ОРИГИНАЛЬНАЯ СТАТЬЯ
2025. № 1 (85). С. 116–126 *Современные технологии. Системный анализ. Моделирование*
DOI 10.26731/1813-9108.2025.1(85).116-126 **УДК** 519.6: 311

Системный подход к моделированию работ по устранению инцидентов информационной безопасности применительно к корпоративной информационной системе

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

Резюме
В статье рассмотрен системный подход к моделированию работ по устранению инцидентов информационной безопасности для корпоративной информационной системы. С целью повышения эффективности выполнения работ по защите информации предложено использовать денежный фонд, в котором накапливаются необходимые финансовые средства и затем расходуются. Безопасность корпоративной информационной системы обеспечивается при ограничении финансовых средств, необходимых для нее, поэтому предложены новые показатели в виде однофакторных финансовых рисков. В денежном фонде происходит взаимодействие финансовых потоков по накоплению и расходам. Наличие сложных связей приводит к системному эффекту, который называют эмерджентностью. В нашем случае процесс, описывающий состояние фонда, получается нестационарным, хотя взаимодействующие потоки являются либо регулярными, либо стационарными. Для моделирования этого процесса разработано специальное алгоритмическое обеспечение, основанное на календаре событий. Моделирование происходит от события к событию. Для каждого кода события создается подпрограмма по его обработке. Важным компонентом этих подпрограмм является планирование следующего события с таким же кодом. Предложенное математическое обеспечение с учетом новых показателей эффективности реализовано в виде программного обеспечения, ядром которого является моделирующая программа на основе дискретно-имитационного моделирования. Программное обеспечение разработано с использованием языка программирования Python версии 3.12. В созданном обеспечении используются модули из библиотеки Python (csv, random, sys, time, math и др.). В целях моделирования значений случайных величин, характеризующих интервалы между инцидентами и затраты на их устранение, моделирующая программа поддерживает различные законы распределения, выбор которых обусловлен их применимостью в теории рисков, имитационном моделировании и страховой математике. Проведена апробация созданного программно-алгоритмического обеспечения, показавшая его работоспособность, получены научные и практические рекомендации.

Ключевые слова
имитационное моделирование, денежный фонд, информационная безопасность, показатели эффективности, корпоративная информационная система, календарь событий, двухфакторные риски

Для цитирования
Краковский Ю.М. Системный подход к моделированию работ по устранению инцидентов информационной безопасности применительно к корпоративной информационной системе / Ю.М. Краковский, В.П. Киргизбаев // Современные технологии. Системный анализ. Моделирование. 2025. № 1 (85). С. 116–126. DOI 10.26731/1813-9108.2025.1(85).116-126.

Информация о статье
поступила в редакцию: 17.12.2024 г.; поступила после рецензирования: 25.03.2025 г.; принята к публикации 26.03.2025 г.

A systems approach to modeling incident response work in information security for a corporate information system

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

Abstract
The paper discusses a systematic approach to modeling incident response processes for information security in a corporate information system. To increase the effectiveness of information protection efforts, it is proposed to utilize a budget fund that accumulates and then disburses necessary financial resources. Corporate information system security is ensured under a financial constraint, making the introduction of new indicators in the form of single-factor financial risks essential. The budget fund manages the interaction of financial flows for accumulation and expenditure. Complex interconnections create a systemic effect known as emergence. In this case, the process describing the fund's state becomes non-stationary, although the interacting flows are either regular or stationary. For modeling this process, specialized algorithmic support has been developed based on an event calendar.

The simulation progresses from event to event, with each event code having a dedicated subroutine created for handling it. A crucial component of these subroutines is the scheduling of the next event with the same code. The proposed mathematical support, accounting for new performance indicators, is implemented as software, with a simulation program based on discrete-event modeling as its core. The software was developed using the Python programming language, version 3.12. The system utilizes various Python modules (csv, random, sys, time, math, etc.). To simulate random variable values representing incident intervals and response costs, the simulation program supports various probability distributions, chosen for their applicability in risk theory, simulation modeling, and actuarial mathematics. Testing of the developed software and algorithmic framework confirmed its functionality, yielding both scientific and practical recommendations.

Keywords
simulation modeling, cash fund, information security, performance indicators, corporate information system, events calendar, two-factor risks

For citation
Krakovskii Yu.M., Kirgizbaev V.P. Sistemnyi podkhod k modelirovaniyu rabot po ustraneniyu intsidentov informatsionnoi bezopasnosti primenitelno k korporativnoi informatsionnoi sisteme [A systems approach to modeling incident response work in information security for a corporate information system]. *Sovremennye tekhnologii. Sistemnyi analiz. Modelirovanie* [Modern Technologies. System Analysis. Modeling], 2025. No. 1(85). Pp. 116–126. DOI: 10.26731/1813-9108.2025.1(85).116-126.

Article info
Received: December 17, 2024; Revised: March 25, 2025; Accepted: March 26, 2025.

