без учёта взаимосвязей между рисками невозможно корректно оценить каскадные эффекты, что может привести к существенной недооценке потенциальных угроз для сетевого предприятия.

Четвертый этап – Расчет каскадных эффектов. Следующим этапом анализа является определение цепной реакции рисков в рамках каскадной структуры. В такой структуре узлы представляют отдельные риски, а направленные рёбра – связи между ними, определяемые коэффициентами влияния c_{jk}. На этой основе производится расчёт вероятности реализации каскада и возможного ущерба.

Используемая структура расчёта аналогична байесовской сети: каждый элемент цепи зависит от предыдущего, и общая вероятность каскада приближённо вычисляется через произведение условных зависимостей между рисками. Хотя точные значения $P(r_k|r_j)$ заменить невозможно без полной статистики, коэффициенты c_{jk} позволяют приближённо использовать формулу произведения Байеса для оценки вероятности цепочки:

$$P_{\text{каскад}} = P_1 \cdot \prod_{i=1}^{n-1} c_{i,i+1}. \qquad (1)$$

где P_1 – базовая вероятность начального риска (r_1); $c_{i,i+1}$ –

коэффициент влияния последовательными рисками в каскаде. Ущерб от каскада рассчитывается как:

$$U_{\text{каскад}} = \sum_{i=1}^{n}\left(U_i \cdot T_i \cdot \prod_{j=1}^{i-1} c_{j,j+1}\right), \quad (2)$$

где U_i – потенциальный ущерб от риска r_i; T_i – продолжительность воздействия риска r_i; $c_{j,j+1}$ – коэффициент влияния риска r_j на ущерб r_{j+1}.

Этот этап особенно важен для сетевых моделей, где центральные узлы (например, облачные провайдеры) обладают максимальной разрушительной силой, а также, даже маловероятные сценарии могут привести к катастрофическим потерям.

Пятый этап – Динамическое моделирование роста ущерба – учитывает временное измерение через системную динамику, моделирующую сложные системы с обратными связями, задержками и нелинейностями с помощью дифференциальных уравнений. Для сетевых предприятий с каскадными рисками метод позволяет:

- Учесть взаимозависимость участников.
- Смоделировать эмерджентные эффекты, возникающие из-за сетевой структуры.
- Прогнозировать ущерб в условиях неопределенности и стохастических воздействий.

Дифференциальное уравнение описывает баланс между накоплением ущерба и его снижением:

$$\frac{dU}{dt} = \alpha \times S(t) - \beta \times U(t), \quad (3)$$

где α – коэффициент роста ущерба, отражающий долю потенциальных потерь; β – коэффициент восстановления, характеризующий скорость устранения последствий; $U(t)$ – совокупный ущерб в момент времени t; $S(t)$ – интенсивность каскада рисков, зависящая от времени и структуры взаимодействий.

Интенсивность каскадов рисков $S(t) = P_{\text{каскад}} \cdot I(t)$, где $P_{\text{каскад}}$ – вероятность каскада рисков; $I(t)$ – функция усиления ущерба, описывающая нелинейные эффекты (линейный, экспоненциальный или сигмоидный рост) и калибруемая эмпирическими данными или экспертными оценками.

Данные для α и β могут быть получены из экспертных оценок или исторических данных. α – отношение фактического ущерба к максимально возможному, а β – обратное среднее значение времени восстановления или отношение скорости восстановления к текущему ущербу.

Накопленный ущерб на различных фазах каскада рассчитывается методом Эйлера. Для обеспечения непрерывности ущерба между фазами начальное значение ущерба для текущей фазы берется как конечное значение предыдущей фазы. При расчете динамики внутри фазы используется прошедшее время ($t - t_0$), что позволяет применять фазово-зависимые параметры и функции, сохраняя общий временной масштаб.

Шестой этап – анализ центральности узлов. На этом этапе применяется теория графов для анализа устойчивости и уязвимостей сетевых бизнес-моделей. Устойчивость здесь – это способность системы сохранять функциональность при сбоях или атаках, и зависит не только от характеристик узлов, но и от их позиции в структуре взаимодействий.

Сетевое предприятие представляется ориентированным графом $G = (V, E)$, где:

- $V = \{v_1, v_2, ..., v_n\}$ – узлы (участники: AWS, интеграторы, клиенты и т.д.),
- $E = \{(v_i, v_j) | v_i \to v_j\}$ – ребра, отражающие направленные взаимодействия.

Для оценки значимости узлов рассчитываются следующие метрики центральности:

Центральность по посредничеству $C_B(v)$: показывает, как часто узел участвует в кратчайших путях между другими. Узлы с высокой C_B контролируют потоки данных и рисков. Например, интеграторы, связывающие разработчиков и клиентов.

Степень центральности $C_D(v)$: число прямых связей узла. Высокая степень говорит о сильной вовлечённости. Например, облачный провайдер, взаимодействующий со всеми участниками.

Центральность по близости $C_C(v)$: обратная сумма расстояний до других узлов. Характеризует скорость распространения рисков. Например, клиенты имеют низкую C_C, так как зависят от цепочек взаимодействий.

Центральность по собственному вектору $C_E(v)$: учитывает влияние не только самого узла, но и его связей с другими значимыми участниками. Например, разработчик платформы, связанный с ключевыми узлами.

Для оценки вклада узла в общий ущерб используется:

$$U_{\text{вклад}}(v) = \frac{C_B(v)}{\sum_{i=1}^{n} C_B(v_i)} \cdot U_{\text{каскад}}, \quad (4)$$

чем выше C_B, тем больше ущерб от его отказа.

Кроме того, **устойчивость всей сети** можно оценить через модифицированный показатель Фримена:

$$R = 1 - \frac{\sum_{i=1}^{n} C_B(v_i)^2}{n}, \quad (5)$$

где n – число узлов. Чем выше разбалансированность в значениях центральности, тем ниже устойчивость.

Использование этих метрик позволяет выявить критические узлы и обеспечить адресную защиту ключевых компонентов сетевого предприятия.

Седьмой этап – вероятностная оценка ущерба методом Монте-Карло – учитывает стохастическую природу рисков.

Генерация тысяч сценариев с разными комбинациями вероятностей и корреляций позволяет получить распределение ущерба, а не точечную оценку. В контексте сетевых предприятий этот метод особенно эффективен для анализа каскадных рисков, где нелинейные зависимости и временные задержки усложняют детерминированные расчеты [25]. В результате по формуле (7) оценивается средний ожидаемый ущерб при генерации каскадных сценариев.

Алгоритм моделирования

1. *Генерация случайных чисел:*

Для каждого риска r_j генерируется случайное число $rand_j \in [0, 1]$. Реализация риска происходит, если $rand_j < P_j$.

2. *Учет взаимозависимостей:*

Если реализован риск r_1, вероятность r_2 увеличивается до $P_2' = P_2 + c_{12} \cdot (1 - P_2)$. c_{12} из матрицы влияния. Аналогично для r_3: $P'_3 = P_3 + c_{23} \cdot (1 - P_3)$ при реализации r_2.

3. *Расчет ущерба для каждого сценария:*

$$U_i = U_1 \cdot T_1 \cdot I_1 + U_2 \cdot I_2 + U_3 \cdot I_3 \quad (6)$$

где U_i – ущерб в i-м сценарии, $I_j = 1$, если риск r_j реализован, иначе 0.

4. *Повторение:*

Процедура выполняется $N = 10\,000$ раз для получения распределения ущерба.

