ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.21822/2073-6185-2026-53-1-64-72 Оригинальная статья/ Original article

Оптимизационные задачи, связанные с количественной оценкой уровня защищенности, на основе анализа уязвимостей автоматизированных систем

А.О. Ефимов, Е.А. Рогозин
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. В статье решается проблема количественной оценки уровня защищённости автоматизированных систем органов внутренних дел в условиях постоянного роста числа выявляемых уязвимостей и ограниченности ресурсов, затрачиваемых на их устранение. Проведён анализ существующих подходов к оценке защищённости информационных систем, показаны их ограничения, связанные с отсутствием формализованного учёта ресурсных ограничений и взаимосвязей между уязвимостями. **Метод.** В качестве метода решения поставленной задачи предложен математический аппарат, основанный на совокупности оптимизационных моделей. Рассмотрены три задачи: минимизация вероятности эксплуатации уязвимостей системы путём подбора оптимальных элементов АС ОВД; выбор наиболее уязвимых элементов для приоритетной проверки; выбор комплекта средств устранения уязвимостей с учётом их стоимости и допустимой ошибки. Для формализации применены методы динамического программирования и оптимизации. **Результат.** Результаты вычислительного эксперимента на модельных данных демонстрируют эффективность предложенного подхода, позволяющего переходить от «жадных» алгоритмов устранения уязвимостей к оптимальным стратегиям обеспечения защищённости. Совместное решение оптимизационных задач обеспечивает более рациональное распределение ресурсов и снижение вероятности уязвимостей при ограничениях по времени и стоимости. **Вывод.** Разработанные метод и модели могут быть положены в основу практических механизмов управления защищённостью АС ОВД. Применение предложенного подхода открывает перспективу интеграции количественных методов в процессы оценки и повышения уровня защищённости автоматизированных систем правоохранительных органов.

Ключевые слова: автоматизированные системы, информационная безопасность, уязвимости, количественная оценка защищённости, оптимизационные задачи, динамическое программирование, комбинаторная оптимизация

Для цитирования: А.О. Ефимов, Е.А. Рогозин. Оптимизационные задачи, связанные с количественной оценкой уровня защищенности, на основе анализа уязвимостей автоматизированных систем. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(1):64-72. DOI:10.21822/2073-6185-2026-53-1-64-72.

Optimization tasks related to quantifying the security level based on vulnerability analysis of automated systems

A.O. Efimov, E.A. Rogozin
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov St., Voronezh 394065, Russia

Abstract. **Objective**. The article discusses the problem of quantifying the level of security of automated systems of internal affairs bodies (AS) in the context of a constant increase in the number of identified vulnerabilities and limited resources spent on their elimination. An analysis of approaches to assessing the security of information systems is conducted, and their limitations associated with the lack of a formalized accounting of resource constraints and relationships between vulnerabilities are shown. **Method**. A mathematical apparatus based on a set of optimization

models is proposed. Three tasks are considered: minimizing the likelihood of exploiting system vulnerabilities by selecting the optimal elements of the AS control system; selecting the most vulnerable elements for priority verification; selecting a set of vulnerability mitigation tools, taking into account their cost and error tolerance. Dynamic programming and optimization methods were applied. **Result**. The results of the computational experiment on model data demonstrate the effectiveness of the proposed approach, which makes it possible to move from "greedy" algorithms for eliminating vulnerabilities to optimal security strategies. Joint solution of optimization problems ensures rational allocation of resources and reduction of the probability of vulnerabilities under time and cost constraints. **Conclusion**. The developed method and models can be used as a basis for practical mechanisms for managing the security of ATS automated systems. The application of the proposed approach opens up the prospect of integrating quantitative methods into the assessment processes and increasing the level of security of automated law enforcement systems.

Keywords: automated systems, information security, vulnerabilities, quantitative assessment of security, optimization tasks, dynamic programming, combinatorial optimization

For citation: A.O. Efimov, E.A. Rogozin. Optimization tasks related to quantifying the security level based on vulnerability analysis of automated systems. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):64-72. (In Russ) DOI:10.21822/2073-6185-2026-53-1-64-72.

Введение. Современные автоматизированные системы органов внутренних дел (АС ОВД) функционируют в условиях постоянного воздействия на их программное обеспечение и инфраструктуру со стороны потенциальных нарушителей.