Введение

В условиях стремительного развития цифровых технологий и внедрения искусственного интеллекта все большее внимание уделяется защите информации в различных системах и организациях. Основным объектом защиты становятся корпоративные информационные системы (КИС), включая распределенные решения, использующие различные каналы связи. Важность информационной безопасности растет, так как она направлена на обеспечение целостности и конфиденциальности различных данных от множества угроз, что способствует устойчивой работе бизнеса и минимизации рисков [1, 2].

Дополнительно отметим, что в связи с цифровизацией экономики и наличия внешних факторов в нашей стране в последние годы активизировалось развитие различных отраслей промышленности [3–5], стали реализовываться программы импортозамещения [6–8], создаваться российские варианты информационных технологий и искусственного интеллекта [9–13], а это также влияет на необходимость совершенствовать технологии информационной безопасности КИС.

Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса [14].

Безопасность КИС обеспечивается при ограничении финансовых средств, необходимых для нее, поэтому большое значение имеют вопросы экономики информационной безопасности [15–17].

Информационная безопасность достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств. Процесс обеспечения информационной безопасности включает в себя как правовые и организационные меры, так и технические, в которых выделяют технические, криптографические, программные и аппаратные средства [14]. Такой подход позволяет предотвращать различные инциденты, которые могут нанести ущерб организации.

Инцидентам информационной безопасности посвящено большое число нормативных документов. Приведем следующее определение: «…это следствие одного или нескольких нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации операций бизнеса или создания угрозы информационной безопасности» [14]. В свою очередь событие информационной безопасности – «это какое-либо событие, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности».

Таким образом, современные стандарты информационной безопасности подчеркивают важность защиты информации как одного из активов предприятия. Любая информация, имеющая ценность для бизнеса, должна быть защищена от возможных угроз, как внешних, так и внутренних.

Данная статья является развитием работ авторов [18, 19]. В этих работах при реализации информационной безопасности КИС учитывается важный фактор – ограниченные финансовые ресурсы, выделяемые на ее защиту от различных угроз. Для решения данной задачи предлагается использовать денежный (бюджетный) фонд (ДенФ) для выполнения двух функций:

1. По мере необходимости производится оплата работ, связанных с устранением инцидентов, когда для каждого вида работ определяется периодичность использования фонда (сут.) и стоимость этих работ (тыс. р.).

2. Необходимо проводить накопление платежей с какой-то периодичностью (сут.) и величиной стоимости этих платежей (тыс. р.). Таким образом, в этом фонде происходит взаимодействие двух денежных потоков.

Поступления в фонд предлагается описывать неслучайными величинами как для интервалов, так и для размеров поступлений. В условиях неопределенности интервалы времени между инцидентами и затраты для их устранения являются случайными величинами с известными вероятностными моделями в виде двухпараметрических функций распределений с точностью до значений математических ожиданий и коэффициентов вариации.

Целью данной работы является обоснование необходимости системного подхода к моделированию работ по устранению инцидентов информационной безопасности для КИС.

При реализации этой цели предложены новые (относительно работ [18, 19]) показатели, характеризующие эффективность организации работ по защите информации.

Математическое обеспечение для моделирования состояния денежного фонда и оценки показателей эффективности

Состояние ДенФ предлагается описать случайным нестационарным процессом вида:

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

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

Суммарная величина:

$$Z_j(t) = \sum_{q=1}^{N_j(t)} z_{qj} \text{ , тыс. р.,} \quad (2)$$

где z_{qj} – величина q-го расхода для j-й работы; $N_j(t)$ – число этих расходов за время t.

Суммарная величина:

$$Y_l(t) = Y_{0l} \cdot N_{0l}(t), \text{ тыс. р.,} \quad (3)$$

где Y_{0l} – значение единичного платежа l-го вида при пополнении фонда, тыс. р. (эти величины рассчитываются); $N_{0l}(t)$ – число платежей l-го вида за время t.

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

$$F_{S_0} = g \cdot X \text{ , тыс. р.,} \quad (4)$$

где X – средние финансовые средства (тыс. р.), необходимые для выполнения годового объема всех работ (расходы); g – коэффициент, равный 0,05 или 0,10.

Финансовые средства (тыс. р.), необходимые для выполнения годового объема работ (расходы) для j-го вида работ в среднем равны:

$$X_{0j} = Tg \cdot (mz_j / mt_j), \text{ тыс. р.,} \quad (5)$$

где Tg – число суток в году; mt_j, mz_j – математические ожидания вероятностных моделей интервалов времени и величин затрат.

С учетом (5) суммарные средства по всем видам работ в среднем равны:

$$X = \sum_{j=1}^{m} X_{0j} \text{ , тыс. р.} \quad (6)$$

Средний размер платежа l-го вида равен:

$$P_{0l} = c_l \cdot X, \ \sum_{l=1}^{L} P_{0l} = X \ , \ \sum_{l=1}^{L} c_l = 1, \quad (7)$$

где c_l – доли платежей l-го вида при пополнении ДенФ.

Исходя из (7), средняя суммарная величина доходов за год должна быть равна средней суммарной величине расходов за год.

Чтобы учесть рекомендации теории рисков [20, 21], вводится величина F_{S_0}. В этом

случае доход превышает расход.