5. Статистический анализ результатов:

Средний ожидаемый ущерб рассчитывается как:

$$E[U] = \frac{1}{N}\sum_{i=1}^{N} U_i, \quad (7)$$

Доверительный интервал (95%):

$$E[U] \pm 1.96 \frac{\sigma_U}{\sqrt{N}}, \quad (8)$$

где σ_U – стандартное отклонение ущерба

Распределение ущерба отражается на основе гистограммы и расчет вероятности превышения пороговых значений

Восьмой этап – Оптимизация управления рисками в сетевых предприятиях решается как задача стохастического программирования, минимизирующая ожидаемый ущерб при ограничениях. Вектор x – меры по снижению рисков, ξ – случайные параметры (вероятности, коэффициенты). Целевая функция отражает ожидаемый ущерб с учетом затрат на меры:

$$\min_x E\left[U(x,\xi)\right] + \lambda \cdot \mathrm{Cost}(x), \quad (9)$$

При ограничениях:

$$\begin{cases} \sum_{i=1}^{m} x_i \cdot \mathrm{cost}(x_i) \le B, \\ P_j(x) \le P_j^{допуст}, \forall j, \\ c_{jk}(x) \le c_{jk}^{допуст}, \forall j,k, \end{cases} \quad (10)$$

где $E[U(x)]$ – ожидаемый ущерб при выбранных мерах x; $\mathrm{cost}(x)$ – затраты на реализацию мер x; λ – коэффициент, балансирующий между ущербом и затратами (настраивается); $x = (x_1, x_2, ..., x_m)$ – вектор управляющих переменных (мер); j, k – индексы рисков; i – индекс управляющих мер; $x_i \in \{0, 1\}$ – бинарная управляющая переменная: $x_i = 1$, если мера i применяется, $x_i = 0$, если мера i не применяется; B – общий бюджет на управление рисками; $P_j(x)$ – вероятность реализации риска j после применения мер x; $c_{jk}(x)$ – коэффициент влияния риска j на риск k после применения мер x; $c_{jk}^{\text{допуст}}$; $P_j^{\text{допуст}}$ – допустимые значения.

Коэффициент λ, балансирующий между ущербом и затратами получается несколькими способами:

- Анализом чувствительности (по кривой «затраты – эффективность»),
- Отношением ущерба к бюджету (например, $\lambda = 2$ при ущербе \$10 млн и бюджете \$5 млн),
- Многокритериальной оптимизацией (по Парето-фронту),
- Экспертной оценкой (по готовности бизнеса платить за снижение риска на 1%).

Для решения задачи выбора оптимальных мер управления рисками в условиях неопределенности предлагается комбинированный подход, объединяющий метод ветвей и границ с вероятностным моделированием методом Монте-Карло. Алгоритм реализует последовательный перебор возможных комбинаций защитных мер с эффективным отсечением заведомо неоптимальных вариантов:

1. Инициализация: базовый сценарий ($x = 0$), расчет $E[U(0)]$ по N сценариям Монте-Карло с параметрами ξ.

2. Построение дерева решений:

○ Ветвление: добавление меры $x_i = 1$, актуализация ξ.

○ Пересчет ущерба по сценариям S'.

○ Оценка границ: нижняя (L) — $\min_{s \in S'} U_S(x)$, верхняя (U) — $\max_{s \in S'} U_S(x)$.

Отсечение ветвей: исключение узлов, где $L_{\text{текущий}} > U_{\text{лучший}}$.

Критерии остановки: исчерпание ветвей или достижение точности ϵ.

Метод сочетает перебор вариантов, вероятностную оценку и оптимизацию ресурсов, обеспечивая робастные решения для снижения ущерба в условиях неопределенности сетевых структур.

Предложенная методика экономико-математического моделирования оценки рисков возникла как ответ на необходимость учесть не только отдельные угрозы, но и их каскадные эффекты, а также адаптацию участников к меняющимся условиям. Его структура и методы выбраны исходя из специфики сетевых взаимодействий и практической применимости результатов.

Разработанный подход особенно важен для анализа сложных каскадных сценариев, характерных для сетевых бизнес-моделей. Чтобы продемонстрировать практическую

применимость предложенной последовательности моделирования оценки рисков, рассмотрим конкретный пример каскада рисков в сервисной бизнес-модели на IoT-платформе MindSphere, где реализуется цепочка: сбой облачного провайдера → кибератака через уязвимости API → регуляторные штрафы за нарушение GDPR.

Пример реализации методики для сетевого предприятия на IoT-платформе MindSphere

В качестве объекта исследования рассматривается сетевая бизнес-модель на базе промышленной IoT-платформы MindSphere, разработанной Siemens [26], [27]. Данное решение представляет собой облачную экосистему, объединяющую производителей оборудования, разработчиков приложений, интеграторов и промышленных предприятий для цифровизации производственных процессов.

Ключевые участники экосистемы включают: поставщиков оборудования (Bosch, Schneider Electric), обеспечивающих датчики и контроллеры; облачных провайдеров (AWS, Azure), предоставляющих инфраструктуру; разработчиков аналитических решений (SAP, C3 AI); интеграторов (Accenture, Capgemini), адаптирующих платформу под конкретные предприятия; и конечных клиентов (BMW, BASF), использующих данные для оптимизации производства. На рис. 1 показаны ключевые связи между компонентами экосистемы. Сплошные линии отражают потоки данных.

Функционирование системы строится на непрерывном потоке данных: оборудование собирает информацию о работе станков, которая передается в облако MindSphere, обрабатывается специализированными приложениями и преобразуется в аналитические отчеты

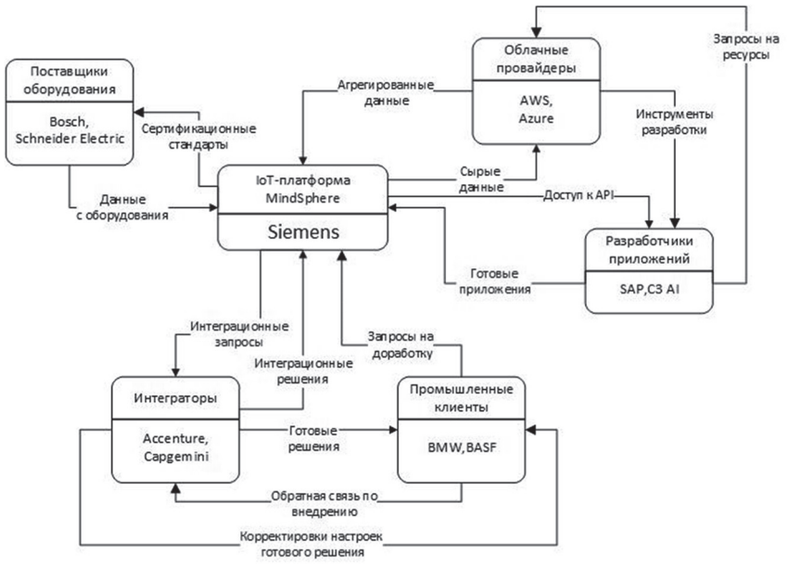

Рис. 1. Схема взаимодействия участников сервисной бизнес-модели на IoT-платформе MindSphere

Fig. 1. Interaction diagram of participants in the service business model on the MindSphere IoT-platform

для принятия решений. Особенность модели – высокая взаимозависимость участников [28], где сбой одного элемента (например, облачного провайдера) может нарушить работу всей цепочки.

