СТАТЬЯ

УДК 33:51-7:004.94

ОПТИМИЗАЦИОННАЯ ЭКОНОМИКО-МАТЕМАТИЧЕСКАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ОРГАНИЗАЦИИ С УЧЕТОМ ЗАТРАТ НА ПРЕДУПРЕЖДЕНИЕ И КОМПЕНСАЦИЮ УГРОЗ

Медведев А.В. ORCID ID 0000-0002-7654-056X

Федеральное государственное бюджетное образовательное учреждение высшего образования «Кемеровский государственный университет», Кемерово, Российская Федерация, e-mail: alexm_62@mail.ru

В работе строится двухкритериальная экономико-математическая модель безопасности функционирования сложной системы на примере информационной системы организации. Информационную защищенность указанной системы предлагается оценивать путем минимизации суммы двух типов рисков – связанных с угрозами безопасности до их реализации (априорные угрозы) и связанных с апостериорными угрозами, возникающими после реализации априорных. Тогда оптимальный уровень защищенности системы, в соответствии с принципом минимакса, определяется как минимум суммарных затрат на купирование априорных и апостериорных угроз. В связи с этим отмечается необходимость построения двухкритериальной математической модели, что обуславливается противоположной монотонной направленностью зависимостей уровня защищенности от указанных рисков. В качестве формы таких зависимостей выбираются линейные функции осуществляемых затрат. Обосновываются существование решения построенной модели и выбор метода ее решения путем перехода к эквивалентной однокритериальной задаче с линейной сверткой критериев и последующим Парето-анализом с использованием автоматизированного программно-аналитического комплекса. Отмечается возможность использования модели в качестве аналитической основы автоматизированной системы поддержки обоснованных решений не только в сфере информационной безопасности, но и в сфере комплексной безопасности сложных систем для анализа и сравнения уровней их защищенности от угроз социального, экономического, информационного, технологического и другого характера, включая комбинации указанных.

Ключевые слова: сложная система, угрозы безопасности, информационная защищенность, информационная система организации, линейная оптимизация, двухкритериальная задача, вычислительный эксперимент, поддержка принятия решений

OPTIMIZATION ECONOMIC-MATHEMATICAL MODEL OF SAFETY FUNCTIONING OF ORGANIZATION TAKING INTO ACCOUNT THE COSTS OF PREVENTION AND COMPENSATION OF THREATS

Medvedev A.V. ORCID ID 0000-0002-7654-056X

Federal State Budgetary Educational Institution of Higher Education "Kemerovo State University", Kemerovo, Russian Federation, e-mail: alexm_62@mail.ru

This paper develops an optimization economic-mathematical model for the operational security of a complex system using an organizational information system as an example. The information security of this system is proposed to be assessed by minimizing the sum of two types of risks: from security threats before their implementation (a priori threats) and from a posteriori threats arising after the implementation of a priori threats. The optimal level of system security, in accordance with the minimax principle, is determined as the minimum of the total costs of mitigating a priori and a posteriori threats. In this regard, the need to construct a two-criterion model is noted, due to the opposite monotonic direction of the dependencies between the level of security and the aforementioned risks. Linear functions of incurred costs are chosen as the form of such dependencies. The existence of a solution to the constructed model and the choice of a solution method by transitioning to an equivalent single-criterion problem with a linear convolution of criteria and subsequent Pareto analysis using an automated software and analytical suite are substantiated. The possibility of using the model as an analytical basis for an automated system to support informed decisions not only in the field of information security but also in the field of comprehensive security of complex systems for analyzing their security against technological, social, economic, information, and other threats, including combinations of these threats, is noted.