Значение единичного платежа l-го вида при пополнении ДенФ:

$$Y_{0l} = P_{0l} / N_l = (c_l \cdot h_l \cdot X) / Tg, \quad (8)$$

где $N_l = Tg/h_l$ – среднее число l-ых платежей за год; h_l– значение интервала времени между поступлениями платежей l-го вида при пополнении ДенФ, сут.

Пусть s – время, когда первый раз $Fs(t) < 0$ (время, когда в фонде закончились деньги на оплату работ), сут. Назовем его временем «обнуления» ДенФ:

$$s = \min_t (t: Fs(t) < 0), \text{ сут.}, \quad (9)$$

S – случайная величина, для которой определяется время s; $(S < S_t)$ – случайное негативное событие, заключающееся в том, что произошло «обнуление» фонда за время S_t, сут.

При имитационном моделировании для времени s образуется упорядоченная по возрастанию выборка объема n:

$$Ts = (s_1, \dots, s_i, \dots, s_n), \quad (10)$$

где i – номер элемента выборки.

В качестве показателей, характеризующих эффективность организации работ по защите информации, предлагаются риски вида:

– вероятность негативного события:

$$p_t = P(S < S_t); \quad (11)$$

– коэффициент вариации для величины S на интервале $(0, S_t)$, %:

$$c_S = (\sigma/\mu) \cdot 100. \quad (12)$$

Здесь σ – значение среднеквадратического отклонения на интервале $(0, S_t)$; μ – значение математического ожидания на этом интервале.

При имитационном моделировании величины (11) и (12) оцениваются через точечные и интервальные оценки, полученные по выборке (10) за время S_t:

– $\tilde{R}_\tau$ – точечная оценка величины (11);

– (τ_1, τ_2) – интервальная оценка величины (11);

– $\tilde{c}_\tau$ – точечная оценка величины (12);

– (ν_1, ν_2) – интервальная оценка величины (12).

При этом

$$\tilde{R}_\tau = k_\tau / n_0, \quad (13)$$

где k_τ – количество реализаций процесса, когда случайное событие $(S < S_t)$ существует;

$$\tilde{c}_\tau = (\sigma_\tau/\mu_\tau) \cdot 100, \%, \quad (14)$$

где μ_τ – оценка математического ожидания на этом интервале:

$$\mu_\tau = \sum_{i=1}^{k_\tau} s_i / k_\tau;$$

σ_τ – оценка среднеквадратического отклонения величины S на интервале $(0, S_t)$:

$$\sigma_\tau = \sqrt{\left(\sum_{i=1}^{k_\tau} s_i^2 - k_\tau \mu_\tau^2\right) \Big/ \left(k_\tau - 1\right)}.$$

Интервальные оценки (τ_1, τ_2) приведены в работе [16]. Приведем интервальные оценки (ν_1, ν_2) [19]:

$$\nu_1 = \exp\left(\ln(\tilde{c}_\tau) - z_\gamma \sqrt{\frac{1 + (\ln(\tilde{c}_\tau))^2}{k_\tau - 1}}\right), (\%)$$

$$\nu_2 = \exp\left(\ln(\tilde{c}_\tau) + z_\gamma \sqrt{\frac{1 + (\ln(\tilde{c}_\tau))^2}{k_\tau - 1}}\right), (\%)$$

где $z_\gamma = 1{,}96$ – критическое значение статистики Z при доверительной вероятности $\gamma = 0{,}95$.

Введем дополнительные показатели эффективности в виде рисков, которые измеряются в рублях:

– финансовый риск по расходам из ДенФ на выполнение работ –

$$RD = M[Dr], \text{ тыс. р.}, \quad (15)$$

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

– финансовый риск по поступлениям в ДенФ –

$$RU = M[Du], \text{ тыс. р.}, \quad (16)$$

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

При имитационном моделировании риски (15) и (16) заменим на точечные (21), (24) и интервальные оценки (22), (23), (25), (26).

Для этого введем две упорядоченные по возрастанию выборки:

$$D = (d_1, \dots, d_i, \dots, d_n), \quad (17)$$

где d_i – итоговое значение расходов по всем работам до времени s_i, s_i – выборочное значение (10).

$$d_i = \sum_{j=1}^{m} Z_j(s_i), \quad (18)$$

где $Z_j(s_i)$ – величина (2), когда число расходов определяется до времени s_i включительно.

$$U = (u_1, \dots, u_i, \dots, u_n), \quad (19)$$

где u_i – итоговое значение поступлений по всем платежам до времени s_i:

$$u_i = F_{S_0} + \sum_{l=1}^{L} Y_l(s_i), \quad (20)$$

где $Y_l(s_i)$ – величина (3), когда число поступлений определяется до времени s_i включительно; F_{S_0} – начальное значение процесса $Fs(t)$ (1).