Характерные особенности MindSphere – распределенная архитектура, стандартизированные интерфейсы и синергия участников – создают не только конкурентные преимущества, но и специфические уязвимости. В таких сложных экосистемах локальные сбои способны запускать цепные реакции, приводящие к значительным операционным и финансовым потерям.

Для демонстрации этого явления рассмотрим реалистичный каскадный сценарий в экосистеме MindSphere: от сбоя облачного провайдера до регуляторных штрафов, проанализировав его с помощью предложенной методики экономико-математического моделирования.

Начало цепочки: Сбой облачного провайдера (AWS). Предположим, из-за аварии в дата-центре AWS в регионе Франкфурт происходит масштабный сбой, длящийся 6 часов [29]. Поскольку MindSphere развернута на инфраструктуре AWS, платформа становится недоступной [30] для всех участников экосистемы: клиенты (например, заводы BMW) теряют доступ к данным с IoT-датчиков, интеграторы не могут настраивать системы, а разработчики приложений лишаются доступа к API. Операционные потери клиентов достигают $5 млн/час из-за простоя оборудования, не получающего аналитику в реальном времени.

Эскалация: Уязвимости API как следствие экстренного восстановления. Чтобы минимизировать время простоя, команда Siemens активирует резервные серверы в другом регионе, но в спешке не успевает провести полный аудит безопасности. Через 12 часов после восстановления работы хакеры эксплуатируют незакрытую уязвимость в API MindSphere (например, недостаточную аутентификацию запросов). [31] Злоумышленники получают доступ к данным 200 промышленных предприятий, включая конфиденциальные параметры производства и логины сотрудников. Ущерб

включает как прямые потери (кражу интеллектуальной собственности), так и репутационные риски: клиенты теряют доверие к платформе.

Кульминация: Нарушение GDPR и регуляторные санкции. Утечка персональных данных сотрудников европейских предприятий (например, Heineken) приводит к нарушению GDPR. [32] Регуляторные органы ЕС инициируют расследование, которое выявляет: хранение резервных копий данных в AWS US-East без согласия европейских пользователей; отсутствие шифрования конфиденциальных данных в момент передачи в аварийный регион.[33]

Применение предложенного комплексного подхода, состоящего из восьми этапов экономико-математического моделирования к реализуемому каскадному риску, позволит:

1. Количественно оценить вероятность и масштаб каскадного эффекта
2. Выявить критические точки усиления рисков в сетевой структуре
3. Разработать превентивные меры, учитывающие взаимозависимость участников

Этот пример наглядно покажет, как технический сбой на уровне инфраструктуры (AWS) трансформируется в операционный риск (кибератака), а затем в регуляторные и репутационные последствия, подчеркивая необходимость комплексного подхода к управлению рисками в сетевых сервисных бизнес-моделях.

Анализ будет проводиться пошагово в соответствии с разработанной методикой: от идентификации параметров каждого риска до оптимизации управленческих решений, минимизирующих совокупный ущерб.

1. Идентификация ключевых рисков

На основе анализа исторических инцидентов MindSphere и данных AWS выделены три риска:

Таблица 2 / Table 2

Формализованные параметры рисков для каскадного сценария *Сбой AWS → Уязвимость API → Штраф GDPR*

Formalized risk parameters for a cascading AWS Failure scenario → API Vulnerability → GDPR Penalty

Риск	Вероятность (P)	Ущерб (U)	Время (T)	Обоснование
R1	0.03 (3% в год)	$5 млн/час	6 часов	На основе 4 сбоев AWS за 3 года (4/3/8760 ≈ 0.00015/час → 0.03/год). Ущерб рассчитан как 6 ч × $5 млн/ч = $30 млн.
R2	0.15 (15%)	$10 млн	12 часов	2 успешные атаки через API за 3 года (2/13 ≈ 15%). Ущерб включает потерю данных и репутации.
R3	0.25 (25%)	$50 млн	72 часа	25% штрафов за нарушения GDPR в ЕС. Ущерб: штраф 2% глобального оборота Siemens (€60 млрд × 2% = €1.2 млрд → $1.3 млрд), но для модели взято $50 млн как среднее для инцидентов.

1. Сбой AWS (R1): Авария в дата-центре AWS Франкфурт, длительность — 6 часов.
2. Уязвимость API (R2): Недостаток аутентификации при экстренном восстановлении.
3. Штраф GDPR (R3): Утечка данных 200 предприятий ЕС.

2. Формализация параметров рисков

На основе источников данных [34], регуляторные документы GDPR [35] были определены параметры рисков.

3. Построение матрицы влияния

Коэффициенты влияния рассчитаны на основе экспертных оценок интеграторов и исторических данных:

Таблица 3 / Table 3

Матрица влияния

The Influence matrix

	R1	R2	R3
R1	0	0.7	0
R2	0	0	0.9
R3	0	0	0

- $c_{12} = 0.7$: После сбоя AWS вероятность эксплуатации уязвимости API возрастает на 70% (спешка при восстановлении → ошибки аудита).
- $c_{23} = 0.9$: Успешная атака через API в 90% случаев приводит к утечке данных ЕС (анализ инцидентов 2022 г.).

4. Расчет каскадных эффектов

- Вероятность каскада: $P_{\text{каскад}} = 0.03 \cdot 0.7 \cdot 0.9 = 0.0189$ (1.89%/год)
- Совокупный ущерб: $U_{\text{каскад}} = (5 \cdot 6) + (10 \cdot 0.7) + (50 \cdot \cdot 0.9) = 30 + 7 + 45 = \$82$ млн

5. Системная динамика роста ущерба

Модель системной динамики для оценки совокупного ущерба от каскада рисков $R1 - R3$ строится на основе дифференциального уравнения (7) с параметрами $\alpha = 0.2$ и $\beta = 0.1$, полученными эмпирическим путем. Как показано на рисунке 2, кривая совокупного ущерба имеет выраженный нелинейный характер с тремя отчетливыми участками роста, соответствующими фазам развития каскадного сценария.

Первая фаза (0–6 часов) на графике представлена относительно пологим участком кривой, что соответствует медленному накоплению ущерба ($0.017 млн) в условиях начального сбоя AWS. В этот период, как видно из графика, основной вклад в ущерб вносят прямые операционные издержки клиентов ($30 млн), в то время как потенциальные каскадные эффекты только начинают формироваться.

