ORIGINAL PAPER
Modern technologies. System analysis. Modeling *2025. No. 2 (86). pp. 131–144*
DOI 10.26731/1813-9108.2025.2(86).131-144 **УДК** 519.6: 311

Сравнительный анализ показателей эффективности в виде рисков при проведении работ по устранению инцидентов информационной безопасности

Ю.М. Краковский✉, В.П. Киргизбаев
Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация
✉yuri.krakovskiy@yandex.ru

Резюме
Исследование посвящено сравнительному анализу показателей эффективности в виде рисков при проведении работ по устранению инцидентов информационной безопасности на основе результатов дискретно-имитационного моделирования. Объектом изучения является моделирование экономических аспектов информационной безопасности различных соответствующих систем организаций. Это связано с тем, что защищенность таких информационных систем осуществляется, как правило, при ограниченных финансовых ресурсах. Предметом исследования служит математическое, алгоритмическое и программное обеспечение для вычисления показателей эффективности в виде рисков, характеризующих защищенность информационных систем организаций. В статье получили развитие предложения авторов, представленные в предыдущих публикациях, а именно: а) по мере необходимости производится оплата работ, связанных с устранением инцидентов (денежный поток по расходам); б) осуществляется накопление платежей в определенном периоде с установленной их стоимостью (денежный поток по доходам). Эти потоки взаимодействуют между собой, создавая результирующий процесс, описывающий состояние фонда в момент времени *t*. В качестве его математической модели предлагается случайный дискретный нестационарный процесс специального вида. Нестационарность заключается в том, что какая-то доля реализаций данного процесса за время моделирования не пересекает ось времени *t*, а другая – пересекает. В этом случае вследствие взаимодействия регулярных и случайных денежных потоков проявляется важнейшее свойство сложных систем – эмерджентность. Время, когда в фонде закончились деньги на оплату работ, названо временем его обнуления. В качестве рисков обозначены: однофакторный риск в виде вероятности обнуления фонда; однофакторный финансовый риск в виде математического ожидания случайных величин, связанных с обнулением; два вида двухфакторных финансовых рисков, также сопряженных с обнулением фонда. Предложенное математическое обеспечение и указанные модели рисков реализованы в виде программного обеспечения (разработанного с использованием языка программирования Python), ядром которого является специальная программа на основе дискретно-имитационного моделирования. С помощью созданного программно-математического обеспечения проведен сравнительный анализ отмеченных рисков.

Ключевые слова
информационные системы организаций, моделирующая программа, однофакторные и двухфакторные риски, инциденты информационной безопасности, показатели эффективности

Для цитирования
Краковский Ю.М. Сравнительный анализ показателей эффективности в виде рисков при проведении работ по устранению инцидентов информационной безопасности / Ю.М. Краковский, В.П. Киргизбаев // Современные технологии. Системный анализ. Моделирование. 2025. № 2 (86). С. 131–144. DOI 10.26731/1813-9108.2025.2(86).131-144.

Информация о статье
поступила в редакцию: 14.05.2025 г.; поступила после рецензирования: 21.05.2025 г.; принята к публикации 22.05.2025 г.

Comparative Analysis of Risk-Based Performance Indicators in Information Security Incident Remediation

Yu.M. Krakovskii✉, V.P. Kirgizbaev
Irkutsk State Transport University, Irkutsk, the Russian Federation
✉yuri.krakovskiy@yandex.ru

Abstract
This study presents a comparative analysis of efficiency indicators expressed as risks during incident-response activities in information security, based on results obtained through discrete-event simulation. The research focuses on modelling the economic aspects of information security for a variety of organizational information systems, recognizing that protection is typically implemented under constrained financial resources. It addresses the mathematical, algorithmic and software tools used to calculate risk-based efficiency indicators that characterize an information systems' security posture. Based on the authors' earlier work, the

paper proposes managing a monetary fund that both pays, whenever necessary, for tasks related to incident remediation creating an outflow cash stream and periodically accumulates fixed-amount payments, thereby generating an inflow cash stream. Interaction between these two streams yields a resultant process that describes the fund's state at any moment in time *t*. This behavior is modelled as a special random, discrete, non-stationary process. Non-stationarity is demonstrated by the fact that, over the simulation horizon, some realizations never cross the time axis while others do. Owing to the interplay between regular and random cash flows, the fund acquires an emergent property typical of complex systems: it exhibits characteristics absent from its individual components when considered in isolation. The instant at which the fund's balance reaches zero is defined as the time of depletion. Several risk metrics related to this event are introduced, namely a single-factor risk that captures the probability of depletion, a single-factor financial risk defined as the expected value of random variables associated with depletion, and two variants of two-factor financial risks that are likewise tied to fund depletion. The proposed mathematical framework and risk models have been implemented in software centered on a discrete-event simulation program written in Python. Using this integrated software–mathematical platform, the study conducts a comparative analysis of the proposed risks and offers both scientific insights and practical recommendations.

Keywords
organizational information systems, simulation program, single-factor and two-factor risks, information security incidents, performance indicators

For citation
Krakovskii Yu.M., Kirgizbaev V.P. Sravnitel'nyi analiz pokazatelei effektivnosti v vide riskov pri provedenii rabot po ustraneniyu intsidentov informatsionnoi bezopasnosti [Comparative Analysis of Risk-Based Performance Indicators in Information Security Incident Remediation]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [Modern Technologies. System Analysis. Modeling], 2025. Vol. 86. No. 2. Pp. 131–144. DOI: 10.26731/1813-9108.2025.2(86).131-144.

Article info
Received: May 14, 2025; Revised: May 21, 2025; Accepted: May 22, 2025.

Введение

В последние годы в нашей стране большое внимание уделяется цифровизации экономики, внедрению искусственного интеллекта (ИИ) в различные отрасли промышленности. Создается, развивается и внедряется импортозамещающая продукция на основе современных технологий. Все это, в свою очередь, предъявляет повышенные требования к средствам защиты информации, присутствующим в различных информационных системах организаций (ИСО). Средства информационной безопасности защищают ИСО от широкого диапазона различных угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации рисков, получения максимальной отдачи от инвестиций [1–3].

Так, в работе [3] подчеркивается, что в условиях глобальной цифровизации объем циркулирующих данных стремительно растет, что повышает вероятность несанкционированного доступа к ним и последующих финансовых, правовых и репутационных потерь для владельцев информационных систем. Авторы отмечают, что, несмотря на совершенствование защитных технологий, число кибератак продолжает увеличиваться, а уязвимости корпоративных и государственных систем остаются значительными. Для повышения устойчивости информационных систем авторы рекомендуют внедрять непрерывный мониторинг, проводить регулярный анализ угроз и уязвимостей.

К инфраструктуре цифровой экономики относится большое количество новейших информационных и коммуникационных технологий, а именно: облачные вычисления для обеспечения удобного сетевого доступа к вычислительным ресурсам; автоматизация обработки больших данных; технологии распределенных вычислений; программные и аппаратные средства, имитирующие интеллектуальную деятельность человека (ИИ, машинное обучение) и др. [4–6]. Сюда же относятся и вопросы информационной безопасности, которые так или иначе присутствуют во всех современных информационных и коммуникационных технологиях. Это, в частности, выводит проблему информационной безопасности за рамки, к примеру, научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», делая ее, по существу, общезначимой для любых информационных технологий. Общие, системные вопросы информационной безопасности, не связанные с конкретными объектами и средствами, целесообразно рассматривать в рамках специальности 2.3.1 «Системный анализ, управление и обработка информации, статистика». С этих позиций излагается предлагаемый материал.

В данной работе объектом исследования является моделирование экономических аспектов информационной безопасности ИСО. Это связано с тем, что их защищенность осуществляется обычно при ограниченных финансовых ресурсах, поэтому этим аспектам уделяется большое внимание в литературе [2, 7–9].

Также в России актуализуются отрасли, связанные с импортозамещением продукции [10, 11], с отечественными вариантами инновационных технологий и ИИ [12–15]. Такое развитие отраслей промышленности требует внедрения различных мер защиты информации. Обеспечение защищенности ИСО сопряжено с предотвращением инцидентов, которые могут нанести ущерб организации посредством нарушения конфиденциальности, целостности и доступности информации.