Используем для точечных и интервальных оценок величин (15) и (16), полученных за время S_t по выборкам (17) и (19) соответственно, следующие обозначения:

– RD_0 – точечная оценка величины RD (15) на интервале $(0, S_t)$:

$$RD_0 = \sum_{i=1}^{k_\tau} d_i / k_\tau, \quad (21)$$

где d_i – величина (18); RD_1, RD_2 – интервальная оценка величины RD:

$$RD_1 = RD_0 - \left(z_\gamma \cdot \sigma_d\right) / \sqrt{k_\tau}; \quad (22)$$

$$RD_2 = RD_0 + \left(z_\gamma \cdot \sigma_d\right) / \sqrt{k_\tau}, \quad (23)$$

где σ_d – оценка среднеквадратического отклонения величины Dr на интервале $(0, S_t)$;

– RU_0 – точечная оценка величины RU (16) на интервале $(0, S_t)$:

$$RU_0 = \sum_{i=1}^{k_\tau} u_i / k_\tau, \quad (24)$$

где u_i – величина (20); RU_1, RU_2 – интервальная оценка величины RU:

$$RU_1 = RU_0 - \left(z_\gamma \cdot \sigma_d\right) / \sqrt{k_\tau}; \quad (25)$$

$$RU_2 = RU_0 + \left(z_\gamma \cdot \sigma_d\right) / \sqrt{k_\tau}, \quad (26)$$

где σ_u – оценка среднеквадратического отклонения величины Du на интервале $(0, S_t)$.

Для вариантов с хорошей организацией работ по устранению инцидентов информационной безопасности риск (11) должен уменьшаться, а риск в виде коэффициента вариации (14) и финансовые риски (15) и (16) увеличиваться.

Обоснование системного подхода при моделировании работ по устранению инцидентов информационной безопасности

На рис. 1 приведена схема процесса моделирования работ, дадим ее описание.

В первый блок поступают исходные данные (Исх), приведенные ранее. Дополнительно используются такие данные: Tm – максимальное время моделирования, сут.; kvt_j, kvz_j – коэффициенты вариации вероятностных моделей интервалов времени и величины затрат для j-й работы.

К исходным данным также относятся виды вероятностных моделей интервалов времени и величины затрат.

В ДенФ поступают платежи для выполнения работ (+П), число потоков платежей равно L, эти потоки регулярные. Из фонда забираются финансовые средства для оплаты работ (–Р). Число таких потоков равно m, эти потоки случайные и стационарные.

В ДенФ происходит взаимодействие $(m + L)$ денежных потоков. Наличие сложных связей приводит к системному эффекту, который называют эмерджентностью, а именно – появление у системы свойств, не присущих ее компонентам по отдельности. В нашем случае процесс (1), описывающий состояние фонда, получается нестационарным, хотя взаимодействующие потоки являются либо регулярными,

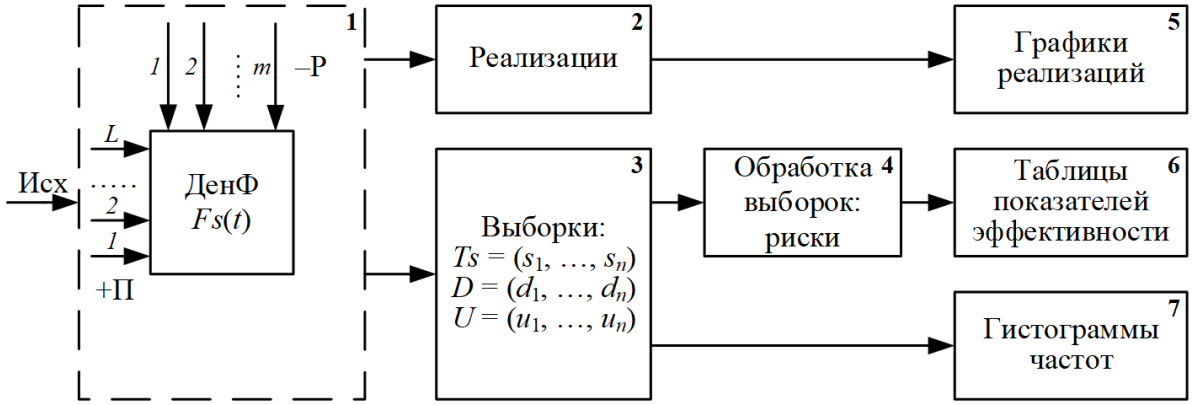

Рис. 1. Схема процесса моделирования работ
Fig. 1. Work modeling process diagram

либо стационарными. Этот системный эффект надо учитывать.

Учитывая нестационарность процесса (1), величины (9) существуют не для всех реализаций:

$$P(S < \infty) < 1. \quad (27)$$

Для того чтобы повысить точность дискретно-имитационного моделирования в данном исследовании число реализаций $n_0 = 20\,000$.

