

Полумарковская модель для оценки эффективности программных систем защиты информации

И.И. Застрожнов¹, О.В. Ланкин¹, Е.А. Рогозин¹, Ю.В. Биктимирова¹, А.А. Лукоянов²

¹Воронежский институт МВД России,

¹394065, г. Воронеж, пр. Патриотов, 53, Россия,

²Всероссийский научно-исследовательский институт документоведения и архивного дела,

²117393, г. Москва, ул. Профсоюзная, 82, Россия

Резюме. Цель. Целью настоящей работы является разработка и обоснование математической модели для оценки вероятностно-временных характеристик программных систем защиты информации (ПСЗИ) в процессе контроля их эффективности. **Метод.** В качестве метода решения поставленной задачи предложен математический аппарат на основе конечных полумарковских процессов (КПП), что позволяет адекватно описать стохастическую природу функционирования ПСЗИ и учесть распределения времени пребывания системы в различных состояниях. **Результат.** Предложена математическая модель для оценки вероятностно-временных характеристик ПСЗИ, основанная на аппарате КПП. Данный подход позволяет адекватно описать стохастическую природу функционирования ПСЗИ и учесть произвольные законы распределения времени выполнения операций. В рамках модели вводится количественный показатель эффективности, определяемый как вероятность выполнения защитных функций в течение времени, не превышающего максимально допустимое. Для аналитического расчета показателя система интегральных уравнений, описывающая динамику КПП, с помощью преобразования Лапласа-Стилтьеса сводится к системе линейных алгебраических уравнений, решаемой методом Гаусса. **Вывод.** Предложенный подход обеспечивает аналитичность исследования вероятностно-временных характеристик ПСЗИ. Полученная система линейных уравнений позволяет вычислять интегральный показатель эффективности системы без необходимости трудоемкого имитационного моделирования, что особенно ценно для оперативного контроля. Данный метод может быть легко алгоритмизирован и внедрен в средства автоматизированного мониторинга защищенных автоматизированных систем.

Ключевые слова: программные системы защиты информации, эффективность, контроль, вероятностно-временные характеристики, полумарковский процесс, преобразование Лапласа-Стилтьеса, показатель своевременности

Для цитирования: И.И. Застрожнов, О.В. Ланкин, Е.А. Рогозин, Ю.В. Биктимирова, А.А. Лукоянов. Полумарковская модель для оценки эффективности программных систем защиты информации. Вестник Дагестанского государственного технического университета. Технические науки. 2026; 53(2):88-95. DOI:10.21822/2073-6185-2026-53-2-88-95

A semi-Markov model for evaluating the effectiveness of information security software systems

I.I. Zastrozhnov¹, O. V. Lankin¹, E.A. Rogozin¹, J. V. Biktimirova¹, A. A. Lukoyanov²

¹Voronezh Institute of the Ministry of Internal Affairs of Russia,

¹53 Patriotov St., Voronezh 394065, Russia

²All-Russian Archival Science and Records Management Research Institute

²82 Trade Union St., Moscow 2117393, Russia

Abstract. Objective. The purpose of this work is to develop and substantiate a mathematical model for evaluating the probabilistic and temporal characteristics of information security

software systems (ISSS) in the process of monitoring their effectiveness. **Method.** A mathematical framework based on finite semi-Markov processes (FSPs) is proposed as a solution to the problem. This allows for an adequate description of the stochastic nature of the functioning of the PSSI and takes into account the distribution of the system's dwell time in various states. **Result.** A mathematical model for assessing the probabilistic-temporal characteristics of a security system (PSS), based on the KPP framework, is proposed. The model adequately describes the stochastic nature of PSS operation and accounts for arbitrary laws of operation time distribution. A quantitative performance indicator is introduced, defined as the probability of performing protective functions within a time limit not exceeding the maximum permissible time. To analytically calculate this indicator, the system of integral equations describing the PPS dynamics is reduced to a system of linear algebraic equations solved using the Gaussian method using the Laplace-Stieltjes transform. **Conclusion.** This approach ensures analytical analysis of the probabilistic and temporal characteristics of security systems. A system of linear equations allows for calculating the integrated system performance indicator without simulation, which is valuable for operational monitoring. The method can be easily algorithmized and integrated into automated monitoring tools for secure automated systems.