Согласно ГОСТ Р 59712–2022, компьютерный инцидент – это факт нарушения и (или) прекращения функционирования информационного ресурса, в том числе произошедший в результате компьютерной атаки. Он является подмножеством инцидентов информационной безопасности (непредвиденное или нежелательное событие, группа событий), характеризующихся подтвержденным фактом нарушения и (или) прекращения функционирования информационного ресурса [2].

Предмет исследования – математическое, алгоритмическое и программное обеспечение для вычисления показателей эффективности в виде рисков по результатам дискретно-имитационного моделирования, характеризующих защищенность ИСО.

Статья является продолжением публикаций авторов [16–18], в которых предлагается использовать денежный фонд (ДенФ) со следующими функциями:

– по мере необходимости производится оплата работ по устранению инцидентов, когда для каждого вида деятельности определяется периодичность использования фонда (сут.) и стоимость (тыс. руб.) (денежный поток по расходам);

– осуществляется накопление платежей в определенный период (сут.) и с установленной величиной их стоимости (тыс. руб.) (денежный поток по доходам).

Эти потоки взаимодействуют между собой, создавая результирующий процесс, описывающий состояние фонда в момент времени *t*.

Для моделирования процесса, описывающего состояние этого фонда, предложен имитационный подход, предполагающий создание моделирующей программы с целью получения необходимых выборочных значений, которые затем обрабатываются статистическими методами для вычисления и визуализации предложенных показателей эффективности в виде рисков.

Цель исследования – сравнительный анализ показателей эффективности в виде рисков при проведении работ по устранению инцидентов информационной безопасности на основе результатов дискретно-имитационного моделирования.

Математическая модель для моделирования состояния денежного фонда

В качестве математической модели, описывающей состояние ДенФ, предлагается случайный дискретный нестационарный процесс вида:

$$Fs(t) = F_{S_0} + \sum_{l=1}^{L} Y_l(t) - \sum_{j=1}^{m} Z_j(t), \text{ тыс. руб.,} \quad (1)$$

где $Y_l(t)$ – суммарная величина доходов по платежам l-го вида за время t, тыс. руб.; L – число видов платежей по пополнению ДенФ; $Z_j(t)$ – суммарная величина расходов для j-й работы за время t, тыс. руб.; m – число видов работ по устранению инцидентов информационной безопасности; F_{S_0} – начальное значение процесса $Fs(t)$, тыс. руб. [18].

Величину F_{S_0} предлагается задавать в долях от величины средних годовых расходов:

$$F_{S_0} = g \cdot X \text{, тыс. руб.,}$$

где X – средние финансовые средства (тыс. руб.), необходимые для выполнения годового объема всех работ (расходы); g – коэффициент. Учитывая рекомендации теории рисков [19], $g > 0$.

Нестационарность процесса (1) заключается в том, что какая-то доля его реализаций за время моделирования (T_m, сут.) не пересекает ось времени t, а другая – пересекает. В данном случае вследствие взаимодействия регулярных и случайных денежных потоков проявляется важнейшее свойство сложных систем, называемое эмерджентностью [20] (появление у системы свойств, которые отсутствуют у ее компонентов вследствие их взаимодействия).

Модели показателей эффективности в виде рисков

Введем важнейшее понятие данной работы, а именно – время обнуления ДенФ. Для этого нам понадобится время, когда в фонде закончились деньги на оплату работ s (сут.). Оно и будет временем обнуления ДенФ. Введем случайную величину S, для которой определяется время s. Тогда $(S < S_t)$ – негативное случайное событие, заключающееся в том, что обнуление ДенФ произошло на интервале $(0, S_t)$, сут.

Время обнуления возникает в связи с тем, что случайный процесс (1), характеризующий состояние ДенФ, является нестационарным, поэтому некоторые реализации процесса пересекают ось времени (значение реализации процесса в момент времени s становится отрицательным). Для таких процессов вероятность $P(S < \infty) < 1$.

Рассмотрим два варианта технологии определения времени обнуления ДенФ:

Вариант А: s – время, когда первый раз значение $Fs(t) < 0$ (произошло обнуление ДенФ), процесс моделирования реализации процесса (1) прекращается:

$$s = \min_t (t: Fs(t) < 0), \text{ сут.} \quad (2)$$

При имитационном моделировании с помощью созданной моделирующей программы для времени s образуется упорядоченная по возрастанию выборка объема n:

$$T_s = (s_1, \dots, s_i, \dots, s_n), \quad (3)$$

где i – номер элемента выборки (номер реализации процесса (1), для которой произошло обнуление ДенФ).

Вариант В, когда выполнилось условие (2) и до конца месяца даже при поступлении каких-то платежей значение $Fs(t) < 0$, то считаем, что в момент времени (2) произошло обнуление ДенФ. Формируется выборка (3), процесс моделирования реализации (1) прекращается (рис. 1).

Если до конца месяца за счет поступлений значение функции $Fs(t)$ стало больше нуля, то величину s не учитываем (обнуление ДенФ не произошло). Моделирование реализации процесса (1) продолжается. Для варианта В предполагается, что оплату работ можно осуществлять с задержкой, но оплата должна произойти в течение текущего месяца за счет поступлений.

Вероятность обнуления ДенФ до времени S_t:

$$p_t = P(S < S_t), \quad (4)$$

предлагается в качестве показателя эффективности (в теории рисков величина (4) – это однофакторная модель риска).

Необходимо так организовать поступление денежных платежей в фонд, чтобы при появлении инцидентов информационной безопасности и проведения работ по их устранению однофакторный риск (4) был минимален.

При имитационном моделировании показатель (4) заменяется на точечную $(\tilde{R}_\tau)$ и интервальную (τ_1, τ_2) оценки:

$$\tilde{R}_\tau = k_\tau / n_0, \quad (5)$$

где k_τ – число реализаций процесса (1), для которых создается точечная оценка (5); n_0 – число моделируемых реализаций процесса (1).

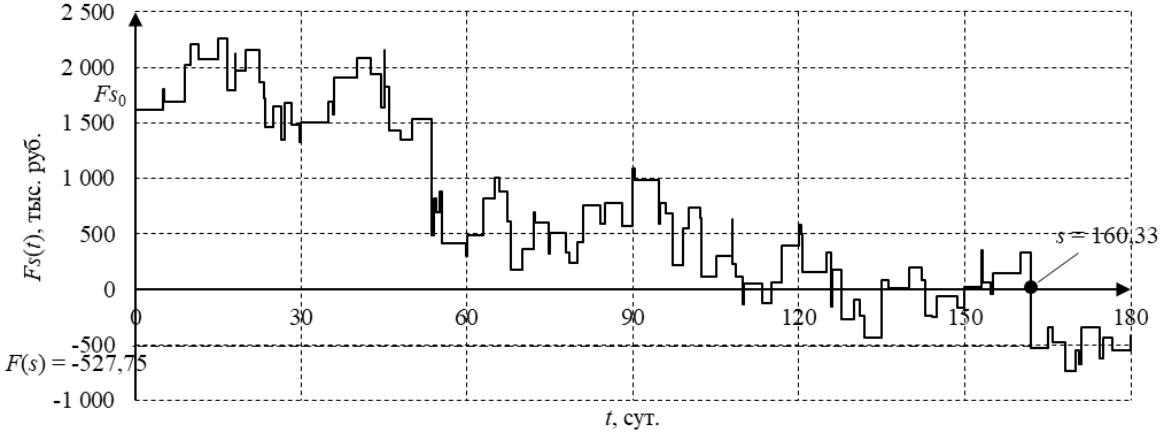

Рис. 1. График реализации с «обнулением» денежного фонда при технологии определения времени обнуления B

Fig. 1. Graph of the implementation with «zeroing» of the monetary fund under «zeroing» determination technology B

Это значение должно обеспечить необходимую точность моделирования. Определение интервальной оценки (τ_1, τ_2) можно посмотреть в [16].