Непрерывный рост количества выявляемых уязвимостей программного обеспечения, а также расширение спектра угроз информационной безопасности существенно осложняют задачу обеспечения защищённости таких систем. Специфика функционирования АС ОВД предполагает необходимость гарантированной устойчивости к деструктивным воздействиям, поскольку сбои в их работе напрямую затрагивают выполнение государственных функций в сфере правопорядка и безопасности. Вопросы выявления, анализа и устранения уязвимостей в автоматизированных системах традиционно исследуются в рамках оценки соответствия требованиям информационной безопасности, анализа рисков и управления жизненным циклом программного обеспечения. Однако существующие подходы в большинстве случаев опираются на экспертные методы или ориентированы на «жадные» стратегии устранения уязвимостей без учёта ограничений ресурсов и взаимосвязей между отдельными уязвимостями. Это снижает эффективность принимаемых решений и затрудняет формирование оптимальных мер защиты в условиях ограниченного времени, количества специалистов и доступных средств устранения уязвимостей.

Постановка задачи. Актуальность разработки методов количественной оценки уровня защищённости АС ОВД обусловлена рядом факторов.

Во-первых, постоянный рост числа выявляемых уязвимостей программного обеспечения требует перехода от качественных экспертных подходов к строгим количественным методам, позволяющим формализовать процесс оценки защищённости. Во-вторых, практическая деятельность органов внутренних дел характеризуется ограниченностью ресурсов – временных, кадровых и финансовых, что обуславливает необходимость применения методов оптимизации для выбора наиболее эффективных решений. В-третьих, существующие модели оценки защищённости информационных систем зачастую не учитывают совокупность ограничений, возникающих при реализации процессов устранения уязвимостей, и тем самым не позволяют выстроить комплексный механизм управления защищённостью. В этих условиях разработка математического аппарата, позволяющего формализовать задачи выбора, приоритизации и устранения уязвимостей, становится научно и практически значимой. Решение данной задачи обеспечивает возможность перехода от фрагментарных и локальных методов обеспечения защищённости к оптимизированным стратегиям,

учитывающим специфику функционирования автоматизированных систем органов внутренних дел.

Методы исследования. Современные подходы к обеспечению информационной безопасности автоматизированных систем органов внутренних дел опираются на необходимость комплексной оценки защищённости с учётом уязвимостей. В нормативной базе закреплены ключевые положения, касающиеся понятийного аппарата, показателей защищённости и общих принципов обеспечения безопасности [1, 9, 10, 19-24].

В частности, в документах ФСТЭК России определяются методики оценивания уровня критичности уязвимостей, что позволяет формировать количественные показатели для практического применения в системах защиты [19]. Значительное внимание уделяется разработке методов формализации уязвимостей и их классификации по критериям влияния на надёжность и устойчивость систем [3, 16]. Исследования показывают, что уязвимости представляют собой ключевой фактор, определяющий эффективность защиты информации, и требуют построения моделей взаимосвязей компонентов безопасности [3]. С этим согласуются работы, посвящённые формированию методологических основ интеллектуальной защиты, основанных на системно-кибернетическом подходе [17].

Широкое распространение получили количественные методы анализа уязвимостей, основанные на международных метриках, таких как CVSS [2, 6], а также на методиках OWASP [7]. В отечественных исследованиях рассматриваются вопросы выявления уязвимостей средствами анализа параметрических данных вычислительных сетей [5], а также методики оценивания надёжности систем защиты от несанкционированного доступа [24].

В последние годы активно развиваются методы статического и динамического анализа программного обеспечения для выявления уязвимостей [12]. Появились инструменты, использующие машинное обучение и глубокие нейронные сети для автоматизации анализа исходного кода [13, 15]. Применение технологий fuzzing и методов, учитывающих целостность контрольных сумм, позволяет повысить точность обнаружения критических дефектов [14]. Современные исследования подчеркивают значимость интеграции методов искусственного интеллекта в систему оценки уязвимостей [11, 15].

Вопросы практической реализации оценки защищённости тесно связаны с построением показателей и моделей управления рисками. В ряде работ предложены концептуальные основы оценки уровня защищённости на основе характеристик уязвимостей [11, 18], что соответствует современным тенденциям перехода от экспертных оценок к формализованным количественным методикам. При этом важную роль играют карты источников, содержащих сведения об уязвимостях [8], позволяющие строить прогностические модели и учитывать динамику угроз.