Keywords: information security software systems, effectiveness, monitoring, probabilistic-time characteristics, semi-Markov process, Laplace-Stieltjes transform, timeliness indicator.

For citation: I.I. Zastrozhnov, O.V. Lankin, E.A. Rogozin, J.V. Biktimirova, A.A. Lukoyanov. A semi-Markov model for evaluating the effectiveness of information security software systems. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(2):88-95. (In Russ) DOI:10.21822/2073-6185-2026-53-2-88-95

Введение. Актуальность обеспечения информационной безопасности автоматизированных систем (АС) в современных условиях невозможно переоценить. Рост сложности кибератак, увеличение объемов обрабатываемой информации и ужесточение нормативных требований диктуют необходимость использования надежных программных систем защиты информации (ПСЗИ). Однако сама по себе установка ПСЗИ не является гарантией защищенности. Ключевое значение приобретает регулярный контроль их эффективности, направленный на поддержание способности системы выполнять свои функции в условиях реальных угроз и нагрузок. В соответствии с требованиями документов, регламентирующих защиту информации в АС [1-6] и, в частности, с пунктом 3.7 Руководящего документа Гостехкомиссии России [4], такой контроль должен носить периодический характер.

Одним из критически важных аспектов эффективности ПСЗИ являются ее вероятностно-временные характеристики (ВВХ). Скорость реакции системы на инцидент или запрос напрямую влияет на уровень защищенности АС. Задержка в выполнении защитных функций, превышающая максимально допустимое время, может не только привести к реализации угрозы конфиденциальности, целостности или доступности информации, но и негативно сказаться на общей производительности автоматизированной системы по ее прямому назначению [7-10].

Постановка задачи. Целью настоящей работы является разработка и детальное обоснование математической модели для оценки вероятностно-временных характеристик ПСЗИ в процессе контроля их эффективности. Модель основывается на аппарате конечных полумарковских процессов (КПП), что позволяет адекватно описать стохастическую природу функционирования ПСЗИ и учесть распределения времени пребывания системы в различных состояниях.

Методы исследования. В рамках модели вводится и аналитически рассчитывается количественный показатель эффективности, определяемый как вероятность своевременного выполнения ПСЗИ всех необходимых защитных функций. Программная система защиты информации представляет собой комплекс взаимодействующих модулей, реализующих заданный набор защитных функций (аутентификация, авторизация, аудит,

шифрование и т.д.). Эффективность функционирования такой системы в значительной степени определяется временем τ_{pi} , требуемым для обработки запроса и выполнения соответствующих защитных действий [10-12]. Это время отсчитывается от момента обращения к ПСЗИ до момента полного завершения обработки данного обращения. Эксплуатационной документацией на автоматизированную систему устанавливается максимально допустимое время τ_m выполнения защитных функций. Превышение времени τ_{pi} над τ_m является недопустимым по двум основным причинам [8-12]:

1. **Угроза безопасности.** Задержка может позволить злоумышленнику воспользоваться «окном уязвимости» для реализации атаки.
2. **Снижение производительности АС.** Длительная обработка запросов защиты создает «бутылочное горло», замедляющее работу автоматизированной системы.

Центральной задачей контроля эффективности становится оценка вероятности того, что ПСЗИ выполнит свои функции за время, не превышающее τ_m . Данная вероятность и предлагается в качестве ключевого количественного показателя эффективности E [11, 12]:

$$E = P(\tau_{pi} \leq \tau_m) \quad (1)$$

Для адекватности модели предполагается, что максимально допустимое время τ_m является случайной величиной, распределенной по экспоненциальному закону. Этот закон широко применяется для аппроксимации времени выполнения задач сложными системами, так как он характеризуется простотой и отсутствием последствия.