Keywords: complex system, security threats, information security, organizational information system, linear optimization, two-criterion problems, computational experiment, decision support

Введение

Функционирование сложных систем порождает необходимость решения проблем их безопасности различного генезиса – социального, экономического, технического, информационного и др. Это объективно связано в первую очередь с возникновением сопутствующих рисков и влечет необходимость решения соответствующих задач – от математического моделирования

до разработки систем поддержки принятия решений при управлении рисками сложных систем. Вопросы безопасности сложных социальных, экономических, технических систем являются ключевыми при оценке эффективности их функционирования. Например, для организации, производящей продукцию (товары и/или услуги), вложения в безопасность (в частности, информационную), как нематериальный актив организации, являются фактором ее стратегической стабильности, уменьшая риски критических финансовых потерь в связи с нарушением безопасности функционирования, что, по сути, превращает указанные вложения в инвестиционные и делает актуальной тему данной статьи.

В настоящее время опубликовано значительное количество работ, касающихся вопросов моделирования защищенности (экономической, информационной, технологической и др.) различных систем функционирования организации, большинство из которых в первую очередь рассматривают аспект информационной безопасности (ИБ). В работе [1] описывается современное состояние проблемы обеспечения, контроля и информационной защищенности в эргасистемах, как сложных системах управления объектами технических, технологических, организационных, экономических комплексов, имеющих существенный признак обязательного наличия человеческого или социального фактора в них. В монографии [2, с. 45–74] обоснована целесообразность использования методов исследования операций в системах управления ИБ, предложены возможные области применения моделей и методов комплексного управления информационной защитой объектов информатизации. Экономический аспект учета рисков ИБ организации рассматривается в работе [3]. Статьи [4; 5] посвящены анализу основных подходов к определению оптимального объема инвестиций, необходимого для обеспечения информационной безопасности информационной системы в рамках математической модели Гордона – Лоеба, в которой рассмотрены затраты на предотвращение угроз ИБ. В работе [6] акцентирована необходимость рассмотрения потоков затрат на компенсацию ущерба, возникающего при реализации угроз ИБ. В современных научных трудах по математическому моделированию задач информационной безопасности информационных систем организаций рассматриваются различные аналитические методы. В работе [7] использованы методы теории графов, а в [8] – теоретико-информационный метод энтропийно-вероятностного анализа дерева событий. В работах [9; 10] применены модели многокритериальной и дискретной оптимизации соответственно. В основу указанных методов чаще всего положен вероятностный принцип оценки рисков ИБ, в настоящее время подвергающийся обоснованной критике в литературе (например, [11]). Кроме того, среди описываемых моделей, алгоритмов и методов решения задачи оценки уровня информационной защищенности информационной системы организации (ИЗИСО) редко встречаются легко интерпретируемые, понятные практикам оптимизационные модели, для которых разработаны эффективные средства их автоматизированного анализа, наличие которых является необходимым условием разработки систем поддержки принятия решений в задачах управления ИЗИСО.

Цель исследования – построение двухкритериальной математической модели оценки уровня информационной защищенности информационной системы организации для определения оптимального распределения инвестиционного ресурса, включающего как потоки затрат, ориентированные на предотвращение угроз, так и потоки затрат на компенсацию возникающего ущерба от реализации угроз безопасности.

Материалы и методы исследования

Пусть изучаемая сложная система представляет собой информационную систему организации (ИСО). Очевидно, что информационная защищенность ИСО тем выше, чем ниже риски реализации различных угроз ее функционированию – нарушения работы электронных сред контроля систем управления, технологических цепочек, документооборота; отказов работоспособности аппаратного, программного обеспечения ИСО, связанных с внешним вмешательством или недостаточной квалификацией сотрудников, управленцев и др. При этом безопасность (в том числе информационная) сложной системы определяется не только мерами по предотвращению ее угроз, но и мерами по нейтрализации возможного ущерба в случае реализации этих угроз. Поэтому общий уровень ИЗИСО определяется минимумом суммы рисков предупреждения угроз безопасности и рисков компенсации ущерба, возникшего в связи с реализацией этих угроз, что соответствует использованию принципа минимакса, заключающегося в минимизации интегрального ущерба, который лицо, принимающее решения (ЛПР), не может предотвратить при развитии событий по наихудшим для него сценариям. Это требует рассмотрения как минимум двух критериев при решении задач ИЗИСО.