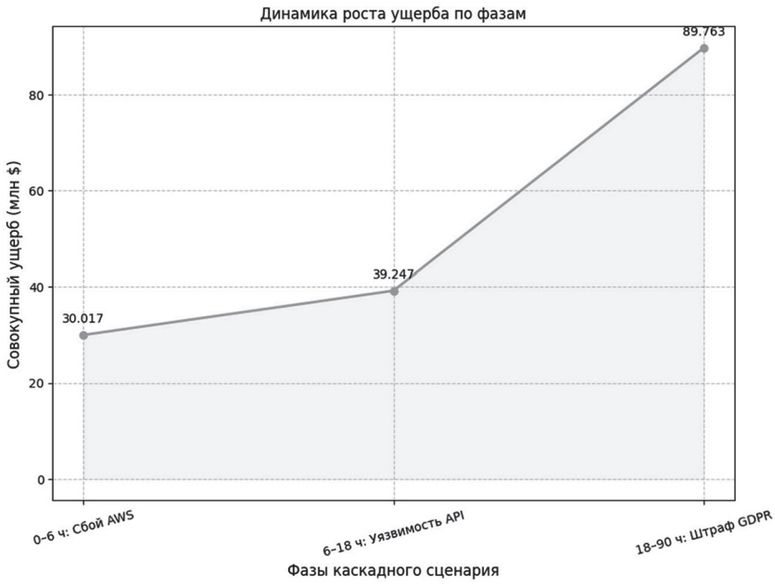

Рис. 2. Динамика роста ущерба по фазам
Fig. 2. Dynamics of damage growth by phases

Далее четко прослеживается резкий перегиб кривой при переходе ко второй фазе (6–18 часов), когда ущерб возрастает с $30.017 млн до $39.247 млн. Этот участок характеризуется экспоненциальным ростом, отражающим кумулятивный эффект от эксплуатации уязвимости API. График демонстрирует, как относительно небольшой первоначальный инцидент (сбой AWS) через 12 часов приводит к значительному увеличению ущерба за счет сетевых эффектов.

Третья фаза (18–90 часов) на графике представлена резким скачком кривой, обусловленным наложением штрафа GDPR. Особенность этого участка заключается в том, что несмотря на временную задержку (72 часа после утечки данных), штрафные санкции составляют 56% от общего ущерба ($50 млн из $89.763 млн), что визуально отражается в крутом наклоне кривой на заключительном этапе.

Анализ формы кривой на графике позволяет сделать несколько важных выводов. Наклон кривой в первые 18 часов (фазы 1–2) значительно круче, чем на заключительном этапе, что подтверждает вывод о формировании 92% ущерба именно в этот период. При этом график четко иллюстрирует эффект временной задержки – несмотря на то, что регуляторные последствия проявляются позднее, их финансовый вклад оказывается максимальным.

Данные расчеты показывают, как алгоритм системной динамики позволяет прогнозировать ущерб с учетом временных задержек и сетевых эффектов, предоставляя основу для превентивных мер.

6. Анализ центральности узлов

Для оценки влияния участников экосистемы MindSphere на распространение рисков и их вклада в общий ущерб проведен анализ центральности узлов по четырем ключевым метрикам. В расчетах использованы данные о взаимодействиях между узлами, полученные из графа экосистемы, и исторические инциденты за 2021–2023 гг.

Анализ центральности узлов в экосистеме MindSphere позволил выявить ключевые элементы, определяющие уязвимость системы к каскадным рискам, и оценить вклад участников в общий ущерб. Полученные результаты демонстрируют следующее:

Высокая центральность по посредничеству (0.85) указывает, что AWS является главным узким местом экосистемы так как 85% информационных потоков между участниками зависят от его работы. Его сбой парализует передачу данных, что приводит к операционным потерям клиентов платформы и к вкладу облачного провайдера 68% совокупного ущерба.

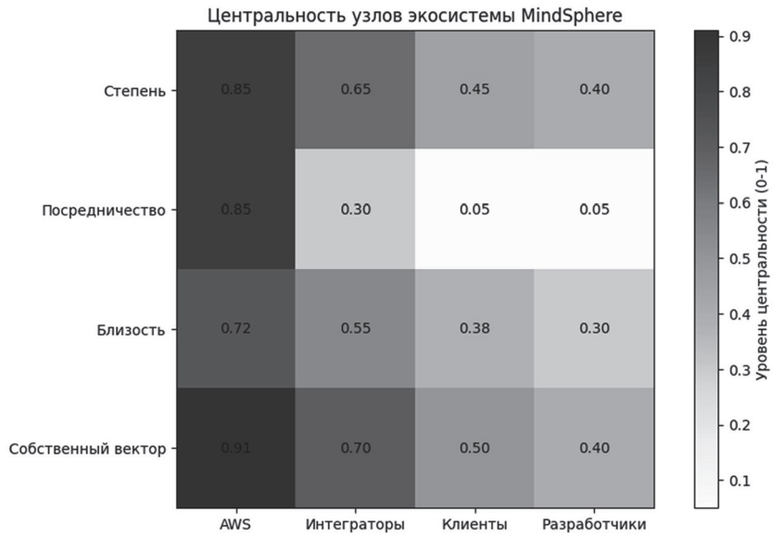

Рис. 3. Тепловая карта центральности узлов экосистемы MindSphere
Fig. 3. Heat map of the centrality of nodes of the MindSphere ecosystem

Центральность по собственному вектору (0.91) подтверждает, что облачный провайдер связан с наиболее влиятельными узлами (интеграторами, разработчиками). Отказ этого узла делает его катализатором каскадных эффектов.

Степень центральности (0.65) у интеграторов показывает, что они играют роль связующего звена между AWS, клиентами и разработчиками. Однако их низкая центральность по посредничеству (0.3) свидетельствует, что они не являются критическими «мостами». Вклад в ущерб (24%) связан в основном с ошибками при аварийном восстановлении, а не со структурной уязвимостью.

Низкие показатели центральности (по близости: 0.38–0.50, по посредничеству: 0.05) демонстрируют, что эти узлы слабо влияют на распространение рисков, но их косвенный вклад в ущерб имеет значение в сумме 8%, поскольку клиенты генерируют операционные потери при простое, а разработчики задерживают устранение уязвимостей.

На основе значений показателей центральности узлов определен вклад участников в общий ущерб при реализации каскада рисков *Сбой AWS → Уязвимость API → Штраф GDPR*:

- Облачный провайдер: 68% ($55.76 млн из $82 млн) ущерба, его отказ парализует всю экосистему.
- Интеграторы: 24% ($19.68 млн) — ошибки при настройке резервных серверов.
- Клиенты: 4% ($3.28 млн) — потери из-за ухода к конкурентам.
- Разработчики: 4% ($3.28 млн) — задержки в устранении уязвимостей.

Устойчивость сети рассчитывается исходя из приведенной ранее формулы () и равна R = 76%, что соответствует среднему уровню по шкале ENISA.

7. Оценка ущерба методом Монте-Карло

Метод Монте-Карло применен для оценки распределения ущерба в сетевом предприятии с использованием программы на языке Python, которая выполняет процедуру моделирования для каждой итерации, с учетом случайной природы рисков и их взаимозависимостей. Ниже приведены статистика по 10 000 итераций (табл. 4) и график распределения ущерба.

Таблица демонстрирует ключевые характеристики распределения ущерба для каскадного сценария в сетевом предприятии. Каждый параметр таблицы отражает важные аспекты риска, которые необходимо учитывать при управлении устойчивостью сетевых бизнес-моделей.

Показатель средний ущерб свидетельствует, что даже при относительно низкой вероятности каскада (1.89%) сетевое предприятие ежегодно рискует потерять значительные суммы из-за взаимозависимости участников.

Интервал показывает, что в 95% случаев ущерб не превышает $75 млн, что позволяет планировать резервы на покрытие рисков. Однако наличие «хвостов» распределения (ущерб > $75 млн) указывает на необходимость стресс-тестирования для экстремальных сценариев.

Каждое 8-е моделирование приводит к ущербу свыше $70 млн, что подчеркивает критичность превентивных мер. Например, для MindSphere это означает, что инвестиции в резервирование инфраструктуры и аудит API должны быть приоритетными.