Полумарковская модель динамики функционирования ПСЗИ. Для формализации процесса функционирования ПСЗИ используется графовый подход [12-16]. Состояния ПСЗИ представляются в виде вершин графа, а переходы между состояниями (например, «Ожидание запроса» → «Аутентификация пользователя» → «Проверка прав доступа» → «Завершение обработки») – в виде ориентированных ребер. Общее число состояний обозначим как n . Состояние 1 является начальным (момент обращения к ПСЗИ), а состояние n – конечным, поглощающим (успешное завершение обработки запроса). Время τ_{pi} в этой модели есть время перехода из состояния 1 в состояние n .

Динамика такого процесса адекватно описывается с помощью конечного полумарковского процесса (КПП) [14-16]. В отличие от марковского процесса, где время пребывания в состоянии распределено экспоненциально, полумарковский процесс позволяет использовать произвольные законы распределения времени переходов между состояниями, что более точно отражает реальное поведение программных компонентов.

Математически модель задается полумарковской матрицей $H(\tau) = [H_{ij}(\tau)]$, где каждый элемент $H_{ij}(\tau)$ представляет собой функцию распределения вероятности того, что процесс, находясь в состоянии i , перейдет в состояние j за время, меньшее τ .

Эта функция выражается как $H_{ij}(\tau) = p_{ij} \cdot G_i(\tau)$,

где: p_{ij} – вероятность перехода из состояния i в состояние j (вероятностная составляющая); $G_i(\tau)$ – функция распределения времени нахождения процесса в состоянии i (временная составляющая).

Обсуждение результатов. Для анализа ВВХ такого поглощающего КПП используется аппарат интервально-переходных вероятностей [14,15]. Обозначим за $Q_i(\tau)$ вероятность того, что процесс, начавшийся в состоянии i , достигнет поглощающего состояния n за время, меньшее τ . Для определения этих вероятностей составляется система интегральных уравнений полной вероятности, учитывающая первый переход из начального состояния:

$$Q_i(\tau) = p_{in} \cdot G_i(\tau) + \sum_{j=1}^{n-1} p_{ij} \cdot G_i(\tau) * Q_j(\tau), \text{ для } i = 1, 2, \dots, n-1 \quad (2)$$

$$Q_n(\tau) = 1$$

Данная система утверждает, что вероятность попасть из состояния i в n за время τ равна сумме вероятностей всех возможных путей: перейти сначала в какое-либо состояние j , затратив на это время u , и затем из j попасть в n за оставшееся время $(\tau - u)$.

Решение системы интегральных уравнений (2) представляет значительную вычислительную сложность. Для ее упрощения применяется преобразование Лапласа-Стилтьеса

$$q_n(v) = 1 / v$$
$$q_n(v) = 1 / v$$
$$h_{ij} = h_{ij}(v); \quad q_i = q_i(v).$$
$$\left\{ \begin{array}{l} (1-h_{1,1})q_1 - h_{1,2}q_2 - h_{1,3}q_3 - \dots - h_{1,n-1}q_{n-1} = h_{1,n}; \\ -h_{2,1}q_1 + (1-h_{2,2})q_2 - h_{2,3}q_3 - \dots - h_{2,n-1}q_{n-1} = h_{2,n}; \\ \\ -h_{n-1,1}q_1 - h_{n-1,2}q_2 - h_{n-1,3}q_3 - \dots + (1-h_{n-1,n-1})q_{n-1} = h_{n-1,n}. \end{array} \right.$$

1. Прямой ход: последовательное исключение неизвестных путем элементарных преобразований строк системы.
2. Обратный ход: последовательное нахождение неизвестных, начиная с последнего уравнения.