В связи со сказанным, в отличие от однокритериальной модели работы [12], где были рассмотрены риски ИСО от угроз до их реализации (априорные угрозы), здесь рассмотрим еще и риски, возникающие в связи с реализацией апостериорных угроз ИЗИСО. В отличие от использованной в однокритериальной модели обратно пропорциональной линейной зависимости риска $r_1 \sim a_1 - b_1 \cdot x$ от затрат (инвестиций) x, выделенных на предотвращение априорных угроз, для целей купирования апостериорных угроз используем зависимость, имеющую прямую пропорцию связи риска r_2 функционирования ИСО с затратами y на компенсацию ущерба: $r_2 \sim a_2 + b_2 \cdot y$. Иначе говоря, предполагается, что суммарный риск ИЗИСО на обеих стадиях функционирования ИСО понижается, если увеличивается сумма затрат на избежание угроз и компенсацию ущерба от реализации угроз (рисков), что соответствует росту ИЗИСО. Заметим, что коэффициент a_1 может трактоваться как максимальный объем затрат, который понадобится в случае реализации угроз при отсутствии инвестиций в купирование априорных угроз, а коэффициент a_2 – как минимальный объем затрат, который будет необходим для компенсации ущерба ИСО при отсутствии инвестиций в купирование апостериорных угроз. Минимальную сумму затрат x на защиту (избежание, устранение, уменьшение) от априорных угроз и затрат y на компенсацию (избежание, устранение, уменьшение) ущерба от апостериорных угроз будем считать оптимумом (максимальным уровнем) ИЗИСО. При этом оптимальные общие затраты должны соответствовать равенству $x = y$, которое становится очевидным при использовании нелинейных зависимостей уровня ИЗИСО от осуществляемых затрат x и y, в случае их противоположной монотонной направленности (например, [6, с. 52]). Следует отметить, что для универсальной организации, вообще говоря, трудно разделить бюджеты затрат на защиту от априорных угроз и на компенсацию ущерба от апостериорных угроз, вследствие чего целесообразно рассмотреть дополнительный управляющий параметр α, учитывающий соотношение оптимальных инвестиций x и y. Для производственной организации, производящей товары и/или услуги, гибкость управления ИЗИСО будет обусловлена соотношениями бюджетов общих затрат, затрат на защиту от априорных угроз, на компенсацию ущерба от апостериорных угроз, а также диапазонами выделяемых средств на купирование каждой угрозы в отдельности. Указанные соотношения могут иметь многочисленные варианты в зависимости от структуры менеджмента организации и его отношения к рискам безопасности.

Рассмотрим следующую математическую модель информационной защищенности информационной системы организации. Пусть N – количество априорных угроз ИБ, а L – количество видов ущерба ИС, соответствующих апостериорным угрозам ИБ;

x_k ($k = 1, \ldots, N$) – инвестиции в предотвращение k-й угрозы ИБ, денежных единиц (д.е.);

x_{N+l} ($l = 1, \ldots, L$) – затраты на устранение ($N+l$)-го ущерба, д.е.;

$(b1)_k$ ($k = 1, \ldots, N$) – весовые коэффициенты значимости k-й угрозы ИБ;

$(b2)_l$ ($l = 1, \ldots, L$) – весовые коэффициенты значимости l-го ущерба ИБ;

Z – общий бюджет на обеспечение ИЗИСО, д.е.;

Z_1 – бюджет на предупредительные мероприятия по обеспечению ИЗИСО, д.е.;

Z_2 – бюджет на мероприятия по компенсации ущерба в связи с нарушениями ИЗИСО, д.е.;

α – коэффициент соотношения суммарных затрат на предупредительные мероприятия (априорные угрозы) и суммарных затрат на мероприятия по компенсацию ущерба (апостериорные угрозы).

