Научная статья
УДК 004.056; DOI: 10.61260/2218-130X-2026-2-82-91

МЕТОДИКА ФОРМИРОВАНИЯ ПОКАЗАТЕЛЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

✉**Лукоянов Алексей Александрович.**
АНО «Проектный офис по развитию туризма и гостеприимства Москвы», Москва, Россия.
Рогозин Евгений Алексеевич.
Воронежский институт МВД России, г. Воронеж, Россия.
Рогозин Руслан Евгеньевич.
МИРЭА – Российский технологический университет, Москва, Россия.
Калач Андрей Владимирович.
Воронежский институт ФСИН России, г. Воронеж, Россия
✉***9261781233@mail.ru***

Аннотация. Рассматривается задача формирования показателя защищенности информационных систем как инструмента оценки текущего состояния защиты информации. Актуальность исследования обусловлена необходимостью перехода от частных результатов контроля и мониторинга к единой интегральной количественной оценке. Предложена математическая модель показателя, включающая базовую интегральную оценку состояния защищенности и корректирующий коэффициент, учитывающий интегральный показатель остаточного риска. Базовая часть строится на основе взвешенного геометрического среднего частных критериев, отражающих состояние ключевых направлений защиты: выявление угроз и управление уязвимостями, контроль конфигураций и обновлений, управление доступом, мониторинг информационной безопасности, результаты контроля уровня защищенности и способность системы к восстановлению значимых функций. Интегральный показатель остаточного риска характеризует факторы, сохраняющие негативное влияние на состояние защиты информации после учета базовых характеристик защищенности. Научная новизна работы состоит в формализации процедуры расчета показателя защищенности автоматизированных информационных систем в виде аналитической модели, учитывающей как уровень реализации процессов защиты, так и влияние остаточного риска. Практическая значимость заключается в возможности применения подхода при внутреннем контроле защищенности, анализе динамики состояния систем, подготовке управленческих решений и автоматизированном расчете показателя.

Ключевые слова: информационная безопасность, информационная система, защищенность, показатель защищенности, контроль уровня защищенности, управление уязвимостями, мониторинг информационной безопасности, управление доступом

Для цитирования: Методика формирования показателя защищенности автоматизированных информационных систем / А.А. Лукоянов [и др.] // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 2. С. 82–91. DOI: 10.61260/2218-130X-2026-2-82-91

Scientific article

METHODOLOGY FOR DEVELOPING A SECURITY INDEX FOR AUTOMATED INFORMATION SYSTEMS

✉**Lukoyanov Alexey A.**
Project office for the development of tourism and hospitality in Moscow, Moscow, Russia.
Rogozin Evgeniy A.
Voronezh Institute of the Ministry of the Interior of Russia, Voronezh, Russia.
Rogozin Ruslan E.
MIREA – Russian technological university, Moscow, Russia.
Kalach Andrey V.
VRI of the FPS of Russia, Voronezh, Russia
✉***9261781233@mail.ru***

Abstract. The article considers the problem of forming a security index for information systems as a tool for assessing the current state of information protection. The relevance of the study is determined by the need to move from partial control and monitoring results to a unified integral quantitative assessment. A mathematical model of the index is proposed. The model includes a basic integral assessment of the security state and a corrective coefficient that takes into account an integral residual risk indicator. The basic part is constructed using a weighted geometric mean of partial criteria reflecting key areas of protection: threat identification and vulnerability management, configuration and update control, access management, information security monitoring, security-level control results, and the ability of the system to restore significant functions. The residual risk indicator characterizes factors that continue to have a negative impact on the state of information protection after the basic security characteristics have been taken into account. The novelty of the study lies in the formalization of the procedure for calculating the security index of automated information systems in the form of an analytical model that takes into account both the level of implementation of protection processes and the impact of residual risk. The practical significance lies in the possibility of applying the approach to internal security control, analysis of system dynamics, managerial decision-making, and automated calculation of the index.