Используя преобразования прямого хода метода Гаусса получаем систему:

$$\left\{ \begin{array}{l} q_1 - h_{1,2}^{(1)} q_2 - h_{1,3}^{(1)} q_3 - \dots - h_{1,n-1}^{(1)} q_{n-1} = h_{1,n}^{(1)}; \\ \quad q_2 - h_{2,3}^{(2)} q_3 - \dots - h_{2,n-1}^{(2)} q_{n-1} = h_{2,n}^{(2)}; \\ \dots \\ \quad \quad \quad q_{n-1} = h_{n-1,n}^{(n-1)}. \end{array} \right. \quad (6)$$

$$\text{где } h_{k,j}^{(k)} = \frac{h_{k,j}^{(k-1)}}{1 - h_{k,k}^{(k-1)}}, \quad h_{i,j}^{(k)} = h_{i,j}^{(k-1)} + h_{i,k}^{(k-1)} h_{k,j}^{(k)},$$

$$h_{ij}^{(0)} = h_{ij}, k=\overline{1, n-1}, i=\overline{k+1, n-1}, j=\overline{k+1, n}. \quad (7)$$

[illegible]

91

что позволяет точнее настраивать модель на реальные характеристики ПСЗИ. Приведем выражения для $g_i(v)$ для некоторых типовых распределений [12, 13]:

Экспоненциальное распределение (параметр b_i):

$$g_i(v) = \frac{1}{1+b_iv} \quad (9)$$

Равномерное распределение на отрезке $[a_i, b_i]$:

$$g_i(v) = \frac{\exp(-a_iv)[1-\exp(-b_iv)]}{b_iv} \quad (10)$$

Нормальное распределение с математическим ожиданием μ_i и дисперсией σ_i^2

$$(\text{при условии малой дисперсии}): g_i(v) = \exp(-\mu_iv + \frac{1}{2}\sigma_i^2v^2) \quad (11)$$

Итоговый показатель эффективности E , определяемый выражением (1), рассчитывается через найденную функцию $Q_1(\tau)$ в точке τ_m . Поскольку τ_m предполагается экспоненциально распределенной величиной с параметром $v_m = \frac{1}{\tau_m}$, искомый показатель вычисляется как значение преобразования Лапласа $q_1(v)$ при аргументе v_m :