Тогда математическая модель ИЗИСО принимает следующий вид:

Критерии эффективности ИЗИСО

$$J_1 = \sum_{k=1}^{N} (b1)_k x_k \to max, \quad \sum_{k=1}^{N} (b1)_k = 1;$$
$$J_2 = \sum_{l=1}^{L} (b2)_l x_{N+l} \to max, \quad \sum_{l=1}^{L} (b2)_l = 1. \qquad (1)$$

Ограничения финансирования ИЗИСО:

$$\sum_{m=1}^{N+L} x_m \le Z, \ \sum_{k=1}^{N} x_k \le Z_1, \ \sum_{l=1}^{L} x_{N+l} \le Z_2,$$
$$\sum_{k=1}^{N} x_k \le \alpha \sum_{l=1}^{L} x_{N+l}, \ ZMIN_m \le x_m \le ZMAX_m,$$
$$x_m \ge 0, \ m = 1, \ldots, N+L. \qquad (2)$$

Результаты исследования и их обсуждение

Модель (1)–(2) обобщает модель в [12] на случай рассмотрения двух типов затрат на обеспечение ИЗИСО – на предупредительные мероприятия до и на компенсацию ущерба после реализации угроз ИБ. Путем

замены переменных $y_m = x_m - ZMIN_m$ задачу (1)–(2) можно привести к эквивалентной задаче, содержащей нулевое решение, что, учитывая компактность допустимого множества, позволяет доказать существование решения для любого набора параметров задачи. Кроме того, учитывая линейность модели, ее можно свести к эквивалентной ей, однокритериальной задаче с выпуклой линейной сверткой критериев:

$$J = \mu J_1 + (1-\mu) J_2,\ \mu \in (0;1),$$

где μ – экспертно задаваемый весовой коэффициент значимости критериев. Нетривиальные решения (1)–(2) получаются с помощью оптимизационного пакета, описанного в [13, с. 96–111]. Принятие решений по распределению инвестиций и оценке уровня ИЗИСО может основываться как на изучении зависимостей от параметра μ, так и на анализе получаемого Парето-множества модели, автоматизированные средства которого также содержатся в указанном оптимизационном пакете. Отметим, что представленную математическую модель ИЗИСО, вообще говоря, можно использовать как основу для поддержки обоснованных решений не только в сфере информационной безопасности, но и для решения задач комплексной безопасности сложных систем, по аналогии с тем, как это сделано в работах [14; 15] относительно системы поддержки принятия решений при оценке информационно-экономической безопасности организации. Для проверки работоспособности модели (1)–(2) проведем модельный вычислительный эксперимент.

Пусть имеются следующие значения входных параметров модели (1)–(2):

$$N = L = 2;\ Z = 1300 \text{ д.е.},\ Z_1 = 800 \text{ д.е.},$$

$$Z_2 = 900 \text{ д.е.};\ (b1)_1 = 0{,}55,\ (b1)_2 = 0{,}45;$$

$$(b2)_1 = 0{,}4,\ (b2)_2 = 0{,}6;\ ZMAX_1 = 700 \text{ д.е.},$$

$$ZMAX_1 = 1500 \text{ д.е.},\ ZMAX_3 = 300 \text{ д.е.},$$

$$ZMAX_4 = 400 \text{ д.е.},\ ZMIN_{1\text{-}4} = 0 \text{ д.е.}$$

Произведем расчеты при заданных входных значениях и построим графики зависимостей $J(\mu)$, придавая параметру α значения 0; 0,5; 1; 1,5; 2 (рис. 1).