Keywords: information security, information system, security, security index, security-level control, vulnerability management, information security monitoring, access management

For citation: Methodology for developing a security index for automated information systems / A.A. Lukoyanov [et al.] // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 2. P. 82–91. DOI: 10.61260/2218-130X-2026-2-82-91

Введение

Проблема количественной оценки защищенности информационных систем занимает важное место в исследованиях по информационной безопасности. В отечественных работах отмечается, что методы оценки защищенности автоматизированных и информационных систем существенно различаются по критериям, математическому аппарату и области применения, а универсальный подход к формированию интегральной оценки защищенности в процессе эксплуатации пока отсутствует [1–3]. Исследования в этой области охватывают сравнительный анализ методов оценки защищенности автоматизированных систем [1], подходы к оценке уровня защищенности информационных систем в процессе эксплуатации [2], а также методики оценивания защищенности на основе семантических моделей метрик и данных [3]. Наряду с этим предложены подходы к комплексной оценке состояния информационной безопасности предприятия и эффективности систем защиты информации [4–6]. Однако такие работы либо ориентированы на более широкий класс задач, либо не связаны непосредственно

с формированием показателя защищенности в соответствии с положениями методического документа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 12 апреля 2026 г[1].

В зарубежных исследованиях проблема SecurityMetrics (метрик информационной безопасности) рассматривается как задача построения измеримых, интерпретируемых и контекстно-зависимых показателей для оценки состояния безопасности и поддержки управленческих решений [7–12]. Область метрик информационной безопасности характеризуется терминологической неоднородностью и множественностью подходов [7], требует формальных оснований и увязки с задачами риск-менеджмента [8], а также допускает формализованное представление связи уязвимостей, угроз и механизмов защиты [9]. Метрики информационной безопасности должны разрабатываться с учетом целей организации, особенностей управленческих процессов, класса защищаемой системы и условий ее эксплуатации [10–12].

Целью работы является разработка модели формирования показателя защищенности информационных систем для оценки текущего состояния защиты информации. Для достижения цели решаются задачи обоснования состава частных критериев, разработки математической модели показателя защищенности и демонстрации ее применения на примере.

Материалы и методы исследования

Теоретическую основу исследования составили положения методического документа ФСТЭК России от 12 апреля 2026 г., а также требования к защите информации, закрепленные приказом ФСТЭК России от 11 апреля 2025 г. № 117[2]. При построении модели учитывались положения национальных стандартов в области мониторинга информационной безопасности, регистрации событий безопасности, идентификации и аутентификации, разработки безопасного программного обеспечения и управления компьютерными инцидентами[3]. Наряду с этим использовались международные подходы к измерению, мониторингу и оценке информационной безопасности[4]. Их учет позволяет рассматривать состояние защиты информации как совокупность измеримых показателей, пригодных для мониторинга, анализа и последующего принятия управленческих решений.

В ходе исследования применялись методы системного анализа, формализации, агрегирования частных критериев и математического моделирования. Методическая логика

[1] Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах: метод. документ (утв. ФСТЭК России 12 апр. 2026 г.). Доступ из инф.-правового портала «Гарант»

[2] Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений: утв. приказом ФСТЭК России от 11 апр. 2025 г. № 117. Доступ из инф.-правового портала «Гарант»

[3] ГОСТ Р 59547–2021. Защита информации. Мониторинг информационной безопасности. Общие положения; ГОСТ Р 59548–2022. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации; ГОСТ Р 58833–2020. Защита информации. Идентификация и аутентификация. Общие положения; ГОСТ Р 56939–2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования; ГОСТ Р 59710–2022. Защита информации. Управление компьютерными инцидентами. Общие положения. Доступ из инф.-правового портала «Гарант»

[4] ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation; ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks; National Institute of Standards and Technology. NIST SP 800–55 Vol. 1. Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures. Gaithersburg, MD, 2024; National Institute of Standards and Technology. NIST SP 800–55 Vol. 2. Measurement Guide for Information Security: Volume 2 – Developing an Information Security Measurement Program. Gaithersburg, MD, 2024

построения показателя определяется рядом исходных положений. Состояние защиты информации изменяется во времени под воздействием организационных и технических факторов. Защищенность информационной системы должна оцениваться по нескольким направлениям, а не по одному частному признаку. Существенные остаточные нарушения не должны полностью компенсироваться высокими значениями иных частных показателей. Итоговый показатель должен быть ограничен заданным интервалом и сохранять интерпретируемость. Совокупность указанных предпосылок обусловливает целесообразность построения двухкомпонентной модели, включающей базовую интегральную оценку и корректирующий коэффициент остаточного риска.