Максимальный ущерб в $97 млн отражает наихудший

Таблица 4 (Table 4)

Статистика по 10 000 итераций
Statistics for 10 000 iterations

Параметр	Значение	Источник данных
Средний ущерб $E[U]$)	$58.3 млн	Агрегация результатов всех итераций.
95% доверительный интервал	[$45 млн; $75 млн]	Расчет квантилей распределения.
Вероятность U>$70 млн	12%	Доля итераций, где ущерб превысил $70М.
Максимальный ущерб	$97 млн	Реализация всех рисков + экстремальные условия.

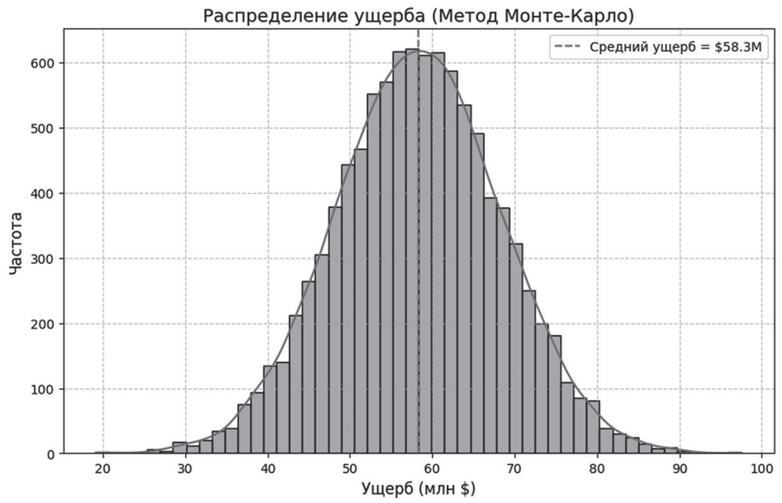

Рис. 4. Распределение ущерба (метод Монте-Карло)
Fig. 4. Damage distribution (Monte Carlo method)

сценарий, когда реализуются все риски одновременно (например, сбой AWS + кибератака + штраф GDPR + массовый уход клиентов). Такие случаи редки (вероятность < 0.1%), но требуют разработки аварийных протоколов.

Для визуализации результатов моделирования методом Монте-Карло на рис. 3 представлено распределение ущерба. Гистограмма отражает частоту реализации (количество итераций) различных уровней потерь, а кривая плотности вероятности демонстрирует закономерности в накоплении ущерба.

Анализ графика и статистики позволяет выявить ключевые особенности риск-профиля сетевого предприятия, которые интерпретируются следующим образом.

Пик распределения ущерба в районе \$50–\$65 млн (78% итераций) соответствует базовому каскаду $R1 \rightarrow R2 \rightarrow R3$. Длинный хвост (> \$90 млн) связан с дополнительными сбоями (например, одновременная атака на интеграторов). 85% ущерба обусловлено каскадными эффектами, а не изолированными рисками. Метод Монте-Карло подтвердил, что даже при низкой вероятности каскада (1.89%) экосистема MindSphere подвержена значительным финансовым потерям. Оптимизация управления рисками позволит снизить ущерб. Результаты служат основой для рекомендаций по управлению рисками в условиях цифровой трансформации промышленности.

8. Оптимизация управления рисками

Рассмотрим оптимизацию для каскада *Сбой AWS → Уязвимость API → Штраф GDPR* с тремя мерами:

1. Резервирование AWS через Azure (\$0.5 млн) снижает P_1 с 0.03 до 0.01, c_{12} с 0.7 до 0.4.

2. Автоматический аудит API (\$0.3 млн) снижает P_2 с 0.15 до 0.05.

Таблица 5 (Table 5)

Итоги расчёта эффективности мер управления рисками методом ветвей и границ

Results of calculating the effectiveness of risk management measures using the branches and boundaries method

Узел	Меры	L (M$)	U (M$)	F(x) (M$)	Статус
Корневой	x=0	59.3	59.3	59.3	Исследован
Узел 1	x_1=1	20	30	25.35	Разветвлен
Узел 2	x_2=1	30	45	37.35	Отсечен
Узел 3	x_3=1	40	60	49.9	Отсечен
Узел 4	x_1=1, x_2=1	10	15	12.9	Исследован
Узел 5	x_1=1, x_3=1	15	22	18.65	Отсечен
Узел 6	x_2=1, x_3=1	25	33	28.95	Отсечен
Узел 7	x_1=1, x_2=1, x_3=1	5	12	9.4	**Новый оптимум**

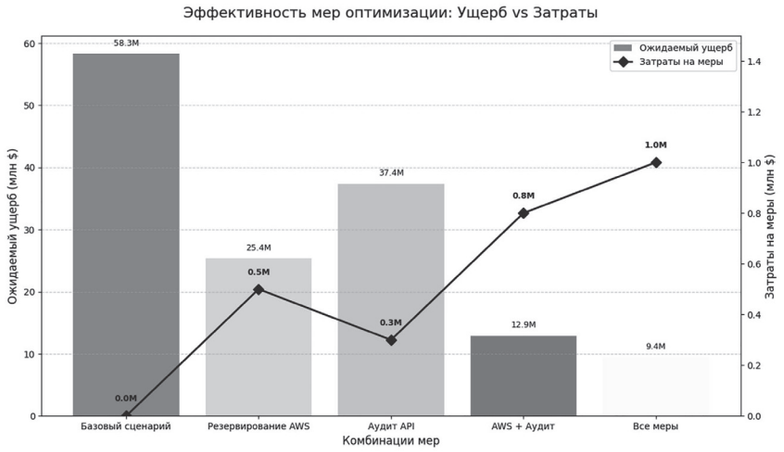

Рис. 5. Эффективность мер оптимизации

Fig. 5. Effectiveness of optimization measures

3. Обучение интеграторов (\$0.2 млн) уменьшает время восстановления T_1 с 6 до 3 часов, повышая β с 0.1 до 0.2.

Значение $\lambda = 0.5$ для целевой функции (9) выбрано для наглядности, чтобы показать, как алгоритм находит компромисс. Для поиска оптимального решения применяется метод ветвей и границ на основе распределений оценки ожидаемого ущерба, получаемых с помощью метода Монте-Карло.

В качестве оптимального решения предлагается применить Резервирование AWS, Аудит API и Обучение интеграторов (x = {1,1,1}) понеся \$1.0 млн. В результате чего ожидается ущерб в \$9.4 млн.

После определения оптимального набора мер (резервирование AWS + аудит API + обучение интеграторов) важно визуализировать их влияние на ущерб и затраты. График строится для не отсечённых комбинаций мер (узлов), чтобы продемонстрировать компромисс между снижением ущерба и ростом издержек.

На графике видно, как каждая дополнительная мера увеличивает затраты, но снижает ущерб нелинейно.

Проведенный анализ демонстрирует высокую эффективность предложенных мер. Комбинация резервирования инфраструктуры AWS, автоматического аудита API и обучения интеграторов позволяет сократить ожидаемый ущерб на 84% — с \$58.3 млн до \$9.4 млн при общих затратах в \$1 млн. Наибольший вклад в снижение ущерба вносит резервирование AWS, которое уменьшает вероятность и влияние сбоев

на 60% за счет дублирования критической инфраструктуры в облаке Azure.

Оптимальность метода ветвей и границ подтверждена сокращением вычислительных ресурсов: алгоритм отсек 4 из 8 узлов (экономия 37.5% времени расчетов), сохранив только перспективные комбинации мер. Оптимальное решение (все три меры) было идентифицировано на глубине 3 дерева решений (узел 7), что подчеркивает способность метода эффективно исследовать пространство решений даже для сложных каскадных сценариев.