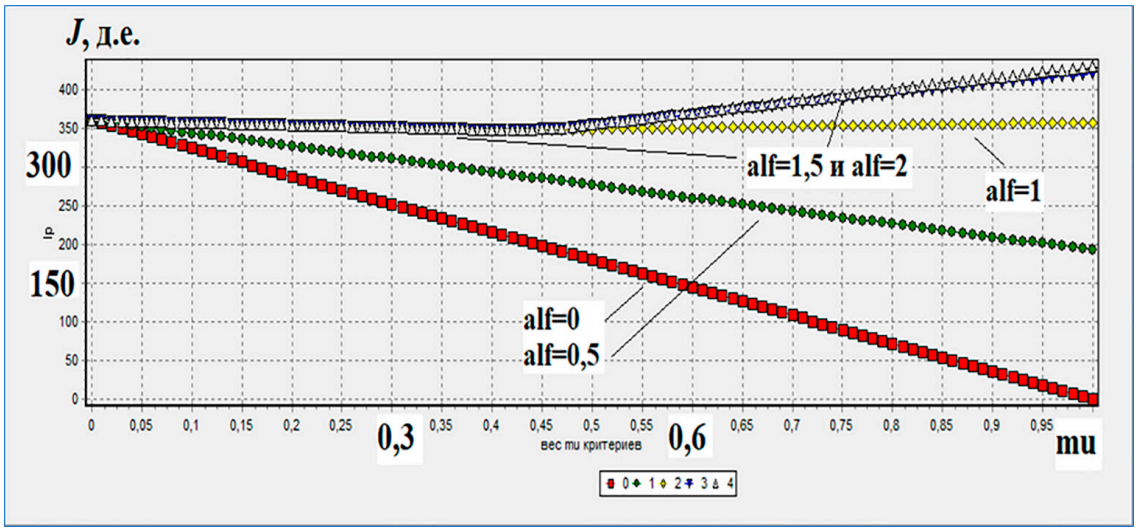

Рис. 1. Зависимости J(μ)
Примечание: составлен авторами по результатам исследования

Оптимальные решения и значения свертки критериев J

α	x_1	x_2	x_3	x_4	J
0	0	0	300	400	180
0,5	350	0	300	400	276,25
1	650	0	250	400	348,75
1,5	700	80	120	400	354,5
2	700	100	100	400	355

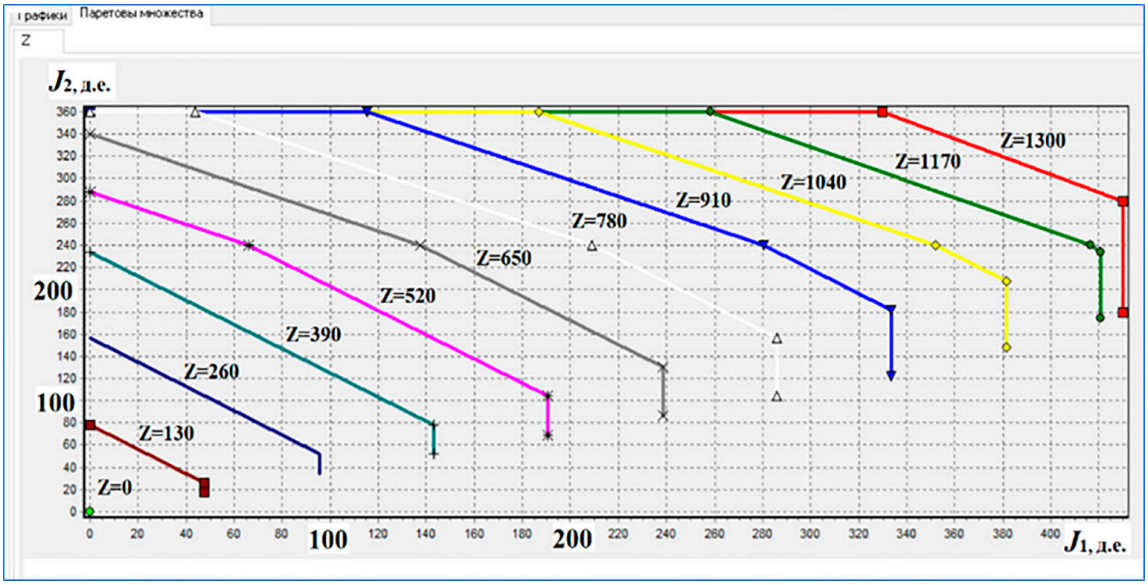

Рис. 2. Парето-множества по параметру Z при α = 2
Примечание: составлен авторами по результатам исследования