Результаты исследования и их обсуждение

Принципы формирования показателя защищенности информационных систем. В настоящей работе показатель $K_{\text{зи}}$ предлагается формировать на основе пяти принципов: динамичности, нормирования частных критериев, предметной полноты, ограничения взаимной компенсации и учета остаточного риска. Принцип динамичности отражает изменение эффективности мероприятий по защите информации во времени, а принцип предметной полноты требует включения критериев, характеризующих ключевые процессы защиты информации. Ограничение взаимной компенсации реализуется через использование взвешенного геометрического среднего, тогда как учет остаточного риска позволяет отразить факторы, ухудшающие фактическое состояние защищенности.

Математическая модель.

Предлагается рассчитывать показатель защищенности информационной системы по формуле (1).

$$K_{\text{зи}}(t) = K_{\text{б}}(t) \cdot K_{\text{кор}}(t), \quad (1)$$

где: $K_{\text{б}}(t)$ – базовая интегральная оценка состояния защищенности; $K_{\text{кор}}(t)$ – корректирующий коэффициент остаточного риска.

Базовая часть определяется как взвешенное геометрическое среднее частных критериев согласно формуле (2).

$$K_{\text{б}}(t) = \left(k_{vu}(t)^{w_1} \cdot k_{cf}(t)^{w_2} \cdot k_{ac}(t)^{w_3} \cdot k_{mo}(t)^{w_4} \cdot k_{ct}(t)^{w_5} \cdot k_{rs}(t)^{w_6} \right)^{\frac{1}{\sum_{i=1}^{6} w_i}}, \quad (2)$$

где: $k_{vu}(t)$ – частный критерий состояния по угрозам и уязвимостям; $k_{cf}(t)$ – частный критерий конфигурационной целостности и актуальности обновлений; $k_{ac}(t)$ – частный критерий состояния идентификации, аутентификации и управления доступом; $k_{mo}(t)$ – частный критерий мониторинга информационной безопасности и регистрации событий безопасности; $k_{ct}(t)$ – частный критерий результатов контроля уровня защищенности; $k_{rs}(t)$ – частный критерий устойчивости и восстановления значимых функций; w_i – коэффициенты значимости частных критериев.

Состав базовых критериев соответствует структуре процессов защиты информации, закрепленных в методическом документе ФСТЭК России[5] и профильных стандартах[6]. На рис. 1 представлена схема формирования итогового показателя защищенности на основе частных критериев и факторов остаточного риска.

[5] Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах: метод. документ (утв. ФСТЭК России 12 апр. 2026 г.). Доступ из инф.-правового портала «Гарант»

[6] ГОСТ Р 59547–2021; ГОСТ Р 59548–2022; ГОСТ Р 58833–2020; ГОСТ Р 56939–2024; ГОСТ Р 59710–2022. ISO/IEC 27004:2016; ISO/IEC 27005:2022; NIST SP 800–55 Vol. 1-2 (Measurement Guide for Information Security), 2024. Доступ из инф.-правового портала «Гарант».