$$E = q_1(v_m) \quad (12)$$

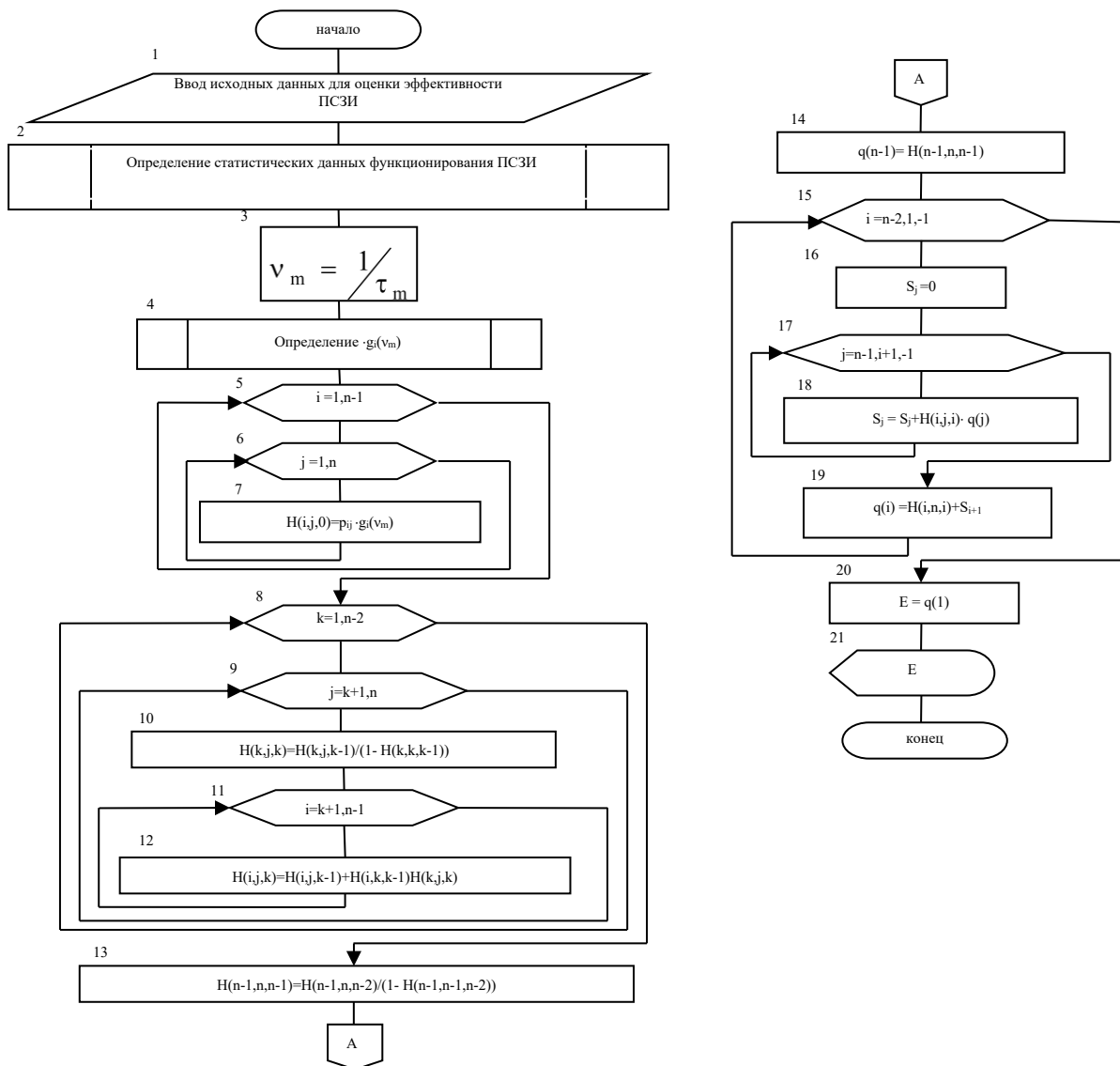


Рис. 1- Схема алгоритма оценки количественного показателя эффективности ПСЗИ

Fig. 1- Scheme of the algorithm for evaluating the quantitative indicator of the Efficiency of ISSS

Алгоритм оценки количественного показателя эффективности ПСЗИ представлен на рис. 1 и включает следующие шаги:

1. Формализация: построение графа состояний ПСЗИ и определение полумарковской матрицы $H(\tau)$ (оценка вероятностей p_{ij} и выбор законов распределения $G_i(\tau)$ на основе статистических данных или экспертных оценок) (блоки 1-2).
2. Подготовка расчетов: для заданного среднего значения $M[\tau_m]$ вычисляется параметр v_m . Для каждого состояния i вычисляется $g_i(v_m)$ по формуле (9)-(11) в соответствии с выбранным законом распределения (блоки 3-4).
3. Формирование системы: рассчитываются элементы $h_{ij}(v_m) = p_{ij} \cdot g_i(v_m)$ и формируется система линейных уравнений (4) (блоки 5-7).
4. Решение системы: система решается методом Гаусса, находится значение $q_i(v_m)$ (блоки 8-19).
5. Расчет показателя: по формуле (12) вычисляется итоговое значение вероятности своевременного выполнения функций E (блок 20).

Вывод. Разработанная математическая модель предоставляет мощный и гибкий инструмент для анализа вероятностно-временных характеристик программных систем защиты информации. Использование аппарата полумарковских процессов позволяет адекватно отразить стохастическую природу функционирования ПСЗИ и учесть различные законы распределения времени выполнения операций.

Основное преимущество предложенного подхода заключается в его аналитичности. Полученная система линейных уравнений позволяет вычислять интегральный показатель эффективности E без необходимости трудоемкого имитационного моделирования, что особенно ценно для оперативного контроля. Данный метод может быть легко алгоритмизирован и внедрен в средства автоматизированного мониторинга защищенных автоматизированных систем.