Приведем показатели эффективности в виде однофакторных финансовых рисков, которые измеряются в рублях:

1. Финансовый риск по расходам –

$$RD = M[Dr], \text{ тыс. руб.,} \quad (6)$$

где Dr – случайная величина, характеризующая итоговые расходы фонда до времени его обнуления; $M[Dr]$ – математическое ожидание этой величины.

2. Финансовый риск по поступлениям –

$$RU = M[Du], \text{ тыс. руб.,} \quad (7)$$

где Du – случайная величина, характеризующая итоговые поступления в фонд до времени его обнуления; $M[Du]$ – математическое ожидание этой величины [17].

При имитационном моделировании риски (6) и (7) заменим на точечные и интервальные оценки. Точечная оценка величины (6), характеризующая средние расходы на интервале $(0, S_t)$:

$$RD_0 = \sum_{i=1}^{k_\tau} d_i / k_\tau , \quad (8)$$

где d_i – значение расходов по всем работам до времени s_i:

$$d_i = \sum_{j=1}^{m} Z_j(s_i), \quad (9)$$

где $Z_j(s_i)$ – величина из модели (1).

Точечная оценка величины (7), характеризующая средние поступления на интервале $(0, S_t)$:

$$RU_0 = \sum_{i=1}^{k_\tau} u_i / k_\tau , \quad (10)$$

где u_i – значение поступлений по всем видам платежей до времени s_i:

$$u_i = F_{S_0} + \sum_{l=1}^{L} Y_l(s_i),$$

где $Y_l(s_i)$ – величина из модели (1).

Определение интервальных оценок рисков (6) и (7) можно посмотреть в [17].

Следует отметить, что разность между точечными оценками рисков (8) и (10) равна:

$$RD_0 - RU_0 = -\sum_{i=1}^{k_\tau} F_s(s_i) \Big/ k_\tau , \quad (11)$$

где $Fs(s_i)$ – значение процесса (1) в момент обнуления ДенФ; s_i – выборочное значение (3).

Так как значения $Fs(s_i)$ отрицательные (см. рис. 1), то перед суммой стоит знак минус. Подчеркнем, что формула (11) справедлива для обеих технологий обнуления фонда.

Из нее вытекает, что точечные оценки финансовых рисков (8) и (10) дублируют друг друга, значение RD_0 всегда больше значения RU_0 на правую часть (11). Авторы рекомендуют использовать из этих двух однофакторных финансовых рисков финансовый риск по расходам (6), потому что именно расходы связаны с оплатой работ по устранению инцидентов и событий информационной безопасности.

Для оценки эффективности работ по устранению инцидентов помимо однофакторных финансовых рисков предложены двухфакторные риски двух видов. Рассмотрим первый вид:

$$RD2 = M[p_0 \cdot D_r], \text{ тыс. руб.;} \quad (12)$$

$$RU2 = M[p_0 \cdot D_u], \text{ тыс. руб.} \quad (13)$$

Здесь p_0 – вероятность обнуления ДенФ до времени s_i (4); Dr и Du – случайные величины, описанные ранее; $M[\cdot]$ – математическое ожидание произведения величин.

Учитывая изложенную рекомендацию, будем рассматривать риск (12) (экспериментально показано, что риски (12) и (13) дублируют друг друга).

Введем выборку Q оценок вероятности p_0 (q_i) для i-й реализации процесса (1) после упорядочивания по возрастанию выборки (3):

$$Q = (q_1, \ , q_i, \ , q_n), q_i = i / n_0. \quad (14)$$

Среднее значение оценки вероятности p_0 на интервале $(0, S_t)$ равно:

$$q_0 = \sum_{i=1}^{k_\tau} q_i \Big/ k_\tau = (k_\tau + 1)/(2 \cdot n_0).$$

Введем дополнительно выборку:

$$D2 = (q_1 \cdot d_1, \ldots, q_i \cdot d_i, \ldots, q_n \cdot d_n).$$

Здесь d_i – величина (10); q_i – величина (14).

При имитационном моделировании риск (12) заменим на точечную и интервальную оценки: $RD2_0$ – точечная оценка величины $RD2$ на интервале $(0, S_t)$:

$$RD2_0 = \sum_{i=1}^{k_\tau} q_i \cdot d_i \Big/ k_\tau . \quad (15)$$

Определение интервальной оценки величины (12) можно посмотреть в [18].

Рассмотрим второй вид двухфакторных финансовых рисков на примере расходов:

$$PD0 = p_0 \cdot RD, \quad (16)$$

где p_0 и RD – величины (4) и (6) соответственно.

Подчеркнем, что финансовый риск (12) – это математическое ожидание произведения этих величин, а риск (16) – произведение вероятности обнуления на математическое ожидание.

При имитационном моделировании риск (16) заменим на точечную и интервальную оценки: RPD_0 – точечная оценка величины $PD0$ на интервале $(0, S_t)$:

$$RPD_0 = \tilde{R}_\tau \cdot RD_0 = \sum_{i=1}^{k_\tau} d_i \Big/ n_0 \ . \qquad (17)$$

где $\tilde{R}_\tau$, RD_0 – величины (5) и (8); (RPD_1, RPD_2) – интервальная оценка величины $PD0$ [21]:

$$RPD_\Delta = z_\gamma \sqrt{\left(\tilde{R}_\tau \cdot \sigma_d^2 + \tilde{R}_\tau \cdot \left(1 - \tilde{R}_\tau\right) \cdot RD_0^2\right) \Big/ n_0} \ , \qquad (18)$$

$$RPD_1 = RPD_0 - RPD_\Delta, \qquad (19)$$

$$RPD_2 = RPD_0 + RPD_\Delta, \qquad (20)$$

где σ_d – оценка среднеквадратического отклонения величины Dr на интервале $(0, S_t)$; z_γ = 1,96 – критическое значение (квантиль) статистики Z (нормированное нормальное распределение) при доверительной вероятности $\gamma = 0{,}95$.

Чтобы обосновано использовать формулы для доверительных интервалов (интервальной оценки) (18)–(20), надо показать, что случайная величина $PD0$ имеет нормальный закон. Именно в этом случае можно использовать в формулах квантиль z_γ. Для этого необходимо создать по величине (17) выборочные значения. Эти значения для примера найдем при g = 0,04 и S_t = 365 сут., для чего проведем 1 000 моделирований при разных начальных значениях генератора случайных чисел (каждое моделирование требует создания 20 000 реализаций процесса (1)).

Полученная гистограмма плотности распределения вероятностей с наложенной кривой нормального распределения приведена на рис. 2.

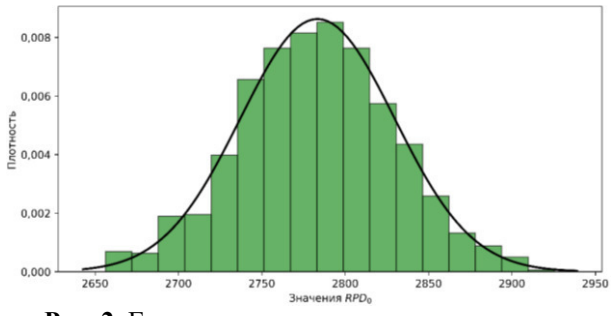

Рис. 2. Гистограмма плотности распределения с кривой нормального распределения для $PD0$
Fig. 2. Probability density histogram with a normal distribution curve for $PD0$

Сформулируем нулевую и альтернативную гипотезы для проверки распределения этой величины. Нулевая гипотеза (H_0): генеральная совокупность значений величины $PD0$ имеет нормальное распределение. Альтернативная гипотеза (H_1): генеральная совокупность значений величины $PD0$ не имеет нормальное распределение.

Для проверки этих гипотез применим статистический тест Шапиро – Уилка [22], уровень значимости α = 0,05. Получены следующие результаты: значение статистики W = 0,9982; p = 0,3888. Данные значения получены с использованием функции shapiro из подмодуля scipy.stats библиотеки SciPy языка программирования Python.

Так как $p > 0{,}05$, то нулевую гипотезу (H_0) можно принять. Таким образом, экспериментально показано, что в формуле (18) можно использовать квантиль z_γ.