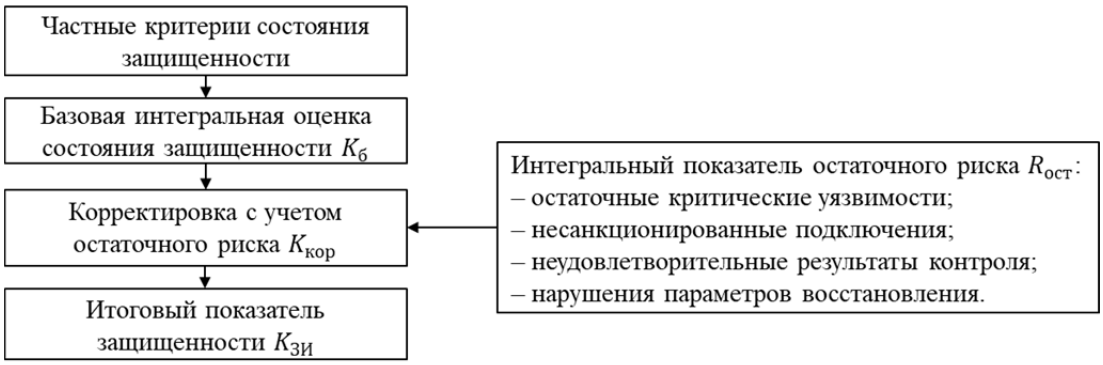

Рис. 1. **Структурная схема формирования показателя защищенности**

Интегральный показатель остаточного риска представляет собой агрегированную количественную оценку факторов, сохраняющих негативное влияние на состояние защиты информации после учета базовых характеристик защищенности. К таким факторам относятся остаточные критические уязвимости, несанкционированные подключения, неудовлетворительные результаты контроля уровня защищенности и превышение установленных интервалов восстановления значимых функций. Выделение данного показателя в отдельный элемент модели обусловлено тем, что эти факторы не должны полностью компенсироваться высокими значениями иных частных критериев.

Корректирующий коэффициент остаточного риска предлагается определять через интегральный показатель остаточного риска:

$$K_{кор}(t) = e^{-\lambda R_{ост}(t)}, \quad 0 < K_{кор}(t) \leq 1, \tag{3}$$

где: $\lambda \geq 0$ – коэффициент чувствительности модели к остаточному риску; $R_{ост}(t)$ – интегральный показатель остаточного риска.

На рис. 2 показана зависимость корректирующего коэффициента остаточного риска от интегрального показателя остаточного риска при трех расчетных сценариях: пониженном ($\lambda = 0{,}5$), базовом ($\lambda = 1{,}0$) и повышенном ($\lambda = 1{,}5$) уровне чувствительности модели. Эти сценарии позволяют сопоставить различные уровни чувствительности модели к остаточному риску при оценке защищенности автоматизированной информационной системы.

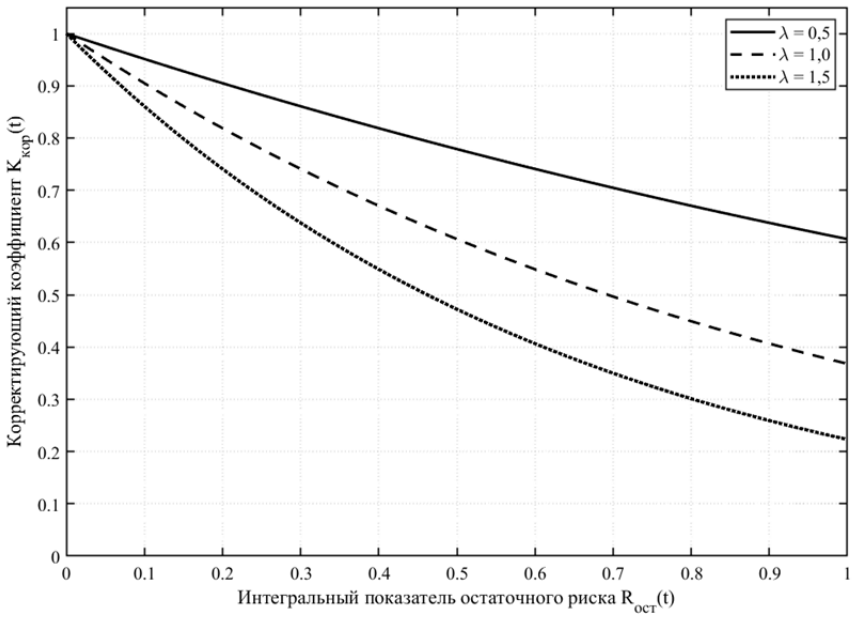

Рис. 2. **Зависимость корректирующего коэффициента остаточного риска от интегрального показателя остаточного риска**

Представленная зависимость показывает, что при увеличении интегрального показателя остаточного риска корректирующий коэффициент монотонно уменьшается. Коэффициент чувствительности определяет характер этого уменьшения и, соответственно, изменение итогового показателя защищенности при изменении интегрального показателя остаточного риска.