На рис. 2 и 3 приведены реализации процесса (1), полученные дискретно-имитационным моделированием (масштаб по оси *y* носит условный характер). На рис. 2 реализация процесса пересекает ось времени, таким образом величина (9) создается (происходит «обнуление» фонда), а на рис. 3 реализация процесса не пересекает ось времени, таким образом величина (9) не создается (не происходит «обнуление» фонда за время моделирования). Учитывая (27), такие реализа-

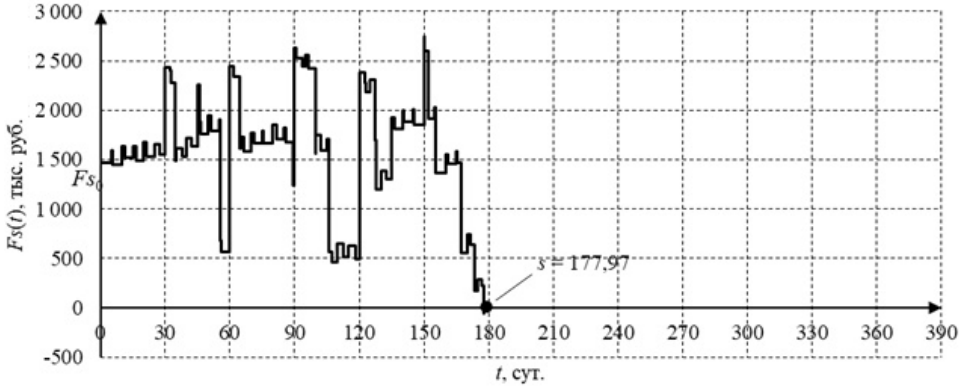

Рис. 2. График реализации с «обнулением» денежного фонда за время моделирования *Tm*
Fig. 2. Graph of implementation with «zeroing» of the monetary fund during the simulation time *Tm*

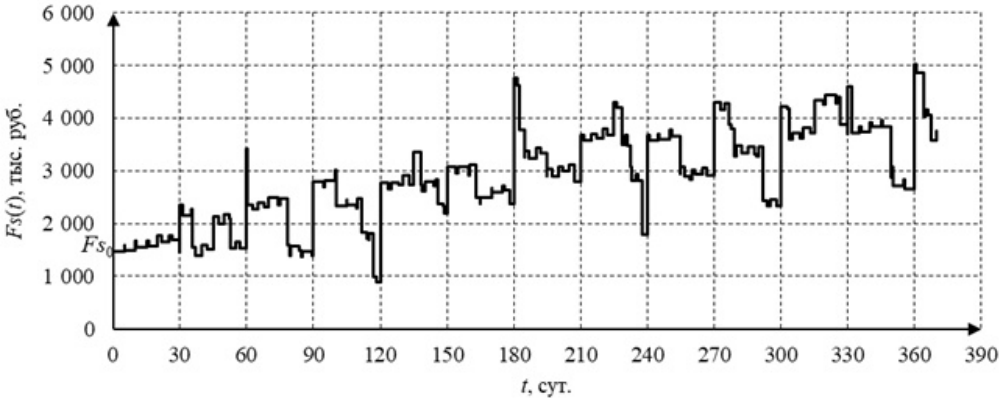

Рис. 3. График реализации без «обнуления» денежного фонда за время моделирования *Tm*
Fig. 3. Graph of implementation without «zeroing» of the monetary fund during the simulation time *Tm*

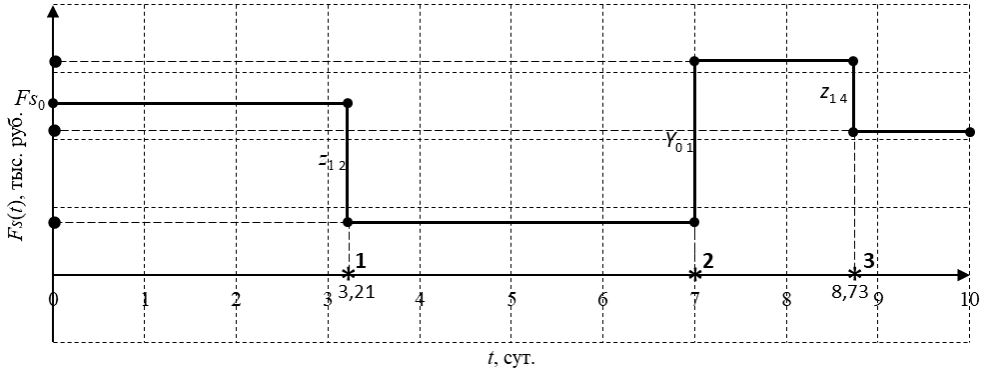

Рис. 4. Фрагмент реализации процесса (1)
Fig. 4. Process implementation fragment (1)

ции будут присутствовать независимо от продолжительности времени моделирования.

Второй блок (см. рис. 1) создает реализации процесса (1), а пятый – представляет их в виде графиков. Третий блок создает выборки (10), (17), (19). Для этого создано специальное алгоритмическое обеспечение, основанное на календаре событий. Это «ядро» дискретно-имитационного моделирования. Календарь событий содержит $(m + L)$ пар чисел: первое число – это код события (КодС); второе число – это время, когда это событие происходит (ТС). Моделирование происходит от события к событию. Всегда выбирается событие, время свершения которого минимально (свершившееся событие удаляется из календаря).

Для каждого кода события создается подпрограмма по его обработке. Важным компонентом этих подпрограмм является планирование следующего события с таким же кодом.

В предлагаемой моделирующей программе первые m кодов $(1, 2, \ldots, m)$ – это коды по расходам, а следующие L кодов $(m + 1, m + 2, \ldots, m + L)$ – это коды по доходам.