Основные преимущества предложенного подхода включают:

- научную обоснованность и математическую строгость;
 - практическую применимость для регулярного контроля;
 - возможность учета специфики конкретных ПСЗИ; вычислительную эффективность.
- Перспективными направлениями дальнейших исследований являются:
1. Разработка методов адаптивного контроля с динамическим изменением параметров модели.
 2. Учет взаимного влияния параллельных процессов в распределенных ПСЗИ.
 3. Создание автоматизированной системы мониторинга и оценки эффективности в реальном времени.

Предложенная методика может быть успешно внедрена в практику обеспечения информационной безопасности автоматизированных систем различного назначения.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 814-ст) — Текст : электронный.
2. ГОСТ Р ИСО/МЭК 15408-2-2013. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности" (утв. и введен в действие Приказом Росстандарта от 08.11.2013 N 1339-ст) — Текст : электронный.
3. ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования: приказ от 24.10.2024 № 1504-ст. — Текст : электронный.
4. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утв. Решением Гостехкомиссии России 30.03.1992). — Текст : электронный.
5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
7. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
8. Даниленко, А.Ю. Безопасность систем электронного документооборота. Технология защиты электронных документов / А.Ю. Даниленко. - М.: Ленанд, 2015. - 232 с.
9. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин: учеб. пособие. — М.: ДМК Пресс, 2017. — 702 с.
10. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / Е.А. Рогозин, М.В. Питолин, О.Ю. Макаров [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. 106 с.
11. Методика управления защитой информационного ресурса электронного документооборота / О.С. Авсентьев и [др.] // Труды СПИИРАН. — 2018. — № 2 (57). — С. 188 — 210. . — Текст : непосредственный.
12. Застрожнов И.И. Методологические основы безопасности использования информационных технологий в системах электронного документооборота [Текст]: монография / И.И. Застрожнов, Е.А. Рогозин, М.А. Багаев. — Воронеж: ИПЦ «Научная книга», 2011. — 252 с. — Текст : непосредственный.
13. Стражева, Н.А. Теория вероятностей и математическая статистика: учебник для вузов / Н.А. Стражева, Т.В. Капустина. — М.: Юрайт, 2021. — 311 с.
14. Тихонов, В.И. Марковские процессы / В.И. Тихонов, М.А. Миронов. — М.: Сов. радио, 1977. — 488 с. — Текст : непосредственный.
15. Ross, S.M. Introduction to Probability Models / S.M. Ross. — Academic Press, 2014. — 784 p.
16. Grinstead, C.M. Introduction to Probability / C.M. Grinstead, J.L. Snell. — American Mathematical Society, 1997. — 510 p.
17. Кудрявцев, В.А. Краткий курс высшей математики: Учебное пособие для вузов / В.А. Кудрявцев, Б.П. Демидович — М.: Наука, 1989. — 656 с. — Текст : непосредственный.
18. Бахвалов, Н.С. Численные методы: учебное пособие для вузов / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. — М.: Лаборатория знаний, 2015. — 636 с.
19. Самарский, А.А. Численные методы: учебное пособие для вузов / А.А. Самарский, А.В. Гулин. — М.: Лаборатория знаний, 2020. — 432 с.

References:

1. GOST R ISO/IEC 15408-1–2012. National Standard of the Russian Federation. Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 1. Introduction and General Model. (approved and enacted by Order of Rosstandart dated November 15, 2012 No. 814-st). Text: electronic. (In Russ)
2. GOST R ISO/IEC 15408-2–2013. National Standard of the Russian Federation. Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 2. Security Functional Components. (approved and enacted by Order of Rosstandart dated November 8, 2013 No. 1339-st). Text: electronic. . (In Russ)
3. GOST R 56939–2024. National Standard of the Russian Federation. Information Protection. Secure Software Development. General Requirements. (approved by Order of Rosstandart dated October 24, 2024 No. 1504-st). Text: electronic. (In Russ)
4. Guidance Document. The Concept of Protection of Computer Equipment and Automated Systems from Unauthorized Access to Information (approved by the Decision of the State Technical Commission of Russia dated March 30, 1992). Text: electronic. (In Russ)
5. Order of the Federal Service for Technical and Export Control of Russia (FSTEC of Russia) No. 17 of February 11, 2013. On Approval of the Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems. (In Russ)
6. Order of the Federal Service for Technical and Export Control of Russia (FSTEC of Russia) No. 239 of December 25, 2017. On Approval of the Requirements for Ensuring the Security of Critical Information Infrastructure Facilities of the Russian Federation. (In Russ)
7. Malyuk, A.A. Information Security: Conceptual and Methodological Foundations of Information Protection. Moscow: GLT, 2016. — 280 p. (In Russ)
8. Danilenko, A.Yu. Security of Electronic Document Management Systems. Technology for Protecting Electronic Documents. Moscow: Lenand, 2015. 232 p. (In Russ)
9. Shangin, V.F. Information Security and Information Protection: Textbook. Moscow: DMK Press, 2017. — 702 p. (In Russ)
10. Rogozin, E.A., Pitolin, M.V., Makarov, O.Yu. et al. Methods and Tools for Evaluating the Efficiency of the Information Protection Subsystem Design in Electronic Document Management Systems: Monograph. Voronezh: Voronezh State Technical University, 2015. — 106 p. (In Russ)
11. Avsentyev, O.S. et al. Methodology for Managing Information Resource Protection in Electronic Document Management Systems. *SPIIRAS Proceedings*, 2018;2 (57):188–210. Text: printed. (In Russ)

12. Zastrozhnov, I.I., Rogozin, E.A., Bagaev, M.A. Methodological Foundations of Security in the Use of Information Technologies in Electronic Document Management Systems: Monograph. Voronezh: Scientific Book Publishing Center, 2011. — 252 p. Text: printed. (In Russ)
13. Strazheva, N.A., Kapustina, T.V. Probability Theory and Mathematical Statistics: Textbook for Universities. Moscow: Yurayt, 2021. 311 p. (In Russ)
14. Tikhonov, V.I., Mironov, M.A. Markov Processes. Moscow: Soviet Radio, 1977. 488 p. Text: printed. (In Russ)
15. Ross, S.M. Introduction to Probability Models. Academic Press, 2014. — 784 p.
16. Grinstead, C.M., Snell, J.L. Introduction to Probability. American Mathematical Society, 1997. — 510 p.
17. Kudryavtsev, V.A. (Кудрявцев В.А.), Demidovich, B.P. A Brief Course in Higher Mathematics: Textbook for Universities. Moscow: Nauka, 1989. — 656 p. Text: printed. (In Russ)
18. Bakhvalov, N.S., Zhidkov, N.P., Kobelkov, G.M. Numerical Methods: Textbook for Universities. Moscow: Knowledge Laboratory, 2015. — 636 p. (In Russ)
19. Samarsky, A.A., Gulin, A.V. Numerical Methods: Textbook for Universities. Moscow: Knowledge Laboratory, 2020. — 432 p. (In Russ)

Сведения об авторах:

Застрожных Игорь Иванович, кандидат технических наук, доцент кафедры автоматизированных информационных систем органов внутренних дел; zasigor@yandex.ru

Ланкин Олег Викторович, доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел; oleg_lankin@mail.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Биктимирова Юлия Вадимовна, адъюнкт института; Biktimirova-02@yandex.ru

Лукоянов Алексей Александрович, главный специалист по защите информации; 9266421233@mail.ru

Information about authors:

Igor I. Zastrozhnov, Cand. Sci. (Eng.), Assoc. Prof., Department of Automated Information Systems of Internal Affairs Bodies; zasigor@yandex.ru

Oleg V. Lankin, Dr. Sci. (Eng.), Assoc. Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; oleg_lankin@mail.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Julia V. Biktimirova, Post-graduate cadet; Biktimirova-02@yandex.ru

Aleksey A. Lukoyanov, Chief Information Security Specialist; 9266421233@mail.ru

Конфликт интересов/Conflict of interest

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest

Поступила в редакцию/Received 30.09.2025.

Одобрена после рецензирования/Reviced 27.10.2025.

Принята в печать/Accepted for publication 17.03.2026.