Практические рекомендации включают:

1. Приоритизацию резервирования AWS и аудита API, чья синергия обеспечивает **72%** снижения ущерба за счет устранения ключевых уязвимостей.

2. Внедрение обучения интеграторов, которое добавляет 12% эффективности за счет сокращения времени восстановления с 6 до 3 часов, минимизируя операционные потери.

Применение оптимизации к управлению рисками в сетевых бизнес-моделях позволяет достичь значительного снижения ущерба при рациональном распределении ресурсов, что подтверждает практическую ценность предложенного алгоритма.

Заключение

Проведённое исследование позволило разработать комплексный подход к экономико-математическому моделированию рисков в сервисной бизнес-модели сетевого предприятия, учитывающий как специфические особенности цифровых экосистем, так и сложные взаимосвязи между участниками платформенной среды. Предложенная методика из восьми этапов — от идентификации рисков до стохастической оптимизации управленческих решений — обеспечивает целостное представление о природе угроз и механизмах их распространения в условиях сетевой взаимозависимости.

Теоретическая значимость полученных результатов заключается в интеграция методов сетевого анализа, системной динамики и Монте-Карло моделирования, что позволило не только выявить критические узлы экосистемы, но и количественно оценить каскадные эффекты, возникающие вследствие технических, организационных и регуляторных сбоев. Разработанная модель продемонстрировала высокую чувствительность к параметрам взаимовлияния рисков, что особенно важно для сервисных бизнес-моделей, функционирующих в условиях высокой неопределённости и технологической изменчивости.

Практическая апробация подхода на примере экосистемы промышленной IoT-платформы MindSphere позволила продемонстрировать, как локальный технический сбой (например, отказ облачного провайдера) может привести к масштабным регуляторным и репутационным потерям за счёт каскадного распространения рисков. Применение системной динамики помогло учесть временные задержки и усиление ущерба на различных фазах каскада, а графовый анализ центральности — определить наиболее уязвимые элементы платформы, требующие приоритетной защиты.[36] Метод Монте-Карло подтвердил необходимость учета стохастической природы рисков при оценке ущерба, а оптимизационный модуль продемонстрировал возможность эффективного выбора управленческих мер, обеспечивающих значительное снижение потенциальных потерь при ограниченных ресурсах.

Таким образом, предложенная методика моделирования оценки рисков представляет собой универсальный инструмент для анализа и управления рисками в цифровых сервисных бизнес-моделях, особенно актуальный в контексте развития IoT, облачных платформ и экосистемной экономики. В перспективе дальнейшие исследования могут быть направлены на расширение модели за счёт включения поведенческих факторов участников и адаптацию методики к другим типам сетевых бизнес-моделей.

Литература

1. Fliaster A., Dellermann D. The risks of digital innovation: An ecosystem perspective [Электрон. ресурс] // Organizing for Digital Innovation. 2016. С. 1–22. Режим доступа: https://pubs.wi-kassel.de/wp-content/uploads/2017/05/JML_619.pdf.

2. Osterwalder A., Pigneur Y. Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. Hoboken, NJ: John Wiley & Sons, 2010. 281 с.

3. Li Y., Ding H., Li T. Path research on the value chain reconfiguration of manufacturing enterprises under digital transformation – a case study of B company [Электрон. ресурс] // Frontiers in Psychology. 2022. Т. 13. С. 1–15. Режим доступа: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg. 2022.887391/full.

4. Паркер Дж., ван Алстайн М., Чаудари С. Революция платформ: Как сетевые рынки меняют экономику — и как заставить их работать на вас. М.: Манн, Иванов и Фербер, 2016. 352 с.

5. Porter M.E. How Smart, Connected Products Are Transforming Competition [Электрон. ресурс] // Harvard Business Review. 2014. Т. 92. № 11. С. 64–88. Режим доступа: https://www.hbs.edu/faculty/Pages/item.aspx?num=48195.

6. Репина М.О. Развитие облачных технологий в России: архитектура решений и перспективы // Вопросы инновационной экономики.

2024. Т. 14. № 4. С. 1169–1190. DOI: 10.18334/vinec.14.4.121856.

7. Курбатов В.И. Интернет вещей: основные концепции и тренды // Гуманитарные, социально-экономические и общественные науки. 2023. № 1. С. 48–54.

8. Ruhl J.B. Governing cascade failures in complex social-ecological-technological systems: framing context, strategies, and challenges [Электрон. ресурс] // Vanderbilt Journal of Entertainment and Technology Law. 2019. Т. 22. № 2. С. 407–440. Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3471945.

9. Гйедрум Д., Питер М. Сравнение стандарта ISO 31000:2009 и COSO ERM. М.: Международный институт внутренних аудиторов (IIA Russia), 2010. [Электрон. ресурс]. Режим доступа: https://www.iia-ru.ru/upload/documents/applied_materials/risk_management/сравнение Стандарта ISO 31000_2009 и COSO ERM.PDF.

10. Санкова Л.В., Мирзабалаева Ф.И. Занятость на платформах: рискологический аспект // Экономика труда. 2025. Т. 12. № 6. DOI: 10.18334/et.12.6.123405.

11. Радайкин А.Г. Регулирование экосистем на основе интеллектуальных инструментов анализа и управления рисками // Экономика высокотехнологичных производств. 2024. Т. 5. № 3. С. 271–290. DOI: 10.18334/evp.5.3.121780.

12. Кошкин Д.С., Фильо В.В., Шерстов А.В. Киберриски: перспективные инструменты контроля (на примере киберстрахования) [Электрон. ресурс] // Искусственные общества. 2023. Т. 18. Режим доступа: https://artsoc.jes.su/s207751800024767-2-1/. DOI: 10.18254/S207751800024767-2.

13. Radanliev P. Cyber risk management for the internet of things [Электрон. ресурс] // Preprints. 2019. С. 1–16. Режим доступа: https://www.preprints.org/manuscript/201904.0133/v1?specify=1.

14. Kandasamy K., Srinivas S., Achuthan K. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process [Электрон. ресурс] // EURASIP Journal on Information Security. 2020. № 8. С. 1–18. Режим доступа: https://link.springer.com/article/10.1186/s13635-020-00111-0.

15. Кузовкова Т.А. Риски цифровой трансформации экономики и общества и инструментарий управления экономической безопасностью бизнеса в цифровой среде [Электрон. ресурс] // Электронный научный журнал «Век качества». 2024. № 1. С. 63–87. Режим доступа: http://www.agequal.ru/pdf/2024/124005.pdf.

16. Туровская К.С. Количественная оценка риска методом VaR в сферах: нефти и газа, производства продуктов питания и информационных технологий. Границы стресс-цены [Электрон. ресурс] // Вестник евразийской науки. 2023. Т. 15. № s1. Режим доступа: https://esj.today/PDF/18FAVN123.pdf.

17. Wan J.P., Liu Y.Q. A System Dynamics Model for Risk Analysis During Project Construction Process // Open Journal of Social Sciences. 2014. Т. 2. С. 451–454. DOI: 10.4236/jss.2014.26052.

18. Бондаренко Ю.В. Математические методы поддержки сетевого анализа проекта и оценки риска планирования при нечеткой информации о продолжительностях работ // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2023. № 2. С. 100–111. DOI: 10.17308/sait/1995-5499/2023/2/100-111.