Апробация созданного математического и программного обеспечения

Предложенное математическое обеспечение и сценарии рисков реализованы в виде программного обеспечения, ядром которого является программа, созданная на основе дискретно-имитационного моделирования [23]. Программное обеспечение разработано с использованием языка программирования Python [24].

Апробацию проведем для пяти видов работ (m = 5), приведенных в статье [17]. Исходные данные для описания вероятностных моделей, необходимых для моделирования затрат на выполнение работ, возьмем из статьи [18] (табл. 1). Учитывались следующие показатели:

1. Вероятностные модели для интервалов (Н, Б, Рв) и вероятностные модели для затрат (Лн, Б-С, П, Г), где «Н» – нормальное распределение; «Б» – бета-распределение; «Рв» – равномерное распределение; «Лн» – логнормальное распределение; «Б-С» – распределение Бирнбаума-Саундерса; «П» – распределение Парето с нулевой точкой; «Г» – гамма-распределение (возможно изменение этих моделей).

2. mt, mz – значения математические ожидания соответственно для интервалов и затрат, а kvt, kvz – коэффициенты вариации для интервалов и затрат (табл. 1).

Для значений из табл. 1 общие средние расходы, необходимые для выполнения годового объема всех работ, равны X = 26 931,26 тыс. руб.

В табл. 2 и 3 приведены результаты моделирования показателей эффективности для двух вариантов поступления платежей (V). Значения показателей (4), (12) и (16) для хорошего варианта должны быть минимальными, а значения показателя (7) – максимальными. Также приведем относительные погрешности в процентах (21)–(24):

$$\Delta_\tau = (\tau_2 - \tau_1) \cdot 100/(2 \cdot \tilde{R}_\tau), \quad (21)$$

$$\Delta_{RD} = (RD_2 - RD_1) \cdot 100/(2 \cdot RD_0), \quad (22)$$

$$\Delta_{RD2} = (RD2_2 - RD2_1) \cdot 100/(2 \cdot RD2_0), \quad (23)$$

$$\Delta_{RPD} = (RPD_2 - RPD_1) \cdot 100/(2 \cdot RPD_0). \quad (24)$$

Из табл. 2 и 3 видно, что вариант $F1$ с точки зрения показателей эффективности предпочтительнее варианта $F2$, так как доверительные интервалы этих показателей почти нигде не пересекаются (исключение составляет незначительное пересечение для показателя (6) при S_t = 91 сут.).

В данной статье при апробации рассматриваются два вида платежей (L = 2), когда доли платежей c_1 = 0,5, c_2 = 0,5. Исследуются два варианта:

1. $F1$, когда интервалы времени между платежами h_1 = 5 сут. и h_2 = 9 сут., соответственно значения единичных платежей $Y_{0\,1}$ = 184,46 тыс. руб. и $Y_{0\,2}$ = 332,03 тыс. руб.

2. $F2$, когда интервал времени между платежами h_1 = 7 сут. и h_2 = 11 сут., а значения единичных платежей $Y_{0\,1}$ = 258,24 тыс. руб. и $Y_{0\,2}$ = 405,81 тыс. руб.

Будем использовать вариант В технологии определения времени обнуления ДенФ. Начальное значение F_{S_0} вычисляется при g = 0,02. Число реализаций при моделировании равно 100 000.

Таблица 1. Вероятностные модели и их числовые характеристики
Table 1. Probabilistic models and their numerical characteristics

Показатели Indicators	Значения математических ожиданий и коэффициентов вариации в соответствии с номером работы Values of mathematical expectations and coefficients of variation according to the work number				
	1	2	3	4	5
Вероятностные модели для интервалов Probability models for intervals	Н	Б	Рв	Б	Н
mt_j, сут.	18,0	24,0	28,0	6,0	22,0
kvt_j	0,20	0,10	0,10	0,10	0,10
Вероятностные модели для затрат Probabilistic models for costs	Лн	Б-С	П	Лн	Г
mz_j, тыс. р.	380,0	340,0	200,0	120,0	250,0
kvz_j	0,15	0,20	1,25	0,25	0,15

Таблица 2. Результаты моделирования для показателей (4) и (6)
Table 2. Simulation results for indicators (4) and (6)

V	S_t, сут.	k_τ	$\tilde{R}_\tau$	τ_1	τ_2	Δ_τ, %	RD_0	RD_1	RD_2	Δ_{RD}, %
$F1$	91	4 719	0,0472	0,0461	0,0483	2,3479	5 009,32	4 963,54	5 055,09	0,91
	182	13 078	0,1308	0,1290	0,1325	1,3448	8 742,13	8 686,54	8 797,71	0,64
	273	19 975	0,1998	0,1977	0,2018	1,0436	11 790,10	11 720,07	11 860,13	0,59
	365	25 676	0,2568	0,2545	0,2590	0,8869	14 533,08	14 449,40	14 616,75	0,58
$F2$	91	8 480	0,0848	0,0834	0,0863	1,7147	4 927,11	4 888,32	4 965,91	0,79
	182	20 894	0,2089	0,2068	0,2111	1,0145	8 388,39	8 342,23	8 434,56	0,55
	273	28 858	0,2886	0,2862	0,2909	0,8184	11 135,19	11 073,23	11 197,15	0,56
	365	34 710	0,3471	0,3446	0,3496	0,7148	13 454,2	13 378,91	13 529,48	0,56

Таблица 3. Результаты моделирования для показателей (12) и (16)
Table 3. Simulation results for indicators (12) and (16)

V	S_t, сут.	k_τ	$RD2_0$	$RD2_1$	$RD2_2$	Δ_{RD2}, %	RPD_0	RPD_1	RPD_2	Δ_{RPD}, %
$F1$	91	4 719	138,17	135,14	141,19	2,19	236,39	229,46	243,32	2,93
	182	13 078	690,59	681,49	699,69	1,32	1 143,30	1 123,63	1 162,96	1,72
	273	19 975	1 465,81	1 449,06	1 482,56	1,14	2 355,07	2 322,68	2 387,47	1,38
	365	25 676	2 369,64	2 344,80	2 394,49	1,05	3 731,51	3 686,68	3 776,35	1,20
$F2$	91	8 480	250,61	246,46	254,76	1,66	417,82	408,70	426,94	2,18
	182	20 894	1 077,11	1 065,41	1 088,81	1,09	1 752,67	1 729,44	1 775,91	1,33
	273	28 858	2 047,97	2 027,39	2 068,55	1,00	3 213,39	3 177,37	3 249,42	1,12
	365	34 710	3 041,91	3 012,71	3 071,10	0,96	4 669,95	4 622,42	4 717,48	1,02

Относительные погрешности вычисления точечных оценок для показателей достаточно небольшие (меньше 2 %, кроме случаев при S_t = 91 сут.). При этом для варианта $F1$ погрешность немного больше, чем для $F2$. Это связано с тем, что для «хорошего» варианта ($F1$) объем выборки (k_τ) меньше.

Результаты моделирования позволяют сделать вывод, что интервалы времени между поступлениями желательно уменьшать.

Риски (12) и (16) дублируют друг друга, при этом риск (16) больше риска (12). Найдем разность их точечных оценок:

$$RPD_0 - RD2_0 = \sum_{i=1}^{k_\tau} (1 - i/k_\tau) d_i \Big/ n_0 > 0. \quad (25)$$

Это связано с тем, что $d_i > 0$ и $(1 - i/k_\tau) > 0$ (при $k_\tau \geq 2$).

Из (25) вытекает, что при выборе показателей эффективности (среди двухфакторных финансовых рисков) для сравнения вариантов поступления платежей можно взять любой из них. Авторы рекомендуют риск (12), так как для него проще найти доверительный интервал.

Рассмотрим зависимости показателей эффективности от коэффициента g для варианта $F1$, обнуление по варианту В.

Зависимости $\tilde{R}_\tau(g)$ от g

Проведем аппроксимацию экспериментальных значений $\tilde{R}_\tau(g)$ (5), полученных имитационным моделированием, функцией вида:

$$y_{\tilde{R}\tau}(g) = A \cdot e^{-a \cdot g}. \quad (26)$$

Отметим, что для нее $y_{\tilde{R}\tau}(0) = A$.