Таким образом, анализ существующих исследований демонстрирует переход от формальных методик методик к формализованным количественным подходам, в основе которых лежит оптимизация процессов выявления и устранения уязвимостей, а также использование интеллектуальных методов анализа и прогнозирования.

Обсуждение результатов. Представим метод и модели количественной оценки уровня защищенности АС ОВД на основе уязвимостей [8, 25-27] в виде схемы (рис. 1).

Схема наглядно демонстрирует ограничения возникающие в процессе выявления и устранения уязвимостей программного обеспечения АС. Среди них необходимо однозначно выделить следующие: ограничение по времени устранения уязвимостей, ограничение по количеству специалистов ИБ и средств устранения уязвимостей, ограничение по выбору средств устранения уязвимостей. Весьма логично, что в связи с постоянным ростом числа выявляемых уязвимостей, ограничения по ресурсам, затрачиваемым на реализацию процесса устранения уязвимостей и защиты от угроз информационной безопасности, становятся более значимыми.

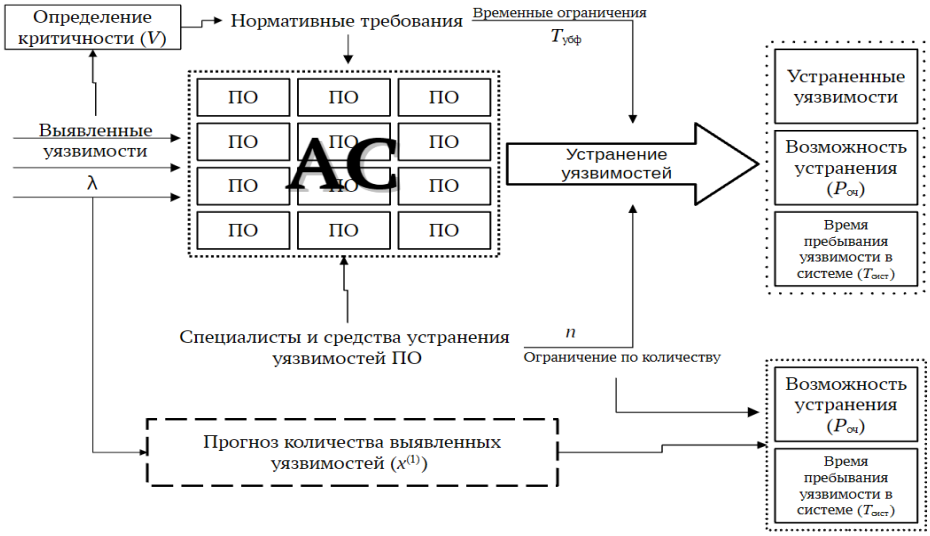

Рис. 1 – Схема реализации метода и моделей количественной оценки уровня защищённости АС ОВД

Fig. 1 – Scheme of implementation of the method and models for quantifying the level of security of the AS

Представим эти ограничения на рис. 2:

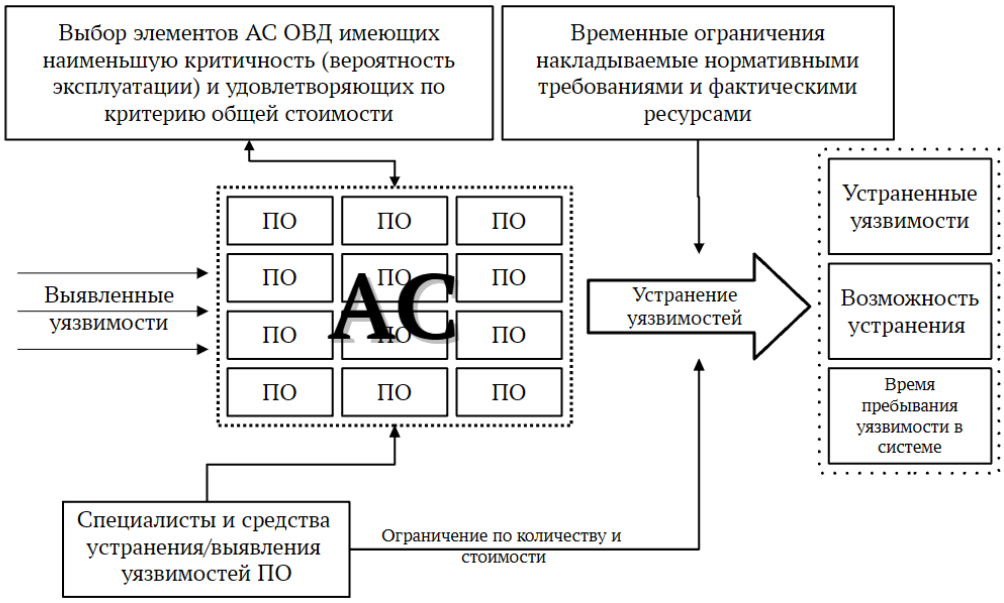

Рис. 2 – Схема, содержащая ограничения, возникающие при реализации метода и моделей количественной оценки уровня защищённости АС ОВД

Fig. 2– A scheme containing limitations that arise when implementing a method and models for quantifying the level of security of an AS

Следовательно, процесс устранения уязвимостей непосредственно связан с решением ряда оптимизационных задач, в связи с этим рассмотренная выше схема будет содержать блок решения оптимизационных задач, и будет представлена следующим образом (рис.3). Сформулируем набор оптимизационных задач, требующих решения:

1. Задача минимизации вероятности эксплуатации уязвимости системы путем подбора оптимальных элементов АС ОВД;
2. Задача выбора наиболее уязвимых элементов АС ОВД;
3. Задача выбора комплекта средств устранения уязвимостей АС ОВД.

Перейдем к формализации и решению представленных задач.

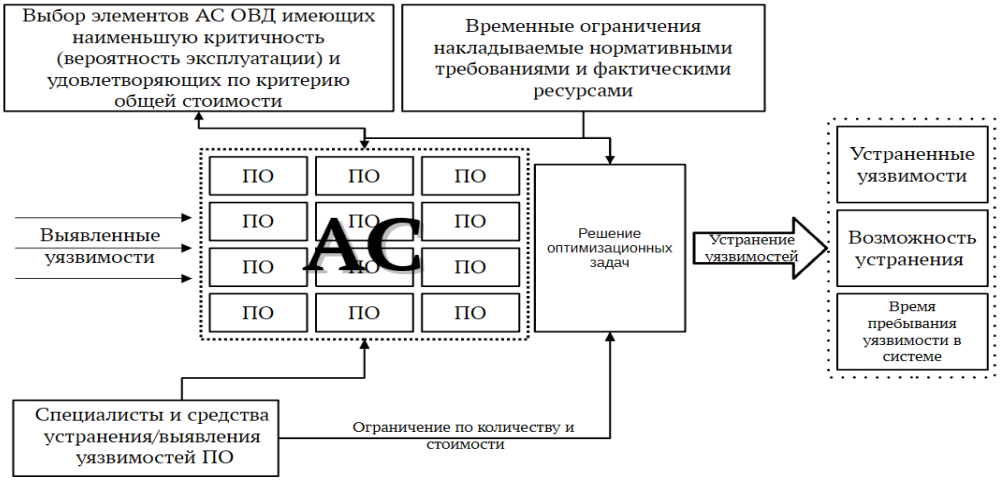

Рис. 3 – Схема, содержащая ограничения и решение оптимизационных задач, возникающие при реализации метода и моделей количественной оценки уровня защищённости АС ОВД
Fig. 3 – A scheme containing limitations and solutions to optimization problems that arise when implementing a method and models for quantifying the level of security of an AS

Задача 1. Задача минимизации вероятности эксплуатации уязвимости системы путем подбора оптимальных элементов АС ОВД.