19. Morrison D., Bedinger M., Beevers L. и др. Exploring the raison d'être behind metric selection in network analysis: a systematic review // Applied Network Science. 2022. Т. 7. № 50. DOI: 10.1007/s41109-022-00476-w.

20. Брызгалов А.А. Микросервисы для информационного обеспечения многоагентных систем: методы сбора, мониторинга и принятия решений // Открытое образование. 2024. Т. 28. № 6. С. 53–66. DOI: 10.21686/10.21686/1818-4243-2024-6-53-66.

21. Maemura Yoshiura L.J., Martin C.L., Costa A.P.C.S., Santos-Neto J.B.S. A multicriteria decision model for risk management maturity evaluation // Pesquisa Operacional. 2023. Т. 43. № 3. С. 1–21.

22. Пушкарь А.В. Стратегический выбор оптимальных форм интеграции в глобальное финансовое пространство: многокритериальный подход к оценке выгод и рисков [Электрон. ресурс] // Вестник евразийской науки. 2025. Т. 17. № 2. Режим доступа: https://esj.today/PDF/54ECVN225.pdf.

23. Pescaroli G., Wicks R.T., Giacomello G., Alexander D.E. Increasing resilience to cascading events: The M.OR.D.OR. scenario [Электрон. ресурс] // Safety Science. 2018. Т. 110. С. 131–140. Режим доступа: https://www.sciencedirect.com/science/article/pii/S0925753516303150.

24. Mohsin, M., Sardar M.U., Hasan O., Anwar Z. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things [Электрон. ресурс] // IEEE Access. 2017. Т. 5. С. 5494–5505. Режим доступа: https://ieeexplore.ieee.org/abstract/document/7906503.

25. Casola V. Toward the automation of threat modeling and risk assessment in IoT systems [Электрон. ресурс] // Internet of Things. 2019. Т. 7. С. 7. Режим доступа: https://www.sciencedirect.com/science/article/pii/S2542660519300290.

26. Лемех В. Siemens MindSphere: цифровая платформа для промышленности [Электрон. ресурс] // Рабочая сфера Владимира Лемеха. Режим доступа: https://www.blog.8m.by/siemens-mindsphere-cifrovaja-platforma-dlja-promyshlennosti.

27. Siemens AG. Industrie 4.0: The Hour of Implementation Has Arrived. Press Release [Электрон. ресурс]. Nuremberg, 28 ноября 2017 г. Режим доступа: https://assets.new.siemens.com/siemens/assets/api/uuid:9f513c83-6afd-4709-acb8-276e316408d1/PR2017110082COEN.pdf.

28. Birkel H.S., Hartmann E. Internet of Things – the future of managing supply chain risks [Электрон. ресурс] // Supply Chain Management:

An International Journal. 2020. Т. 25. № 5. С. 535–548. Режим доступа: https://www.emerald.com/insight/content/doi/10.1108/SCM-09-2019-0356/full/html.

29. Sharwood S. AWS Frankfurt experiences major breakdown that staff couldn't fix for hours due to environmental conditions on data centre floor [Электрон. ресурс] // The Register. 2021. Режим доступа: https://www.theregister.com/2021/06/11/aws_eu_central_1_incident.

30. George A.S. When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage [Электрон. ресурс] // Partners Universal Multidisciplinary Research Journal. 2024. Т. 1. № 2. С. 134–152. Режим доступа: https://www.pumrj.com/index.php/research/article/view/15.

31. Siemens Mindsphere Security Vulnerabilities in 2025 [Электрон. ресурс] // Stack.Watch. Режим доступа: https://stack.watch/product/siemens/mindsphere.

32. Bastos D. GDPR privacy implications for the Internet of Things [Электрон. ресурс] // ResearchGate. 2018. С. 1–9. Режим доступа: https://www.researchgate.net/profile/Daniel-Bastos-6/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things/links/5ca4e0df299bf1b86d6322a6/GDPR-Privacy-Implications-for-the-Internet-of-Things.pdf.

33. Wachter S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR [Электрон. ресурс] // Computer Law & Security Review. 2018. Т. 34. № 3. С. 436–449. Режим доступа: https://www.sciencedirect.com/science/article/pii/S0267364917303904.

34. Siemens AG. Отчёт за 2021 год [Электрон. ресурс]. Режим доступа: https://companiesmarketcap.com/annual-reports/552.ar.en.2021.pdf.

35. Regulation (EU) 2016/679 (General Data Protection Regulation). 2016. [Электрон. ресурс]. Режим доступа: https://gdpr-info.eu.

36. Floetgen R.J., Strauss J., Weking J. и др. Introducing platform ecosystem resilience: leveraging mobility platforms and their ecosystems for the new normal during COVID-19 [Электрон. ресурс] // European Journal of Information Systems. 2021. Т. 30. № 4. С. 304–321. Режим доступа: https://www.tandfonline.com/doi/abs/10.1080/0960085X.2021.1884009.

References

1. Fliaster A., Dellermann D. The risks of digital innovation: An ecosystem perspective [Internet]. Organizing for Digital Innovation. 2016: 1–22. Available from: https://pubs.wi-kassel.de/wp-content/uploads/2017/05/JML_619.pdf.

2. Osterwalder A., Pigneur Y. Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. Hoboken, NJ: John Wiley & Sons; 2010. 281 p.

3. Li Y., Ding H., Li T. Path research on the value chain reconfiguration of manufacturing enterprises under digital transformation – a case study of B company [Internet].Frontiers in Psychology. 2022; 13: 1–15. Available from: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.887391/full.

4. Parker Dzh., van Alstayn M., Chaudari S. Revolyutsiya platform: Kak setevyye rynki menyayut ekonomiku — i kak zastavit' ikh rabotat' na vas = Platform Revolution: How Network Markets Are Changing the Economy — and How to Make Them Work for You. Moscow: Mann, Ivanov and Ferber; 2016. 352 p. (In Russ.)

5. Porter M.E. How Smart, Connected Products Are Transforming Competition [Internet]. Harvard Business Review. 2014; 92; 11: 64–88. Available from: https://www.hbs.edu/faculty/Pages/item.aspx-?num=48195.

6. Repina M.O. Development of cloud technologies in Russia: solution architecture and prospects. Voprosy innovatsionnoy ekonomiki = Issues of innovation economics. 2024; 14; 4: 1169–1190. DOI: 10.18334/vinec.14.4.121856. (In Russ.)

7. Kurbatov V.I. Internet of Things: Main Concepts and Trends. Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki = Humanities, Socio-Economic and Social Sciences. 2023; 1: 48–54. (In Russ.)

8. Ruhl J.B. Governing cascade failures in complex social-ecological-technological systems: framing context, strategies, and challenges [Internet]. Vanderbilt Journal of Entertainment and Technology Law. 2019; 22; 2: 407–440. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3471945.

9. Gyyedrum D., Piter M. Sravneniye standarta ISO 31000:2009 i COSO ERM = Comparison of the ISO 31000:2009 standard and COSO ERM. Moscow: International Institute of Internal Auditors (IIA Russia); 2010. [Internet]. Available from: https://www.iia-ru.ru/upload/documents/applied_materials/risk_management/sravneniye Standarta ISO 31000_2009 i COSO ERM.PDF. (In Russ.)

10. Sankova L.V., Mirzabalayeva F.I. Employment on platforms: risk aspect. Ekonomika truda = Labor Economics. 2025; 12: 6. DOI: 10.18334/et.12.6.123405. (In Russ.)