На рис. 3 и 4 приведены экспериментальные значения и графики функций (26), которые их аппроксимируют для различных S_t.

При S_t = 182 сут. получены следующие значения параметров: A = 0,3764; a = 52,9243; коэффициент детерминации 0,9999. При S_t = 365 сут.: A = 0,5309; a = 37,1426; коэффициент детерминации 0,9994. Как видим, наблюдается хорошая точность аппроксимации для обоих случаев.

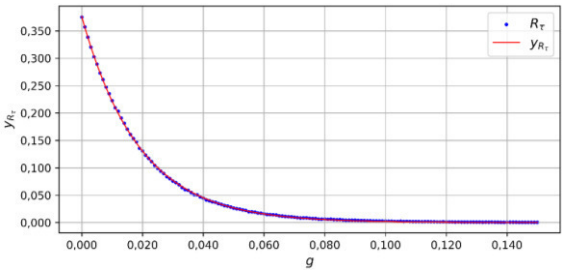

Рис. 3. Аппроксимация $\tilde{R}_\tau(g)$ функцией (26) для S_t = 182 сут.
Fig. 3. Approximation of $\tilde{R}_\tau(g)$ with function (26) for S_t = 182 days

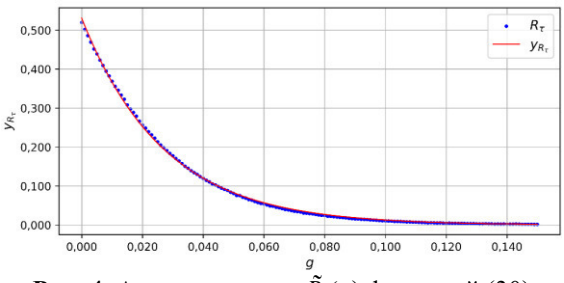

Рис. 4. Аппроксимация $\tilde{R}_\tau(g)$ функцией (30) для S_t = 365 сут.
Fig. 4. Approximation of $\tilde{R}_\tau(g)$ with function (30) for S_t = 365 days

Значения функции $y_{\tilde{R}\tau}(0)$ на рисунках соответствуют значениям коэффициента A.

По функции (26) можно определять значение g_m, когда эта функция равна r_m – заданному уровню вероятности. Это значение можно использовать как максимальное при построении других аппроксимационных зависимостей.

Из уравнения (27)

$$A \cdot e^{-a \cdot g_m} = r_m \quad (27)$$

получим:

$$g_m = \ln\left(A/r_m\right)/a. \quad (28)$$

Пусть r_m = 0,1, тогда, используя (28), при S_t = 182 сут. g_m = 0,025; при S_t = 365 сут. g_m = 0,045. Эти значения показывают, что для нормального функционирования ДенФ совсем не обязательно использовать большое начальное значение F_{S_0}.

Зависимости RD_0 от g

Проведем аппроксимацию экспериментальных значений $RD_0(g)$ (8), полученных имитационным моделированием, функцией вида:

$$y_{RD_0}(g) = A \cdot \ln(g + a) + b. \quad (29)$$

Отметим, что для нее $y_{RD0}(0) = A \cdot \ln(a + b)$.

На рис. 5 и 6 приведены экспериментальные значения и графики функций (33), которые их аппроксимируют для различных S_t.

При S_t = 182 сут. получены следующие значения параметров: A = 2 726,22; a = 0,0155; b = 17 849,66; $y_{RD0}(0)$ = 6 489,73 (соответствует значению на рис. 5); коэффициент детерминации 0,9995. При S_t = 365 сут.: A = 6 476,59; a = 0,0200; b = 35 419,88; $y_{RD0}(0)$ = 10 083,31 (соответствует значению на рис. 6); коэффициент детерминации 0,9995. Как видим, наблюдается хорошая точность аппроксимации для обоих случаев.

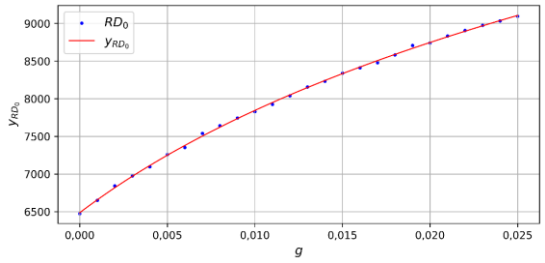

Рис. 5. Аппроксимация $RD_0(g)$ функцией (29) для S_t = 182 сут.
Fig. 5. Approximation of $RD_0(g)$ with function (29) for S_t = 182 days

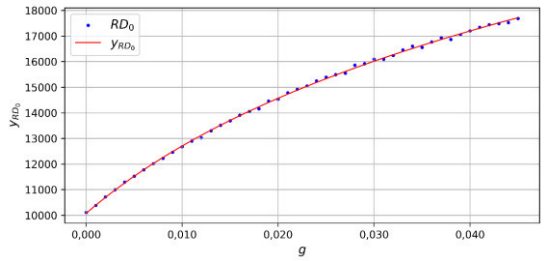

Рис. 6. Аппроксимация $RD_0(g)$ функцией (29) для S_t = 365 сут.
Fig. 6. Approximation of $RD_0(g)$ with function (29) for S_t = 365 days

Зависимости $RD2_0$ от g

Проведем аппроксимацию экспериментальных значений $RD2_0(g)$ (15), полученных имитационным моделированием, функцией вида:

$$y(g) = A \cdot (g + b) \cdot e^{-a \cdot g}. \quad (30)$$

Отметим, что для нее $y(0) = A \cdot b$.

На рис. 7 и 8 приведены экспериментальные значения и графики функций (30), которые их аппроксимируют для различных S_t.

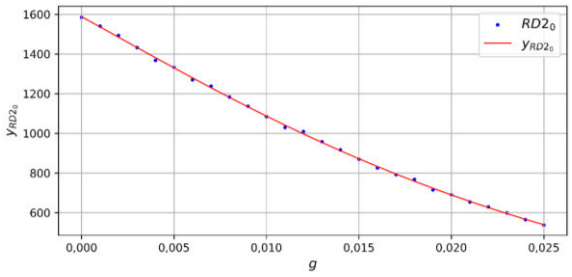

Рис. 7. Аппроксимация $RD2_0(g)$ функцией (30) для S_t = 182 сут.
Fig. 7. Approximation of $RD2_0(g)$ with function (30) for S_t = 182 days

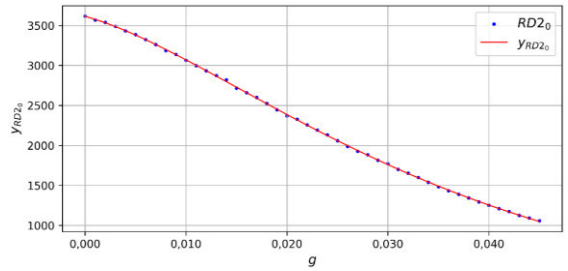

Рис. 8. Аппроксимация $RD2_0(g)$ функцией (30) для S_t = 365 сут.
Fig. 8. Approximation of $RD2_0(g)$ with function (30) for S_t = 365 days

При S_t = 182 сут. получены следующие значения параметров: A = 58 747,94; a = 69,3903; b = 0,0270; $y_{RD20}(0)$ = 1 586,19 (соответствует значению на рис. 7); коэффициент детерминации 0,9996. При S_t = 365 сут.: A = 148 478,85; a = 50,7476; b = 0,0243; $y_{RD20}(0)$ = 3 608,04 (соответствует значению на рис. 8); коэффициент детерминации 0,9999. Как видим, наблюдается хорошая точность аппроксимации для обоих случаев.

Зависимости RPD_0 от g

Проведем аппроксимацию экспериментальных значений $RPD_0(g)$ (17), полученных имитационным моделированием, функцией (30).

На рис. 9 и 10 приведены экспериментальные значения и графики функций (30), которые их аппроксимируют для различных S_t.

При S_t = 182 сут. получены следующие значения параметров: A = 105 192,12; a = 68,9911; b = 0,0231; $y_{RPD0}(0)$ = 2 429,94 (соответствует значению на рис. 9); коэффициент детерминации 0,9995. При S_t = 365 сут.: A = 246 767,67; a = 49,8234; b = 0,0213; $y_{RPD0}(0)$ = 5 256,15 (соответствует значению на рис. 10); коэффициент детерминации 0,9999. Как видим, наблюдается хорошая точность аппроксимации для обоих случаев.