Пусть система P состоит из N элементов, которые характеризуются вероятностями эксплуатации уязвимости $q_1,q_2,\ldots q_n$ и их значениями $d_1,d_2,\ldots d_N$. Требуется минимизировать вероятность эксплуатации уязвимостей (поражения системы) Q, а также предусмотреть ограничение по стоимости её элементов, чтобы данное значение не превышало заданной величины D, то есть необходимо определить количество элементов каждого типа x_j:

$$Q = \min\left(1 - \prod_{j=1}^{N}\left(1 - q_j^{x_j}\right)\right). \quad (1)$$

$$\sum_{j=1}^{N} d_j x_j \le D, x_j = 1,2,3\ldots \quad (2)$$

Введем в рассмотрение $f_n(D_n)$:

$$f_n(D_n) = \min_{x_j}\left(1 - \prod_{j=1}^{N}\left(1 - q_j^{x_j}\right)\right). \quad (3)$$

$$D_n = \sum_{j=1}^{N} d_j x_j \le D. \quad (4)$$

Функциональное уравнение Беллмана примет следующий вид:

$$f_n(D_n) = \min\left(f_{n-1}(D_n - d_n x_n) + q_n^{x_n} f_{n-1}(D_n - d_n x_n) q_n^{x_n}\right), D_n < D. \quad (5)$$

Задача 2. Задача выбора наиболее уязвимых элементов АС ОВД

В рассматриваемой АС ОВД необходимо определить наиболее уязвимые элементы (с уязвимостями максимальной критичности). Определим q_j – вероятность поражения j-го элемента к моменту проверки; $T_{доп}$ – допустимое время проверки; t_j – время проверки j-го элемента.

$$Q = \left(1 - \prod_{j=1}^{N}\left(1 - q_j(t_j)\right)\right). \quad (6)$$

$$\sum_{j=1}^{N} t_i \le T_{доп}\,. \quad (7)$$

$$f_n(T_n) = \max_{t_j}(1 - \prod_{j=1}^{N}\left(1 - q_j(t_j)\right). \quad (8)$$

$$T_n = \sum_{j=1}^{N} t_j. \quad (9)$$

Функциональное уравнение Беллмана примет следующий вид:

$$f_n(T_n) = \max\left(f_{n-1}(T_n - t_n) + q_n(t_n)f_{n-1}(T_n - t_n)q_n(t_n)\right). \quad (10)$$
$$T_n \le T_{\text{доп}}.$$

Задача 3. Задача выбора комплекта средств устранения уязвимостей АС ОВД

Необходимо найти набор средств m с минимальной стоимостью C и суммарной ошибкой не превосходящей заданной величины Q. Дополнительно определим: C_i – стоимость i-го средства; $|x_{ij}|$ – матрица (1 – контроль j-уязвимости i-средством; 0 – в противном случае); q_{ij} – достоверность проверки.

$$q_{ij} = \alpha_{ij} + \beta_{ij}, \quad (11)$$

где α_{ij}, β_{ij} – ошибки первого и второго рода соответственно.

$$C = min \sum_{i=1}^{m} C_i y_i. \quad (12)$$

$$\sum_{i=1}^{m} z_{ij} = 1, \qquad j = \overline{1,n}. \quad (13)$$

$$z_{ij} \le x_{ij} y_i, \qquad i = \overline{1,m}, \qquad j = \overline{1,n}. \quad (14)$$

$$\sum_{j=1}^{n}\sum_{i=1}^{m} q_{ij} z_{ij} \le Q, y_i \in \{0,1\}. \quad (15)$$

$$x_{ij} = \begin{cases} 1, \text{возможно применение } i-\text{го средства} \\ 0, \text{в противном случае} \end{cases}. \quad (16)$$

$$y_i = \begin{cases} 1, \text{средство включено} \\ 0, \text{в противном случае} \end{cases}. \quad (17)$$

$$z_{ij} = \begin{cases} 1, \text{уязвимость } j \text{ устранена средством } i \\ 0, \text{в противном случае} \end{cases}. \quad (18)$$

Таким образом, представленный набор оптимизационных задач формирует математический аппарат для управления защищенностью АС ОВД в условиях ограниченных ресурсов. Совместное решение этих задач позволяет перейти от «жадного» алгоритма устранения уязвимостей к оптимальным вариантам обеспечения защищенности АС ОВД.

Вывод. Проведенное исследование позволяет констатировать, что проблема количественной оценки уровня защищенности автоматизированных систем органов внутренних дел в условиях нарастающей динамики выявляемых уязвимостей и объективной ограниченности ресурсов требует перехода от качественных, экспертно-ориентированных методик к строго формализованному математическому аппарату. Существующие подходы, несмотря на свою распространенность, демонстрируют системную недостаточность, обусловленную отсутствием комплексного учета ресурсных ограничений и взаимного влияния уязвимостей, что приводит к принятию субоптимальных решений при планировании и реализации мер защиты.