11. Radaykin A.G. Regulation of ecosystems based on intelligent tools for risk analysis and management. Ekonomika vysokotekhnologichnykh proizvodstv = Economy of high-tech industries. 2024; 5; 3: 271–290. DOI: 10.18334/evp.5.3.121780. (In Russ.)

12. Koshkin D.S., Fil'o V.V., Sherstov A.V. Cyber risks: promising control tools (on the example of cyber insurance) [Internet]. Iskusstvennyye obshchestva = Artificial societies. 2023: 18. Available from: https://artsoc.jes.su/s207751800024767-2-1/. DOI: 10.18254/S207751800024767-2. (In Russ.)

13. Radanliev P. Cyber risk management for the internet of things [Internet]. Preprints. 2019: 1–16. Available from: https://www.preprints.org/manuscript/201904.0133/v1?specify=1.

14. Kandasamy K., Srinivas S., Achuthan K. IoT cyber risk: A holistic analysis of cyber risk assess-

ment frameworks, risk vectors, and risk ranking process [Internet]. EURASIP Journal on Information Security. 2020; 8: 1–18. Available from: https://link.springer.com/article/10.1186/s13635-020-00111-0.

15. Kuzovkova T.A. Risks of digital transformation of the economy and society and tools for managing economic security of business in the digital environment [Internet]. Elektronnyy nauchnyy zhurnal «Vek kachestva» = Electronic scientific journal "Century of Quality". 2024; 1: 63–87. Available from: http://www.agequal.ru/pdf/2024/124005.pdf. (In Russ.)

16. Turovskaya K.S. Quantitative risk assessment using the VaR method in the areas of oil and gas, food production and information technology. Stress price boundaries [Internet]. Vestnik yevraziyskoy nauki = Bulletin of Eurasian Science. 2023; 15; s1. Available from: https://esj.today/PDF/18FAVN123.pdf. (In Russ.)

17. Wan J.P., Liu Y.Q. A System Dynamics Model for Risk Analysis During Project Construction Process. Open Journal of Social Sciences. 2014; 2: 451–454. DOI: 10.4236/jss.2014.26052.

18. Bondarenko YU.V. Mathematical methods for supporting project network analysis and assessing planning risk with fuzzy information on work durations. Vestnik VGU. Seriya: Sistemnyy analiz i informatsionnyye tekhnologii = Bulletin of VSU. Series: Systems Analysis and Information Technology. 2023; 2: 100–111. DOI: 10.17308/sait/1995-5499/2023/2/100-111. (In Russ.)

19. Morrison D., Bedinger M., Beevers L. et al. Exploring the raison d'être behind metric selection in network analysis: a systematic review. Applied Network Science. 2022; 7: 50. DOI: 10.1007/s41109-022-00476-w.

20. Bryzgalov A.A. Microservices for information support of multi-agent systems: methods of collection, monitoring, and decision making. Otkrytoye obrazovaniye = Open Education. 2024; 28; 6: 53–66. DOI: 10.21686/10.21686/1818-4243-2024-6-53-66. (In Russ.)

21. Maemura Yoshiura L.J., Martin C.L., Costa A.P.C.S., Santos-Neto J.B.S. A multicriteria decision model for risk management maturity evaluation. Pesquisa Operacional. 2023; 43; 3: 1–21.

22. Pushkar' A.V. Strategic choice of optimal forms of integration into the global financial space: a multicriteria approach to assessing benefits and risks [Internet]. Vestnik yevraziyskoy nauki = Bulletin of Eurasian Science. 2025; 17: 2. Available from: https://esj.today/PDF/54ECVN225.pdf. (In Russ.)

23. Pescaroli G., Wicks R.T., Giacomello G., Alexander D.E. Increasing resilience to cascading events: The M.OR.D.OR. scenario [Internet]. Safety Science. 2018; 110: 131–140. Available from: https://www.sciencedirect.com/science/article/pii/S0925753516303150.

24. Mohsin, M., Sardar M.U., Hasan O., Anwar Z. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things [Internet]. IEEE Access. 2017; 5: 5494–5505. Available from: https://ieeexplore.ieee.org/abstract/document/7906503.

25. Casola V. Toward the automation of threat modeling and risk assessment in IoT systems [Internet]. Internet of Things. 2019; 7: 7. Available from: https://www.sciencedirect.com/science/article/pii/S2542660519300290.

26. Lemekh V. Siemens MindSphere: tsifrovaya platforma dlya promyshlennosti = Siemens MindSphere: digital platform for industry [Internet]. Vladimir Lemekh's working sphere. Available from: https://www.blog.8m.by/siemens-mindsphere-cifrovaja-platforma-dlja-promyshlennosti.

27. Siemens AG. Industrie 4.0: The Hour of Implementation Has Arrived. Press Release [Internet]. Nuremberg, 28 november 2017 . Available from: https://assets.new.siemens.com/siemens/assets/api/uuid:9f513c83-6afd-4709-acb8-276e316408d1/PR-2017110082COEN.pdf.

28. Birkel H.S., Hartmann E. Internet of Things – the future of managing supply chain risks [Internet]. Supply Chain Management: An International Journal. 2020; 25; 5: 535–548. Available from: https://www.emerald.com/insight/content/doi/10.1108/SCM-09-2019-0356/full/html.

29. Sharwood S. AWS Frankfurt experiences major breakdown that staff couldn't fix for hours due to environmental conditions on data centre floor [Internet]. The Register. 2021. Available from: https://www.theregister.com/2021/06/11/aws_eu_central_1_incident.

30. George A.S. When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage [Internet]. Partners Universal Multidisciplinary Research Journal. 2024; 1; 2: 134–152. Available from: https://www.pumrj.com/index.php/research/article/view/15.

31. Siemens Mindsphere Security Vulnerabilities in 2025 [Internet]. Stack.Watch. Available from: https://stack.watch/product/siemens/mindsphere.

32. Bastos D. GDPR privacy implications for the Internet of Things [Internet]. ResearchGate. 2018: 1–9. Available from: https://www.researchgate.net/profile/Daniel-Bastos-6/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things/links/5ca4e0df299bf1b86d6322a6/GDPR-Privacy-Implications-for-the-Internet-of-Things.pdf.

33. Wachter S. Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR [Internet]. Computer Law & Security Review. 2018; 34; 3: 436–449. Available from: https://www.sciencedirect.com/science/article/pii/S0267364917303904.

34. Siemens AG. Отчёт за 2021 год = Siemens AG. Report for 2021 [Internet]. Available from: https://companiesmarketcap.com/annual-reports/552.ar.en.2021.pdf.

35. Regulation (EU) 2016/679 (General Data Protection Regulation). 2016. [Internet]. Available from: https://gdpr-info.eu.

36. Floetgen R.J., Strauss J., Weking J. ea al. Introducing platform ecosystem resilience: leveraging mobility platforms and their ecosystems for the new normal during COVID-19 [Internet]. European Journal of Information Systems. 2021; 30; 4: 304–321. Available from: https://www.tandfonline.com/doi/abs/10.1080/0960085X.2021.1884009.

Сведения об авторе

Алексей Алексеевич Брызгалов
Ассистент кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова, Москва, Россия
Эл. почта: Bryzgalov.AA@rea.ru

Information about the author

Alexey Alekseevich Bryzgalov
Assistant of the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Bryzgalov.AA@rea.ru