На рис. 4 приведен фрагмент реализации процесса (1), который поясняет работу календаря событий: 1) первым произошло событие, связанное с расходом, например, КС = 2, расход равен $z_{1\,2}$, ТС = 3,21 сут.; 2) далее произошло событие, связанное с поступлением, например, КС = 6 ($m = 5$), Y_{01} – значение единичного платежа 1-го вида; ТС = 7 сут.; 3) далее произошло событие, связанное с расходом, например, КС = 4, расход равен $z_{1\,4}$, ТС = 8,73 сут. и т.д.

Четвертый блок обрабатывает выборки, создает точечные и интервальные оценки предложенных показателей эффективности.

Шестой блок формирует значения этих показателей в виде таблиц и графиков, а седьмой – создает по выборкам гистограммы частот.

Апробация созданного программного обеспечения по моделированию работ для устранения инцидентов

Предложенное математическое обеспечение с учетом новых показателей эффективности (15)–(26) реализовано в виде программного обеспечения, ядром которого является моделирующая программа на основе дискретно-имитационного моделирования [21, 23].

Программное обеспечение разработано с использованием языка программирования Python версии 3.12 [24]. В созданном обеспечении используются модули из библиотеки Python (csv, random, sys, time, math и др.).

Для моделирования значений случайных величин, характеризующих интервалы между инцидентами и затраты на их устранение, моделирующая программа поддерживает следующие законы распределения: равномерное (Равн.), нормальное (Норм.), логнормальное (Логнорм.), бета, гамма, Парето с нулевой точкой (Парето), Бирнбаума-Саундерса (Б.-С.). Выбор этих распределений обусловлен их применимостью в теории рисков, имитационном моделировании и страховой математике [21, 22, 25].

Апробацию созданного программно-математического обеспечения проведем для пяти видов работ ($m = 5$):

1) поддержка и модернизация программных средств защиты информации;

2) восстановление работоспособности технических и программно-аппаратных средств защиты информации;

3) резервное копирование важной информации (облачное хранение, зеркалирование и т.д.);

4) поддержка, восстановление и модернизация средств защиты информации для сложных сетевых инфраструктур (Dallas Lock и т.д.);

5) поддержка и модернизация криптографических средств защиты информации, включая программно-аппаратные комплексы [18].

В табл. 1 приведены исходные данные для этих работ [19] (вероятностные модели и их числовые характеристики): В. м. для интер. – вероятностные модели для интервалов; В. м. для затрат – вероятностные модели для затрат. Другие исходные данные описаны ранее.

Учитывая формулу (6) и значения из табл. 1, общие средние расходы, необходимые для выполнения годового объема всех работ, равны $X = 29\,440$ тыс. р. Начальное значение (4) вычисляется при $g = 0{,}05$ или $g = 0{,}10$.

В данной статье при апробации рассматривается три вида платежей ($L = 3$) для двух вариантов по интервалам: доли платежей l-го вида: $c_1 = 0{,}333$; $c_2 = 0{,}333$; $c_3 = 0{,}334$; В1: интервалы между платежами: $h_1 = 7$ сут., $h_2 = 13$ сут., $h_3 = 25$ сут. Учитывая формулу (8), значения единичных платежей $Y_{0\,1} = 190{,}62$ тыс. р.; $Y_{0\,2} = 354{,}02$ тыс. р.; $Y_{0\,3} =$ $= 682{,}84$ тыс. р.; В2: интервалы между платежами: $h_1 = 3$ сут., $h_2 = 9$ сут., $h_3 = 17$ сут. Значения единичных пла-

тежей Y_{01} = 81,70 тыс. р.; Y_{02} = 245,09 тыс. р.; Y_{03} = 464,33 тыс. р.

Варианты В1 и В2 отличаются величиной интервалов между платежами, в варианте В2 они меньше.

В табл. 2 и 3 приведены результаты моделирования (значения однофакторных показателей эффективности), V – варианты моделирования с учетом значения коэффициента g.

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

j	1	2	3	4	5
В. м. для интер.	Норм.	Бета	Равн.	Бета	Норм.
mt_j, сут.	30,0	60,0	30,0	5,0	45,0
kvt_j	0,20	0,10	0,10	0,10	0,10
В. м. для затрат	Логнорм.	Б.-С.	Парето	Логнорм.	Гамма
mz_j, тыс. р.	700,0	1 000,0	200,0	120,0	500,0
kvz_j	0,25	0,25	1,25	0,30	0,15

Таблица 2. Результаты моделирования 1: значения показателей эффективности
Table 2. Simulation results 1: values of performance indicators