Интегральный показатель остаточного риска определяется по формуле:

$$R_{\text{ост}}(t) = \mu_1 r_v(t) + \mu_2 r_u(t) + \mu_3 r_c(t) + \mu_4 r_r(t), \qquad \sum_{j=1}^{4} u_j = 1, \tag{4}$$

где: $r_v(t)$ – нормированная оценка остаточных критических уязвимостей; $r_u(t)$ – нормированная оценка фактов несанкционированных подключений неразрешенных устройств; $r_c(t)$ – нормированная оценка неудовлетворительных результатов контроля уровня защищенности, включая моделирование реализации актуальных угроз и тренировки; $r_r(t)$ – нормированная оценка нарушений параметров восстановления значимых функций; $\mu_1, \mu_2, \mu_3, \mu_4$ – весовые коэффициенты значимости соответствующих компонент интегрального показателя остаточного риска ($\mu_j \in [0;1]$, $\sum_{j=1}^{4} \mu_j = 1$). Значения коэффициентов μ_j задаются экспертно с учетом особенностей автоматизированной информационной системы, значимости защищаемых ресурсов и потенциальных последствий реализации соответствующих факторов риска.

Включение именно этих компонент в формулу (4) обусловлено содержанием методического документа ФСТЭК России. В документе отдельно акцентируются критичность уязвимостей и необходимость их своевременного устранения либо применения компенсирующих мер, выявление несанкционированных подключений, результаты контроля уровня защищенности, а также соблюдение интервалов восстановления значимых функций. Интегральный показатель остаточного риска в предлагаемой модели используется как математический механизм учета факторов, сохраняющих непосредственное влияние на реальное состояние защищенности.

Использование экспоненциальной функции в формуле (3) обусловлено тем, что она обеспечивает ограничение коэффициента в интервале $(0;1]$, сохраняет непрерывность модели и позволяет регулировать влияние остаточного риска на итоговую оценку. При $R_{\text{ост}}(t) = 0$ коэффициент $K_{\text{кор}}(t)$ равен единице и не изменяет базовую оценку; при росте остаточного риска итоговое значение $K_{\text{зи}}(t)$, определяемое по формуле (1), уменьшается.

Формирование частных критериев.

Каждый частный критерий $k_i(t)$ предлагается рассчитывать по общей нормированной схеме:

$$k_i(t) = \frac{\sum_{j=1}^{n_i} \alpha_{ij} s_{ij}(t)}{\sum_{j=1}^{n_i} \alpha_{ij}}, 0 \le s_{ij}(t) \le 1, \tag{5}$$

где: $s_{ij}(t)$ – нормированное значение $j-$го признака, характеризующего $i-$е направление защиты; α_{ij} – коэффициент значимости соответствующего признака. Для критерия $k_{vu}(t)$ в качестве признаков могут использоваться доля уязвимостей, устраненных в нормативный срок, доля критических уязвимостей, для которых реализованы компенсирующие меры, полнота актуализации сведений об уязвимостях и качество выявления актуальных угроз. Для критерия $k_{cf}(t)$ признаками могут выступать доля объектов инвентаризации, соответствующих утвержденным конфигурациям, доля выявленных и устраненных несанкционированных изменений, а также доля программных компонентов с актуальными и проверенными обновлениями. Критерий $k_{ac}(t)$ может включать долю учетных записей, отвечающих установленным требованиям идентификации и аутентификации, долю

привилегированных учетных записей, учтенных и контролируемых в установленном порядке, и долю субъектов доступа с минимально необходимыми правами. Критерий $k_{mo}(t)$ может учитывать полноту регистрации событий безопасности, долю источников, подключенных к централизованному сбору событий, своевременность анализа событий, качество корреляции и полноту реагирования. Критерий $k_{ct}(t)$ должен опираться на результаты периодического контроля уровня защищенности, включая долю успешно пройденных проверок, долю невоспроизводимых сценариев реализации актуальных угроз, отсутствие несанкционированных подключений и результаты тренировок. Критерий $k_{rs}(t)$ может строиться на основе доли значимых функций, восстановленных в нормативный интервал времени, полноты резервного копирования, успешности тестов восстановления и наличия ресурсов для непрерывного функционирования.