Отметим, что зависимости $J(\mu)$ совпадают при α = 1,5 и α = 2. Приведенные на рис. 1 данные свидетельствуют о нетривиальной зависимости уровня ИЗИСО по модели (1)–(2) от значений параметра α даже при небольшом количестве рассматриваемых априорных и апостериорных угроз ИБ, что, безусловно, требует дальнейшего изучения свойств и многопараметрического анализа построенной модели. В таблице приведены также оптимальные решения и соответствующие значения свертки J критериев задачи при μ = 0,5.

Как видно из таблицы, полученные оптимальные решения существенно определяются значениями параметра α и соответствуют содержательному смыслу решаемой задачи. Построим далее Парето-множества задачи (1)–(2) в зависимости от изменения параметра общих затрат Z в диапазоне от 0 до 1300 д.е. с шагом 130 д.е. и α = 2 (рис. 2).

На рис. 2 изображены Парето-множества задачи (1)–(2), причем по осям координат отложены значения каждого из критериев. Используя полученные данные, аналитик ИБ или любое другое ЛПР может определить оптимальные диапазоны изменения значений критериев J_1 и J_2 эффективности затрат на купирование априорных и апостериорных угроз ИБ. Так, например, при $Z = 130$ – $J_1 \in (0;48)$, $J_2 \in (20;80)$, при $Z = 780$ – $J_1 \in (0;285)$, $J_2 \in (100;350)$, а при $Z = 1300$ – $J_1 \in (0;550)$, $J_2 \in (180;355)$.

Заключение

Математическая модель (1)–(2) представляет собой легко интерпретируемую для использования специалистами-практиками, имеющую экономический смысл оптимального распределения ресурсов задачу линейного программирования в стандартной форме. Для ее предварительного анализа автор использовал решающий указанную задачу многопараметрический графоанализатор с возможностями графического и Парето-анализа. Совокупность данных инструментов позволяет реализовать принцип информационной, модельной и алгоритмической сбалансированности, практически необходимый для разработки эффективных автоматизированных систем поддержки принятия решений в условиях значительного количества угроз безопасности функционирования сложных систем. Благодаря идентичности подходов к оценке рисков функционирования сложных систем путем рассмотрения взвешенной комбинации затрат на мероприятия по нивелированию (снижению, устранению, уменьшению, компенсации и пр.) рисков в любой сфере человеческой деятельности, построенная в работе модель может быть применена для оценки оптимальных затрат на защиту от угроз безопасности и тем самым для повышения уровня общей безопасности в социальных, экономических, технических, информационных и других сложных системах.

Список литературы

1. Ловцов Д.А. Теория защищенности информации в эргасистемах: монография. М.: Российский государственный университет правосудия, 2021. 273 с. URL: https://www.elibrary.ru/item.asp?id=48626488 (дата обращения: 13.11.2025).

2. Клименко И.С. Информационная безопасность и защита информации: модели и методы управления. М.: ИНФРА-М, 2020. 180 с. URL: https://www.elibrary.ru/item.asp?id=41333803 (дата обращения: 13.11.2025).

3. Нестерук Л.Г., Нестерук Г.Ф., Суханов А.В., Любимов А.В. К моделированию экономических аспектов защищенности информационных систем // Вопросы защиты информации. 2008. № 2 (81). С. 40–44. URL: https://www.elibrary.ru/item.asp?id=11910821 (дата обращения: 15.11.2025).

4. Собакин И.Б. Анализ подходов к определению оптимального объема инвестиций в информационную безопасность // Труды Института системного анализа Российской академии наук. 2012. Т. 62. № 4. С. 63–68. URL: https://www.elibrary.ru/item.asp?id=19020078 (дата обращения: 15.11.2025).