V, g	S_t, сут.	k_τ	$\tilde{R}_\tau$	τ_1	τ_2	$\tilde{c}_\tau$, %	v_1, %	v_2, %
В1 0,05	90	689	0,0345	0,0324	0,0366	19,80	17,17	22,82
	180	2 416	0,1208	0,1170	0,1247	34,45	32,50	36,52
	270	4 043	0,2021	0,1975	0,2069	39,60	37,97	41,30
	360	5 446	0,2723	0,2671	0,2775	43,99	42,51	45,53
В2 0,05	90	370	0,0185	0,0170	0,0201	20,34	16,79	24,64
	180	1 570	0,0785	0,0754	0,0817	33,26	30,90	35,80
	270	2 948	0,1474	0,1433	0,1516	36,75	34,92	38,68
	360	4 120	0,2060	0,2013	0,2108	40,93	39,29	42,65
В1 0,10	90	18	0,0009	0,0006	0,0013	23,36	10,10	54,06
	180	140	0,0070	0,0061	0,0080	27,58	21,03	36,17
	270	423	0,0211	0,0195	0,0229	26,59	22,70	31,16
	360	829	0,0415	0,0392	0,0438	28,35	25,41	31,63
В2 0,10	90	16	0,0008	0,0005	0,0012	19,90	7,61	52,02
	180	85	0,0043	0,0035	0,0051	31,29	22,55	43,43
	270	276	0,0138	0,0125	0,0152	27,71	22,86	33,59
	360	583	0,0291	0,0272	0,0312	28,32	24,85	32,28

Таблица 3. Результаты моделирования 2: значения показателей эффективности
Table 3. Simulation results 2: values of performance indicators

V, g	S_t, сут.	k_τ	RD_0	RD_1	RD_2	RU_0	RU_1	RU_2
В1 0,05	90	689	6 165,8	6 089,3	6 242,3	5 931,4	5 856,5	6 006,2
	180	2 416	10 405,7	10 275,9	10 535,5	10 173,0	10 043,8	10 302,2
	270	4 043	13 888,8	13 730,7	14 046,9	13 656,9	13 499,1	13 814,7
	360	5 446	17 095,7	16 907,4	17 284,1	16 863,3	16 675,1	17 051,4
В2 0,05	90	370	6 254,4	6 151,9	6 356,9	5 999,2	5 894,5	6 104,0
	180	1 570	11 053,6	10 891,9	11 215,2	10 809,6	10 648,1	10 971,0
	270	2 948	14 934,6	14 752,7	15 116,5	14 689,5	14 507,9	14 871,2
	360	4 120	18 375,2	18 161,1	18 589,2	18 134,2	17 920,1	18 348,2
В1 0,10	90	18	7 745,8	7 254,7	8 236,8	7 411,2	6 872,4	7 950,1
	180	140	13 627,5	13 127,7	14 127,3	13 314,4	12 811,4	13 817,3
	270	423	18 517,9	18 113,2	18 922,7	18 254,1	17 847,3	18 660,9
	360	829	23 187,1	22 788,9	23 585,3	22 932,6	22 533,6	23 331,6
В2 0,10	90	16	7 792,0	7 247,0	8 337,0	7 400,3	6 915,6	7 885,1
	180	85	13 324,8	12 622,2	14 027,4	13 040,2	12 328,9	13 751,4
	270	276	18 769,8	18 244,3	19 295,2	18 501,5	17 974,9	19 028,1
	360	583	23 982,7	23 494,2	24 471,2	23 730,5	23 241,3	24 219,7

Для варианта В2 точечные оценки риска (13) значимо (доверительные интервалы не пересекаются) меньше, чем для варианта В1 для обоих случаев ($g = 0{,}05$ и $g = 0{,}10$). Точечные оценки финансовых рисков (21), (24) для варианта В2 значимо больше, чем для варианта В1 для обоих случаев. Таким образом, можно сделать вывод, что интервалы между платежами желательно уменьшать.

Риск в виде точечной оценки коэффициента вариации (12) также подтверждает этот вывод, но не всегда значимо (доверительные интервалы иногда пересекаются). Это связано с тем, что оценки коэффициента вариации достаточно чувствительны к объему выборки из-за необходимости оценки среднеквадратического отклонения.

Заключение

Проведено обоснование системного подхода при моделировании работ по устранению инцидентов информационной безопасности. Показано, что при использовании денежного фонда процесс, описывающий его состояние, имеет нестационарный характер, хотя взаимодействующие денежные потоки являются либо регулярными, либо стационарными.

Предложены дополнительно к существующим два однофакторных финансовых риска в виде математических ожиданий случайных величин. При имитационном моделировании они вычисляются через точечные и интервальные оценки.

С учетом изменения математического обеспечения доработано программное обеспечение, ядром которого является моделирующая программа на основе дискретно-имитационного моделирования. Программное обеспечение разработано с использованием языка программирования Python версии 3.12.

Проведена апробация предложенного программно-алгоритмического обеспечения, получены научные и практические рекомендации.

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. Ким В.В., Белан Л.С. Экономический рост и перспективы инновационного развития России // Вестн. Тул. филиала Финуниверситета. 2023. № 1. С. 244–245.

4. 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.

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

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

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

8. Ковалева Н.Д., Гузич Ю.В. Применение корпоративных информационных систем в условиях импортозамещения // Актуальные проблемы развития современной экономики : сб. тез. студентов и магистров III межвуз. студен. науч.-теорет. конф. Ростов-на-Дону, 2015. Т. IV. С. 96–102.