Расчет.

По результатам очередного периода наблюдения получены следующие значения частных критериев: $k_{vu} = 0{,}78$; $k_{cf} = 0{,}88$; $k_{ac} = 0{,}91$; $k_{mo} = 0{,}83$; $k_{ct} = 0{,}74$; $k_{rs} = 0{,}86$.

Коэффициенты значимости определены на основе экспертного ранжирования частных критериев по степени их влияния на итоговое состояние защищенности рассматриваемой информационной системы. Основанием для такого ранжирования служили назначение системы, значимость защищаемых ресурсов, последствия возможной реализации угроз и результаты фактических контрольных мероприятий. В соответствии с полученным ранжированием более высокие веса были присвоены критериям, характеризующим выявление угроз и уязвимостей, мониторинг информационной безопасности и результаты контроля уровня защищенности. После этого значения коэффициентов были приведены к нормированному виду при условии равенства их суммы единице: $w_1 = 0{,}22$; $w_2 = 0{,}15$; $w_3 = 0{,}20$; $w_4 = 0{,}18$; $w_5 = 0{,}15$; $w_6 = 0{,}10$.

Тогда по формуле (2) базовая интегральная оценка равна: $K_б = (0{,}78^{0{,}22} \cdot 0{,}88^{0{,}15} \cdot 0{,}91^{0{,}20} \cdot 0{,}83^{0{,}18} \cdot 0{,}74^{0{,}15} \cdot 0{,}86^{0{,}10}) = 0{,}8299$.

Нормированные показатели остаточного риска имеют значения: $r_v = 0{,}20$; $r_u = 0{,}05$; $r_c = 0{,}10$; $r_r = 0{,}08$, а их весовые коэффициенты: $\mu_1 = 0{,}40$; $\mu_2 = 0{,}20$; $\mu_3 = 0{,}25$; $\mu_4 = 0{,}15$.

Тогда по формуле (4) интегральный показатель остаточного риска составит: $R_{ост} = 0{,}40 \cdot 0{,}20 + 0{,}20 \cdot 0{,}05 + 0{,}25 \cdot 0{,}10 + 0{,}15 \cdot 0{,}08 = 0{,}127$.

При λ = 1 по формуле (3) корректирующий коэффициент остаточного риска равен: $K_{кор} = e^{-0{,}127} \approx 0{,}8808$.

Следовательно, по формуле (1) итоговый показатель защищенности автоматизированной информационной системы составит: $K_{зи} = 0{,}8299 \cdot 0{,}8808 \approx 0{,}731$.

Полученный результат показывает влияние остаточного риска на итоговую оценку и подтверждает применимость показателя для количественной оценки состояния защищенности и выбора приоритетных направлений ее повышения.

Анализ и интерпретация результатов. Предложенная модель согласуется с логикой методического документа ФСТЭК России. Использование взвешенного геометрического среднего ограничивает взаимную компенсацию частных критериев, а интегральный показатель остаточного риска обеспечивает учет факторов, существенно влияющих на состояние защиты информации. Модель допускает адаптацию к различным автоматизированным информационным системам за счет настройки состава критериев, весовых коэффициентов и параметра чувствительности.

Заключение

В работе предложена двухкомпонентная модель формирования показателя защищенности автоматизированных информационных систем, включающая базовую интегральную оценку и корректирующий коэффициент остаточного риска. Научный результат состоит в формализации процедуры расчета показателя защищенности, учитывающей уровень реализации ключевых процессов защиты информации и влияние

остаточных критических факторов. Практическая значимость состоит в возможности использования модели для внутреннего контроля защищенности, анализа состояния защищенности систем и обоснования мероприятий по защите информации. Перспективы дальнейших исследований связаны с настройкой весовых коэффициентов, эмпирической апробацией модели и сопоставлением значения $K_{зи}$ с результатами аттестационных и контрольных мероприятий.

Список источников

1. Ступина А.А., Золотарев А.В. Сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем // Вестник СибГАУ. 2012. № 4 (44). С. 56–61.