5. Запечников С.В., Полякова А.С. Исследование моделей оценки оптимального объема инвестиций в информационную безопасность // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2012. № 14 (94). С. 153–168. URL: https://www.elibrary.ru/item.asp?id=18242879 (дата обращения: 16.11.2025).

6. Гончаров В.В., Мишенина О.В. Защита информации в автоматизированных системах: концептуально-математические аспекты // Правовая информатика. 2024. № 3. С. 43–57. URL: https://www.elibrary.ru/item.asp?id=74509297 (дата обращения: 16.11.2025).

7. Хлобыстова А.О., Абрамов М.В., Тулупьев А.Л. Подход наибольшего правдоподобия к задаче выявления траекторий социоинженерных атак и скомпрометированных пользователей информационных систем // Системы управления, связи и безопасности. 2019. № 3. С. 202–219. URL: https://www.elibrary.ru/item.asp?id=40081988 (дата обращения: 13.11.2025). DOI: 10.24411/2410-9916-2019-10310.

8. Дулесов А.С., Федоренко Н.С. Энтропийно-вероятностный анализ дерева событий // Научно-технический вестник Поволжья. 2023. № 6. С. 152–157. URL: https://www.elibrary.ru/item.asp?id=54034631 (дата обращения: 17.11.2025).

9. Базилевский М.П., Наседкин П.Н. Формализация модели информационной безопасности предприятия в виде многокритериальной задачи линейного программирования // Моделирование, оптимизация и информационные технологии. 2023. Т. 11. № 3 (42). С. 10–11. DOI: 10.26102/2310-6018/2023.42.3.021. URL: https://www.elibrary.ru/item.asp?id=54676384 (дата обращения: 18.11.2025).

10. Зегжда П.Д., Анисимов В.Г., Супрун А.Ф. и др. Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем // Проблемы информационной безопасности. Компьютерные системы. 2018. № 1. С. 43–47. URL: https://www.elibrary.ru/item.asp?id=35079334 (дата обращения: 17.11.2025).

11. Федорец А.Г. Новый метод оценки рисков, основанный на неопределенности // Безопасность и охрана труда. 2025. № 1 (102). С. 4–7. URL: https://www.elibrary.ru/item.asp?id=80506739 (дата обращения: 17.11.2025).

12. Медведев А.В. Оптимизационная математическая модель информационной безопасности // Научные исследования в современном мире. Теория и практика: сборник избранных статей Всероссийской (национальной) научно-практической конференции. СПб.: ГНИИ «НАЦРАЗВИТИЕ», 2021. С. 66–68. URL: https://www.elibrary.ru/item.asp?id=47143603 (дата обращения: 13.11.2025).

13. Медведев А.В. Автоматизированная поддержка принятия оптимальных решений в инвестиционно-производственных проектах развития социально-экономических систем: монография. М.: Издательский Дом «Академия Естествознания», 2020. 200 с. URL: https://www.elibrary.ru/item.asp?id=44108542 (дата обращения: 13.11.2025). DOI: 10.17513/np.421.

14. Медведев А.В., Киренберг А.Г., Прокопенко Е.В., Кисляков И.М., Ромашкин В.Д. Применение системы поддержки принятия инвестиционных решений в оценке информационно-экономической безопасности организации // Научно-технический вестник Поволжья. 2024. № 4. С. 298–303. URL: https://www.elibrary.ru/item.asp?id=67203059 (дата обращения: 17.11.2025).

15. Kirenberg A., Medvedev A., Prokopenko E. A mathematical model of information security for a mining company // E3S Web of Conferences (Kemerovo, 19–21 Oct. 2020). Kemerovo, 2020. P. 04012. [Электронный ресурс]. URL: https://www.elibrary.ru/item.asp?id=44046713 (дата обращения: 13.11.2025). DOI: 10.1051/e3sconf/202017404012.

Конфликт интересов: Автор заявляет об отсутствии конфликта интересов.

Conflict of interest: The author declares that there is no conflict of interest.