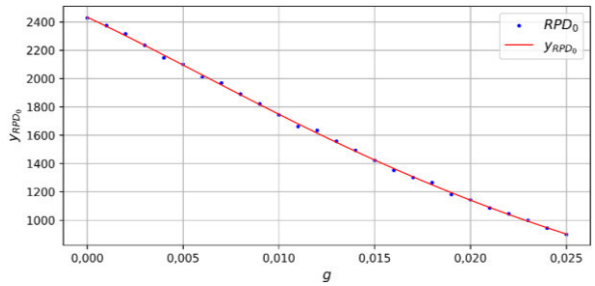

Рис. 9. Аппроксимация $RPD_0(g)$ функцией (30) для S_t = 182 сут.
Fig. 9. Approximation of $RPD_0(g)$ with function (30) for S_t = 182 days

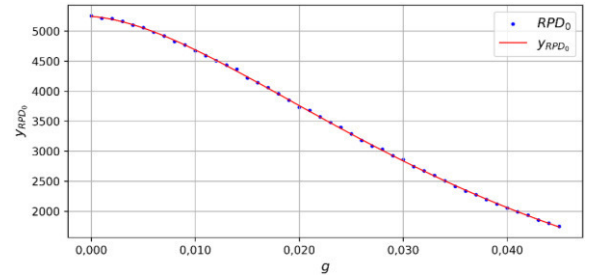

Рис. 10. Аппроксимация $RPD_0(g)$ функцией (30) для S_t = 365 сут.
Fig. 10. Approximation of $RPD_0(g)$ with function (30) for S_t = 365 days

Зависимости $RD2_0$ и RPD_0 от g при обнулении по варианту А

Проведем аппроксимацию экспериментальных значений $RD2_0(g)$ (15) и $RPD_0(g)$ (17), полученных имитационным моделированием, функцией (30) для варианта исходных данных $F1$ при обнулении по варианту А.

На рис. 11–14 приведены экспериментальные значения и графики функций (30), которые их аппроксимируют для различных S_t.

Для $RD2_0(g)$ при S_t = 182 сут. получены следующие значения параметров: A = 251 185,67; a = 73,2431; b = 0,0062; $y_{RD20}(0)$ = 1 547,55 (соответствует значению на рис. 11); коэффициент детерминации 0,9995. При S_t = 365 сут.: A = 390 551,78; a = 50,7908; b = 0,0060; $y_{RD20}(0)$ = 2 339,97 (соответствует значению на рис. 12); коэффициент детерминации 0,9988.

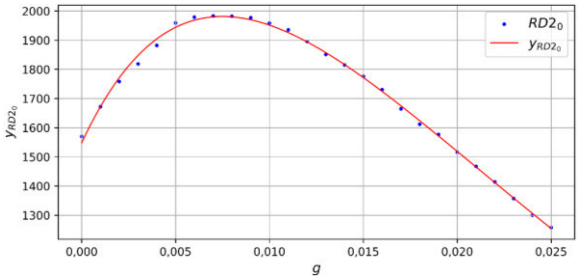

Рис. 11. Аппроксимация $RD2_0(g)$ функцией (30) для S_t = 182 сут. (по варианту А)
Fig. 11. Approximation of $RD2_0(g)$ with function (30) for S_t = 182 days (according to possibility A)

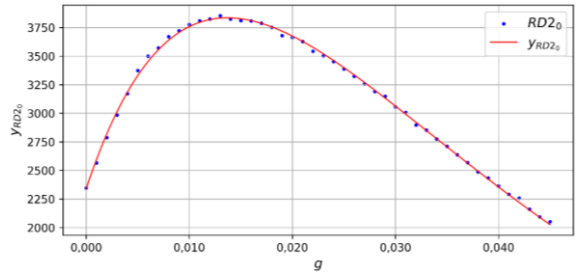

Рис. 12. Аппроксимация $RD2_0(g)$ функцией (30) для S_t = 365 сут. (по варианту А)
Fig. 12. Approximation of $RD2_0(g)$ with function (30) for S_t = 365 days (according to possibility A)

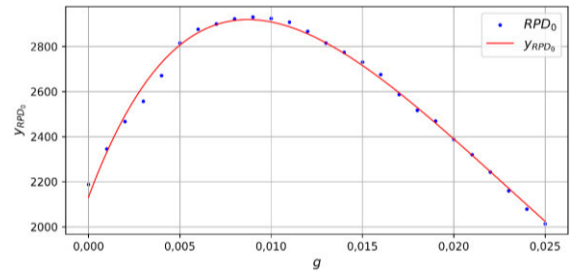

Рис. 13. Аппроксимация $RPD_0(g)$ функцией (30) для S_t = 182 сут.
Fig. 13. Approximation of $RPD_0(g)$ with function (30) for S_t = 182 days

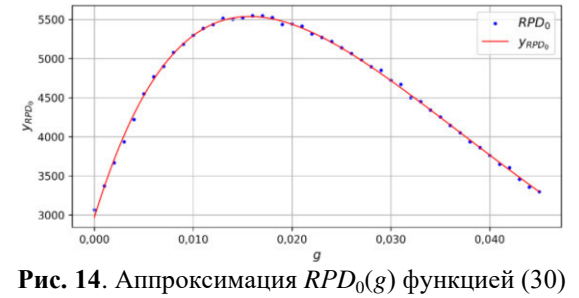

Рис. 14. Аппроксимация $RPD_0(g)$ функцией (30) для S_t = 365 сут.
Fig. 14. Approximation of $RPD_0(g)$ with function (30) for S_t = 365 days

Для $RPD_0(g)$ при S_t = 182 сут. получены следующие значения параметров: A = 364 503,36; a = 68,5914; b = 0,0058; $y_{RPD0}(0)$ = 2 131,11 (соответствует значению на рис. 13); коэффициент детерминации 0,9931. При S_t = 365 сут.: A = 553 670,01; a = 47,4413; b = 0,0054; $y_{RPD0}(0)$ = 2 970,95 (соответствует значению на рис. 14); коэффициент детерминации 0,9985. Как видим, наблюдается хорошая точность аппроксимации для всех четырех случаев.

Из рис. 11–14 видно, что, в отличие от обнуления по варианту В для двухфакторных финансовых рисков, при обнулении по варианту А наблюдается экстремум (максимум), для функции (30) ее экстремум находится в точке:

$$g_0 = 1/a - b. \qquad (31)$$

Для $RD2_0(g)$ при S_t = 182 сут. g_0 = 0,0075; при S_t = 365 сут. g_0 = 0,0137; для $RPD_0(g)$ при S_t = 182 сут. g_0 = 0,0087; при S_t = 365 сут. g_0 = 0,0157. Все значения соответствуют графикам функции на рис. 11–14.

В табл. 4 приведены экспериментальные значения точечных оценок показателей эффективности при S_t = 365 сут. в области максимума двухфакторных рисков.

По данным табл. 4 можно сделать вывод, что «перегиб» (наличие максимума) у двухфакторных рисков возникает из-за того, что скорость уменьшения значений $\tilde{R}_\tau(g)$ и скорость увеличения значений $RD_0(g)$ до экстремума и после него разные. В связи с этим, точечные оценки (15) и (17) сначала возрастают, а затем убывают.

Учитывая формулу (17), величина $RPD_0(g)$ – произведение величин $\tilde{R}_\tau(g)$ и $RD_0(g)$, которое равно сумме величин (9), деленной на n_0. Величина (15) – это сумма взвешенных величин (9), поэтому она меньше $RPD_0(g)$ на правую часть в (25). В связи с этим точка экстремума (31) для величины (15) меньше, чем для (17): в нашем случае 0,0137 и 0,0157.

Отметим, что это достаточно небольшие значения, они меньше рекомендуемых значений (28). При S_t < 365 сут. эти значения еще меньше. Необходимо также подчеркнуть, что экстремумы для экспериментальных и расчетных значений по аппроксимирующим функциям немного отличаются.