9. Верещагин И.Ю. Современные угрозы и риски информационной безопасности корпоративных систем в условиях импортозамещения // Вестник Евразийской науки. 2024. Т. 16. № S4. URL: https://esj.today/PDF/28FAVN424.pdf (Дата обращения 01.02.2025).

10. Алиева М.М. Изменение бизнес-модели корпоративной информационной системы логистической компании в условиях новой реальности // Молодежь и ее роль в современной экономике и обществе: проблемы и перспективы взаимодействия : сб. науч. тр. Междунар. науч.-практ. конф. студентов и молодых ученых. М., 2022. С. 103–107.

11. 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.

12. 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.

13. 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.

14. Краковский Ю.М. Методы и средства защиты информации. СПб. : Лань, 2024. 272 с.

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

16. 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.

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

18. Краковский Ю.М., Киргизбаев В.П. Влияние вероятностных моделей работ, связанных с защитой информации, на значения показателей эффективности // Информационные и математические технологии в науке и управлении. 2024. № 3 (35). С. 112–119.

19. 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.

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

21. Краковский Ю.М., Хоанг Н.А. Моделирование ремонтных работ оборудования на основе случайного процесса риска // Прикладная информатика. 2020. Т. 15. № 6. С. 5–15.

22. Холлендер М., Вулф Д.А. Непараметрические методы статистики. М. : Финансы и статистика, 1983. 518 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.

25. Мак Т. Математика рискового страхования. М. : Олимп-Бизнес, 2005. 432 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. Kim V.V., Belan L.S. Ekonomicheskii rost i perspektivy innovatsionnogo razvitiya Rossii [Economic growth and prospects for innovative development of Russia]. *Vestnik Tul'skogo filiala Finuniversiteta* [Bulletin of the Tula Branch of the Financial University], 2023, no 1, pp. 244–245.

4. 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.

5. 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.

6. 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.

7. 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.

8. Kovaleva N.D., Guzich Yu.V. Primenenie korporativnykh informatsionnykh sistem v usloviyakh importozameshcheniya [The use of corporate information systems under import substitution conditions]. *Sbornik tezisov studentov i magistrantov III mezhvuzovskoi nauchno-teoreticheskoi konferentsii «Aktual'nye problemy razvitiia sovremennoi ekonomiki»* [Proceedings of the III Interuniversity Student Scientific and Theoretical Conference «Actual Issues of Modern Economic Development»]. Rostov-on-Don, 2015, Vol. 4, pp. 96–102.

9. Vereshchagin I.Yu. Sovremennye ugrozy i riski informatsionnoi bezopasnosti korporativnykh sistem v usloviyakh importozameshcheniya [Modern threats and risks to information security of corporate systems under import substitution conditions]. *Vestnik Evraziiskoi nauki* [Bulletin of Eurasian Science], 2024, Vol. 16, iss. S4. Available at: https://esj.today/PDF/28FAVN424.pdf (Accessed February 1, 2025).

10. Alieva M.M. Izmenenie biznes-modeli korporativnoi informatsionnoi sistemy logisticheskoi kompanii v usloviyakh novoi real'nosti [Changing the business model of a corporate information system of a logistics company under the new reality]. *Sbornik nauchnykh trudov ezhegodnoi Mezhdunarodnoi nauchno-prakticheskoi konferentsii studentov i molodykh uchenykh «Molodezh' i ee rol' v sovremennoi ekonomike i obshchestve: problemy i perspektivy vzaimodeistviia»* [Proceedings of the Annual International Scientific-Practical Conference of Students and Young Scientists «Youth and Its Role in the Modern Economy and Society: Problems and Prospects for Interaction»]. Moscow, 2022, pp. 103–107.

11. 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.

12. 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.

13. 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.

14. Krakovskii Y.M. Metody i sredstva zashchity informatsii [Methods and Means of Information Protection]. Saint Petersburg: Lan' Publ., 2024. 272 p.

15. 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.

16. 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.

17. 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.

18. Krakovskii Y.M., Kirgizbaev V.P. Vliyanie veroyatnostnykh modelei rabot, svyazannykh s zashchitoi informatsii, na znacheniya pokazatelei effektivnosti [The influence of probabilistic models of work related to information protection on the values of efficiency indicators]. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii* [Information and Mathematical Technologies in Science and Management], 2024, no 3 (35), pp. 112–119.

19. 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.

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

21. Krakovskii Y.M., Khoang N.A. Modelirovanie remontnykh rabot oborudovaniya na osnove sluchainogo protsessa riska [Modeling of equipment repair works based on a random risk process]. *Prikladnaya informatika* [Applied Informatics], 2020, Vol. 15, no 6, pp. 5–15.

22. Hollander M., Wolfe D.A. Neparametricheskie metody statistiki [Nonparametric Statistical Methods]. Moscow: Finansy i statistika Publ., 1983. 518 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.

25. Mack T. Matematika riskovogo strakhovaniia [Mathematics of Risk Insurance]. Moscow: Olimp-Biznes Publ., 2005. 432 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, Postgraduate Student of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk; e-mail: v.p.kirgizbaev@gmail.com.