2. Борзенкова С.Ю., Казарина Е.Е. Анализ методов оценки уровня защищенности информационных систем в процессе их эксплуатации // Известия Тульского государственного университета. Технические науки. 2020. № 5. С. 93–97.

3. Методика оценивания защищенности на основе семантической модели метрик и данных / Е.В. Дойникова [и др.] // Вопросы кибербезопасности. 2021. № 1 (41). С. 29–40. DOI: 10.21681/2311-3456-2021-1-29-40

4. Александров А.В., Велигура А.В., Соколова Я.В. Методика комплексной оценки состояния информационной безопасности предприятия // Экономический вектор. 2016. № 2 (5). С. 104–112.

5. Комаров В.В., Буйневич М.В. Оценка и мониторинг защищенности информационных ресурсов как нештатная ситуация // Информационные технологии и телекоммуникации. 2023. Т. 11. № 4. С. 1–14. DOI: 10.31854/2307-1303-2023-11-4-1-14

6. Модель оценки эффективности систем защиты информации / Е.С. Митяков [и др.] // Безопасность информационных технологий. 2024. Т. 31. № 4. С. 56–66. DOI: 10.26583/bit.2024.4.03

7. Barabanov R., Kowalski S., Yngström L. Information Security Metrics: State of the P. DSV Report Series. № 11-007. Stockholm: Stockholm University, 2011. 62 p.

8. Trček D. Security Metrics Foundations for Computer Security // The Computer Journal. 2010. Vol. 53. № 7. P. 1106–1112. DOI: 10.1093/comjnl/bxp094

9. Chakraborty A., Sengupta A., Mazumdar C. A Formal Approach to Information Security Metrics // 2012 Third International Conference on Emerging Applications of Information Technology (EAIT). IEEE, 2012. P. 439–442.

10. Philippou E., Frey S., Rashid A. Contextualising and Aligning Security Metrics and Business Objectives: a GQM-based Methodology // Computers & Security. 2020. Vol. 88. P. 101634. DOI: 10.1016/j.cose.2019.101634

11. Diesch R., Krcmar H. SoK: Linking Information Security Metrics to Management Success Factors // Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020). 2020. DOI: 10.1145/3407023.3407059

12. Metrics for Cyber-Physical Security: a Call to Action / G. Gori [et al.] // 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022. P. 1–4. DOI: 10.1109/ISNCC55209.2022.9851735

13. A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems / G. Gori [et al.] // Electronics. 2024. Vol. 13. № 7. P. 1208. DOI: 10.3390/electronics13071208

References

1. Stupina A.A., Zolotarev A.V. Sravnitel'nyj analiz metodov resheniya zadachi ocenki zashchishchennosti avtomatizirovannyh sistem // Vestnik SibGAU. 2012. № 4 (44). S. 56–61.

2. Borzenkova S.Yu., Kazarina E.E. Analiz metodov ocenki urovnya zashchishchennosti informacionnyh sistem v processe ih ekspluatacii // Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2020. № 5. S. 93–97.

3. Metodika ocenivaniya zashchishchennosti na osnove semanticheskoj modeli metrik i dannyh / E.V. Dojnikova [i dr.] // Voprosy kiberbezopasnosti. 2021. № 1 (41). S. 29–40. DOI: 10.21681/2311-3456-2021-1-29-40

4. Aleksandrov A.V., Veligura A.V., Sokolova Ya.V. Metodika kompleksnoj ocenki sostoyaniya informacionnoj bezopasnosti predpriyatiya // Ekonomicheskij vektor. 2016. № 2 (5). S. 104–112.

5. Komarov V.V., Bujnevich M.V. Ocenka i monitoring zashchishchennosti informacionnyh resursov kak neshtatnaya situaciya // Informacionnye tekhnologii i telekommunikacii. 2023. T. 11. № 4. S. 1–14. DOI: 10.31854/2307-1303-2023-11-4-1-14

6. Model' ocenki effektivnosti sistem zashchity informacii / E.S. Mityakov [i dr.] // Bezopasnost' informacionnyh tekhnologij. 2024. T. 31. № 4. S. 56–66. DOI: 10.26583/bit.2024.4.03

7. Barabanov R., Kowalski S., Yngström L. Information Security Metrics: State of the P. DSV Report Series. № 11-007. Stockholm: Stockholm University, 2011. 62 p.