Заключение

1. Развивая предыдущие свои исследования [16–18], авторы уточнили важное свойство денежного фонда и его функций, а именно: понятие времени его обнуления. Описаны два варианта технологии обнуления (А и В).

2. В качестве рисков предложены: однофакторный риск в виде вероятности обнуления фонда; однофакторный финансовый риск в виде математического ожидания случайных величин, связанных с обнулением; два вида двухфакторных финансовых рисков, также связанных с обнулением фонда. Проведен их сравнительный анализ.

3. Доказано, что однофакторные финансовые риски в виде математического ожидания случайных величин, характеризующие итоговые расходы фонда (риск по расходам) и итоговые поступления в фонд (риск по доходам), дублируют друг друга. Рекомендовано использовать один из них, а именно – риск по расходам. Эта рекомендация относится к обеим технологиям обнуления.

4. Доказано, что предложенные два вида двухфакторных финансовых рисков (12) и (16) также дублируют друг друга. Рекомендовано использовать один из них, а именно риск (12) (математическое ожидание произведения вероятности обнуления фонда на случайную величину, характеризующую итоговые расходы фонда).

5. Проведена аппроксимация точечных оценок предложенных рисков различными функциями – (26), (29) и (30) в зависимости от коэффициента g. Задав уровень вероятности r_m, можно по зависимости (26) определить максимальное значение этого коэффициента по формуле (28). Оказывается, что для нормального функционирования ДенФ совсем не обязательно использовать большое начальное значение F_{S_0} .

Таблица 4. Экспериментальные значения показателей эффективности $RD2_0(g)$ и $RPD_0(g)$ возле экстремумов при S_t = 365 сут.

Table 4. Experimental values of the efficiency indicators near the extrema of $RD2_0(g)$ and $RPD_0(g)$ at S_t = 365 days

g	0,005	0,010	0,013	0,015	0,020	0,025
$\tilde{R}_\tau(g)$	0,7750	0,6654	0,6088	0,5709	0,4886	0,4148
$RD_0(g)$	5 870,49	7 960,38	9 057,55	9 660,32	11 140,74	12 387,21
$RD2_0(g)$	3 374,59	3 776,73	3 854,18	3 810,48	3 661,86	3 386,73
$RPD_0(g)$	4 549,51	5 297,08	5 514,15	5 515,27	5 443,03	5 138,71

6. Показано, что при аппроксимации точечных оценок рисков (12) и (16) функцией (30) при обнулении фонда по технологии А наблюдается экстремум, аргумент которого можно определить по формуле (31). Это связано с тем, что точечные оценки (15) и (17) сначала возрастают, а затем убывают. При использовании технологии В этот эффект отсутствует (функции монотонно убывают).

Список литературы

1. Кондауров С.Н., Бунина А.В., Митрофанов А.В. Проблемы обеспечения информационной безопасности в корпоративных сетях // Современные информационные технологии и информационная безопасность : сб. науч. ст. III Всерос. науч.-техн. конф. Курск, 2024. С. 69–72.

2. Краковский Ю.М. Методы защиты информации. Санкт-Петербург : Лань, 2021. 236 с.

3. Шпак А.А. Современные угрозы информационной безопасности // Современное право. 2024. № 1. С. 106–108.

4. Ершова Т.В., Хохлов Ю.Е. Цифровая экономика: от теоретических концепций к российской практике // Журнал Новой экономической ассоциации. 2025. № 2 (67). С. 234–243.

5. Цифровые технологии в российской экономике / К.О. Вишневский, Л.М. Гохберг, В.В. Дементьев и др. М. : НИУ ВШЭ, 2021. 116 с.

6. Стародубова А.А., Исхакова Д.Д. Инновационные стратегии цифровых предприятий для достижения устойчивого развития в регионах // π-Economy. 2023. Т. 16. № 1. С. 39–50.

7. Оганесян Л.Л., Козырь Н.С. Проектное управление в информационной безопасности // Вестник Академии знаний. 2023. № 4 (57). С. 207–209.

8. Сизов В.А., Дрожкин А.А. Моделирование экономики информационной безопасности субъекта экономической деятельности на основе симплекс-метода // Вестн. Рос. эконом. ун-та им. Г.В. Плеханова. 2021. Т. 18. № 1 (115). С. 173–178.

9. Ефимов Е.Н., Лапицкая Е.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Бизнес-информатика. 2015. № 1 (31). С. 51–57.

10. Тебекин А.В. Анализ проблем и перспектив реализации планов импортозамещения в отраслях промышленности // Транспортное дело России. 2022. № 2. С. 159–165.

11. Абдикеев Н.М. Импортозамещение в высокотехнологичных отраслях промышленности в условиях внешних санкций // Управленческие науки. 2022. Т. 12. № 3. С. 53–69.

12. Руднева Л.Н. Тенденции инновационного развития российской экономики // Фундаментальные исследования. 2023. № 2. С. 50–56.

13. Ашихмин Р.С., Борисова О.В. Искусственный интеллект: реальный потенциал для повышения эффективности бизнеса и государства // Вызовы цифровой экономики: технологический суверенитет и экономическая безопасность : сб. ст. VI Всерос. науч.-практ. конф. с междунар. участ. Брянск, 2023. С. 45–48.

14. Авдеенко Е.Е., Шитый А.Д. Использование искусственного интеллекта в целях повышения эффективности развития бизнеса и государства // Вызовы цифровой экономики: технологический суверенитет и экономическая безопасность : сб. ст. VI Всерос. науч.-практ. конф. с междунар. участ. Брянск, 2023. С. 14–18.

15. Сивицкий Д.А. Анализ опыта и перспектив применения искусственных нейронных сетей на железнодорожном транспорте // Вестн. Сибир. гос. ун-та путей сообщ. 2021. № 2 (57). С. 33–41.

16. Краковский Ю.М., Киргизбаев В.П. Программно-математическое обеспечение для исследования показателей эффективности экономики информационной безопасности // System Analysis and Mathematical Modeling. 2024. Т. 6. № 2. С. 209–220.

17. Краковский Ю.М., Киргизбаев В.П. Системный подход к моделированию работ по устранению инцидентов информационной безопасности применительно к корпоративной информационной системе // Современные технологии. Системный анализ. Моделирование. 2025. № 1 (85). С. 116–126.

18. Краковский Ю.М., Киргизбаев В.П. Моделирующая программа для оценки финансового состояния денежного фонда с учетом отдельных работ по устранению инцидентов информационной безопасности // Информационные и математические технологии в науке и управлении. 2025. № 2 (38). С. 74–82.

19. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории рисков. М. : Физматлит, 2011. 620 с.

20. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении. М. : Финансы и статистика, 2009. 368 с.

21. Туганбаев А.А., Крупин В.Г. Теория вероятностей и математическая статистика. СПб. : Лань, 2011. 223 с.

22. Кобзарь А.И. Прикладная математическая статистика. М. : Физматлит, 2006. 813 с.

23. Кельтон В.Д., Лоу А.М. Имитационное моделирование. СПб. : Питер, 2004. 847 с.

24. Лутц М. Изучаем Python. Т. 1. СПб. : Диалектика, 2019. 832 с.

References

1. Kondaurov S.N., Bunina A.V., Mitrofanov A.V. Problemy obespecheniya informatsionnoi bezopasnosti v korporativnykh setyakh [Problems of ensuring information security in corporate networks]. *Sbornik nauchnykh statei III Vserossiiskoi*

nauchno-tekhnicheskoi konferentsii «Sovremennye informatsionnye tekhnologii i informatsionnaya bezopasnost'» [Proceedings of Scientific Articles of the III All-Russian Scientific and Technical Conference «Modern Information Technologies and Information Security»]. Kursk, 2024, pp. 69–72.

2. Krakovskii Y.M. Metody zashchity informatsii [Methods of Information Protection]. Saint Petersburg: Lan' Publ., 2021. 236 p.

3. Shpak A.A. Sovremennye ugrozy informatsionnoi bezopasnosti [Modern threats to information security]. *Sovremennoe pravo* [Modern law], 2024, no 1, pp. 106–108.

4. Ershova T.V., Khokhlov Yu.E. Tsifrovaya ekonomika: ot teoreticheskikh kontseptsii k rossiiskoi praktike [Digital economy: from theoretical concepts to Russian practice]. *Zhurnal Novoi ekonomicheskoi assotsiatsii* [Journal of the New Economic Association], 2025, no 2 (67), pp. 234–243.

5. Vishnevskii K.O., Gokhberg L.M., Dement'ev V.V., Dranev Yu.Ya., Klubova M.A., Kotsemir M.N., Kuz'minov I.F., Lola I.S., Privorotskaya S.G., Rudnik P.B., Sokolov A.V., Strel'tsova E.S., Turovets Yu.V., Fursov K.S., Khabirova E.E., Altynov A.I., Evtushenko V.E., Kuchin I.I., Lobanova P.A. Tsifrovye tekhnologii v rossiiskoi ekonomike [Digital technologies in the Russian Economy]. Moscow: NIU VShE Publ., 2021. 116 p.

6. Starodubova A.A., Iskhakova D.D. Innovatsionnye strategii tsifrovykh predpriyatii dlya dostizheniya ustoichivogo razvitiya v regionakh [Innovative strategies of digital enterprises for achieving sustainable development in the regions], π-Economy, 2023, Vol. 16, no 1, pp. 39–50.

7. Oganesian L.L., Kozyr' N.S. Proektnoe upravlenie v informatsionnoi bezopasnosti [Project management in information security]. *Vestnik Akademii znanii* [Bulletin of the Academy of Knowledge], 2023, no 4 (57), pp. 207–209.

8. Sizov V.A., Drozhkin A.A. Modelirovanie ekonomiki informatsionnoi bezopasnosti sub''ekta ekonomicheskoi deyatel'nosti na osnove simpleks-metoda [Modeling the economics of information security of an economic entity based on the simplex method]. *Vestnik Rossiiskogo ekonomicheskogo universiteta imeni G.V. Plekhanova* [Bulletin of the Plekhanov Russian University of Economics], 2021, Vol. 18, no 1 (115), pp. 173–178.

9. Efimov E.N., Lapitskaya E.M. Otsenka effektivnosti meropriyatii informatsionnoi bezopasnosti v usloviyakh neopredelennosti [Evaluation of the effectiveness of information security measures under conditions of uncertainty]. *Biznes-informatika* [Business Informatics], 2015, no 1 (31), pp. 51–57.

10. Tebekin A.V. Analiz problem i perspektiv realizatsii planov importozameshcheniya v otraslyakh promyshlennosti [Analysis of the problems and prospects of implementing import substitution plans in industry]. *Transportnoe delo Rossii* [Transport Business of Russia], 2022, no 2, pp. 159–165.

11. Abdikeev N.M. Importozameshchenie v vysokotekhnologichnykh otraslyakh promyshlennosti v usloviyakh vneshnikh sanktsii [Import substitution in high-tech industries under external sanctions]. *Upravlencheskie nauki* [Management Sciences], 2022, Vol. 12, no. 3, pp. 53–69.

12. Rudneva L.N. Tendentsii innovatsionnogo razvitiya rossiiskoi ekonomiki [Trends in the innovative development of the Russian economy]. *Fundamental'nye issledovaniia* [Fundamental Research], 2023, no 2, pp. 50–56.

13. Ashikhmin R.S., Borisova O.V. Iskusstvennyi intellekt: real'nyi potentsial dlya povysheniya effektivnosti biznesa i gosudarstva [Artificial intelligence: the real potential for improving the efficiency of business and the state]. *Sbornik statei VI Vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem «Vyzovy tsifrovoi ekonomiki: tekhnologicheskii suverenitet i ekonomicheskaya bezopasnost'»* [Proceedings of the VI All-Russian Scientific and Practical Conference with international participation «Challenges of the digital economy: technological sovereignty and economic security»]. Bryansk, 2023, pp. 45–48.

14. Avdeenko E.E., Shityi A.D. Ispol'zovanie iskusstvennogo intellekta v tselyakh povysheniya effektivnosti razvitiya biznesa i gosudarstva [The use of artificial intelligence in order to improve the efficiency of business and government development]. *Sbornik statei VI Vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarodnym uchastiem «Vyzovy tsifrovoi ekonomiki: tekhnologicheskii suverenitet i ekonomicheskaya bezopasnost'»* [Proceedings of the VI All-Russian Scientific and Practical Conference with international participation «Challenges of the digital economy: technological sovereignty and economic security»]. Bryansk, 2023, pp. 14–18.

15. Sivitskii D.A. Analiz opyta i perspektiv primeneniya iskusstvennykh neironnykh setei na zheleznodorozhnom transporte [Analysis of the experience and prospects of using artificial neural networks in railway transport]. *Vestnik Sibirskogo gosudarstvennogo universiteta putei soobshcheniya* [Bulletin of the Siberian State Transport University], 2021, no 2 (57), pp. 33–41.

16. Krakovskii Y.M., Kirgizbaev V.P. Programmno-matematicheskoe obespechenie dlia issledovaniia pokazatelei effektivnosti ekonomiki informatsionnoi bezopasnosti [Software and mathematical support for studying the efficiency indicators of the information security economy], System Analysis and Mathematical Modeling, 2024, Vol. 6, no 2, pp. 209–220.

17. Krakovskii Yu.M., Kirgizbaev V.P. Sistemnyi podkhod k modelirovaniyu rabot po ustraneniyu intsidentov informatsionnoi bezopasnosti primenitel'no k korporativnoi informatsionnoi sisteme [Systematic approach to modeling work to eliminate information security incidents in relation to a corporate information system]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [Modern Technologies. System analysis. Modeling], 2025, no 1 (85), pp. 116–126.

18. Krakovskii Yu.M., Kirgizbaev V.P. Modeliruyushchaya programma dlya otsenki finansovogo sostoyaniya denezhnogo fonda s uchetom otdel'nykh rabot po ustraneniyu intsidentov informatsionnoi bezopasnosti [Modeling program for assessing the financial condition of a monetary fund, taking into account individual work to eliminate information security incidents]. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii* [Information and mathematical technologies in science and management], 2025, no 2 (38), pp. 74–82.

19. Korolev V.Yu., Bening V.E., Shorgin S.Ya. Matematicheskie osnovy teorii riskov [Mathematical Foundations of Risk Theory]. Moscow: Fizmatlit Publ., 2011. 620 p.

20. Anfilatov V.S., Emel'yanov A.A., Kukushkin A.A. Sistemnyi analiz v upravlenii [System analysis in management]. Moscow: Finansy i statistika Publ., 2009. 368 p.

21. Tuganbaev A.A., Krupin V.G. Teoriya veroyatnostei i matematicheskaya statistika [Probability theory and mathematical statistics]. Saint Petersburg: Lan' Publ., 2011. 223 p.

22. Kobzar' A.I. Prikladnaya matematicheskaya statistika [Applied mathematical statistics]. Moscow: Fizmatlit Publ., 2006. 813 p.
23. Law A.M., Kelton W.D. Imitatsionnoe modelirovanie [Simulation Modeling and Analysis]. Saint Petersburg: Piter Publ., 2004. 847 p.
24. Lutz M. Izuchaem Python. T. 1 [Learning Python. Vol. 1]. Saint Petersburg: Dialektika Publ., 2019. 832 p.

Информация об авторах

Краковский Юрий Мечеславович, доктор технических наук, профессор, профессор кафедры информационных систем и защиты информации, Иркутский государственный университет путей сообщения, г. Иркутск; e-mail: yuri.krakovskiy@yandex.ru.
Киргизбаев Владислав Павлович, аспирант кафедры информационных систем и защиты информации, Иркутский государственный университет путей сообщения, г. Иркутск; e-mail: v.p.kirgizbaev@gmail.com.

Information about the authors

Yurii M. Krakovskii, Doctor of Engineering Science, Full Professor, Professor of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk; e-mail: yuri.krakovskiy@yandex.ru.

Vladislav P. Kirgizbaev, Ph.D. Student of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk; e-mail: v.p.kirgizbaev@gmail.com.