8. Trček D. Security Metrics Foundations for Computer Security // The Computer Journal. 2010. Vol. 53. № 7. P. 1106–1112. DOI: 10.1093/comjnl/bxp094

9. Chakraborty A., Sengupta A., Mazumdar C. A Formal Approach to Information Security Metrics // 2012 Third International Conference on Emerging Applications of Information Technology (EAIT). IEEE, 2012. P. 439–442.

10. Philippou E., Frey S., Rashid A. Contextualising and Aligning Security Metrics and Business Objectives: a GQM-based Methodology // Computers & Security. 2020. Vol. 88. P. 101634. DOI: 10.1016/j.cose.2019.101634

11. Diesch R., Krcmar H. SoK: Linking Information Security Metrics to Management Success Factors // Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020). 2020. DOI: 10.1145/3407023.3407059

12. Metrics for Cyber-Physical Security: a Call to Action / G. Gori [et al.] // 2022 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2022. P. 1–4. DOI: 10.1109/ISNCC55209.2022.9851735

13. A Systematic Analysis of Security Metrics for Industrial Cyber–Physical Systems / G. Gori [et al.] // Electronics. 2024. Vol. 13. № 7. P. 1208. DOI: 10.3390/electronics13071208

Информация о статье:
Статья поступила в редакцию: 21.03.2026; одобрена после рецензирования: 26.04.2026;
принята к публикации: 30.04.2026

Information about the article:
The article was submitted to the editorial office: 21.03.2026; approved after review: 26.04.2026;
accepted for publication: 30.04.2026

Информация об авторах:
Лукоянов Алексей Александрович, специалист по информационной безопасности АНО «Проектный офис по развитию туризма и гостеприимства Москвы» (125009, Москва, ул. Тверская, д. 5А), e-mail: 9261781233@mail.ru
Рогозин Евгений Алексеевич, профессор кафедры автоматизированных информационных систем органов внутренних дел Воронежского института МВД России (394065, г. Воронеж, пр. Патриотов, д. 53), доктор технических наук, профессор, e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535, SPIN-код: 4965-3462
Рогозин Руслан Евгеньевич, доцент кафедры корпоративных информационных систем Института информационных технологий МИРЭА – Российского технологического университета (119454, Москва, проспект Вернадского, д. 78), кандидат технических наук, e-mail: ruslan-96-01-09@mail.ru, https://orcid.org/0000-0002-2913-6038
Калач Андрей Владимирович, начальник кафедры безопасности информации и защиты сведений, составляющих государственную тайну, Воронежского института ФСИН России (394072, г. Воронеж, ул. Иркутская, д. 1А), доктор химических наук, профессор, почетный работник сферы образования Российской Федерации, e-mail: biizssgt@mail.ru, https://orcid.org/0000-0002-8926-3151, SPIN-код: 2584-7456

Information about authors:
Lukoyanov Alexey A., information security specialist at the project office for the development of tourism and hospitality in Moscow (125009, Moscow, Tverskaya st., 5A), e-mail: 9261781233@mail.ru
Rogozin Evgeny A., professor of the department of automated information systems of law enforcement agencies of Voronezh Institute of the Ministry of the Interior of Russia (394065, Voronezh, Patriotov ave., 53), doctor of technical sciences, professor, e-mail: evgenirogozin@yandex.ru , https://orcid.org/0000-0002-4455-7535, SPIN: 4965-3462
Rogozin Ruslan E.., associate professor of the department of corporate information systems at the Institute of information technology of the MIREA – Russian university of technology (119454, Moscow, Vernadsky ave., 78), candidate of technical sciences, e-mail: ruslan-96-01-09@mail.ru, https://orcid.org/0000-0002-2913-6038
Kalach Andrey V., head of the department of information security and protection of information constituting a state secret of Voronezh Institute of the Federal Penitentiary Service of Russia (394072, Voronezh, Irkutskaya str., 1A), doctor of chemical sciences, professor, honorary worker of education of the Russian Federation, e-mail: biizssgt@mail.ru, https://orcid.org/0000-0002-8926-3151, SPIN: 2584-7456