В качестве методологического базиса преодоления указанных ограничений в работе предложен и формализован комплекс взаимосвязанных оптимизационных моделей.

Разработанный аппарат, основанный на методах динамического программирования и комбинаторной оптимизации, позволяет структурировать и решить три ключевые задачи управления защищенностью:

Представленные оптимизационные модели обладают свойствами полноты, адекватности и практической применимости. Они могут быть положены в основу создания автоматизированных систем поддержки принятия решений для руководителей подразделений информационной безопасности органов внутренних дел. Перспективой дальнейших исследований видится углубление моделей за счет учета цепочек взаимосвязанных уязвимостей, интеграции методов машинного обучения для прогнозирования появления новых уязвимостей и адаптации предложенного аппарата для задач управления защищенностью в гетерогенных и динамически изменяющейся инфраструктуре АС ОВД.

Библиографический список:

1. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. – 2014. – № 3(4). – С. 20–28. – EDN SSYPXV.
2. Бокова О.И., Дровникова И.Г., Етепнев А.С. [и др.] Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах//Труды СПИИРАН. – 2019. – Т. 18, № 6. – С. 1301–1332. DOI 10.15622/sp.2019.18.6.1301-1332. – EDN YBHXOB.
3. ГОСТ Р 53114-2008. Информационная технология. Защита информации. Основные термины и определения. – Введ. 2009-01-01. – М.: Стандартинформ, 2009. – 14 с.
4. ГОСТ Р 56546-2015. Информационная безопасность. Защита информации. Показатели защищённости информационных систем. – Введ. 2016-01-01. – М.: Стандартинформ, 2016. – 12 с.
5. ГОСТ Р 58142-2018. Информационная безопасность. Методы и средства защиты информации. Общие положения. – Введ. 2018-12-01. – М.: Стандартинформ, 2018. – 24 с.
6. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно-управляющие системы. – 2017. – № 6(91). – С. 76–87. – DOI 10.15217/issn1684-8853.2017.6.76. – EDN ZXWUWH.
7. Дровникова И.Г., Етепнев А.С., Рогозин Е.А. Основные виды уязвимостей и взаимосвязь компонентов безопасности при обосновании показателей надёжности системы защиты информации от несанкционированного доступа в автоматизированных системах // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 3. – С. 59–64. – EDN VWGOHY.
8. Ефимов А.О., Лившиц И.И., Мещерякова Т.В., Рогозин Е.А. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости // Безопасность информационных технологий. – 2023. – Т. 30, № 2. – С. 63–79. DOI 10.26583/bit.2023.2.04. – EDN LGPQZP.
9. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем посредством комбинированного метода анализа параметрических данных, определяемых системами мониторинга вычислительных сетей//Альманах современной науки и образования. – 2016. – № 11(113). – С. 60–66. – EDN XEEDXH.
10. Кравченко, А.С. Аппаратно-программные средства и информационные процессы защиты систем предоставления пользователям доступа к программным ресурсам/А. С. Кравченко, С. В. Родин, Т. Е. Смоленцева//Современные проблемы науки и образования. – 2015. – № 1-1. С.357. EDN VIDYLR.
11. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков//Вопросы кибербезопасности. – 2013. – № 2(2). – С. 29–33. EDN SZEDHH.
12. Ланкин О.В., Сумин В.И., Воронова Е.В. Системно-комплексный кибернетический подход к формированию методологических основ интеллектуальной защиты информации от несанкционированного доступа // Вестник Воронежского государственного технического университета. – 2011. – Т. 7, № 8. – С. 174–176. – EDN NYIJQT.
13. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов//Труды СПИИРАН. – 2020. – Т. 19, №2. – С.383–411. DOI 10.15622/sp.2020.19.2.6. EDN DPCIDQ.
14. Математическая модель локальной политики безопасности с учетом структурных особенностей автоматизированной информационной системы информационного центра/ В.И. Сумин, А.В. Душкин, С.В. Родин, М.А. Жукова//Математические методы и информационно-технические средства:материалы IX Всероссийской научно-практической конференции, Краснодар, 21–22 июня 2013г./редколлегия: И.Н. Старостенко ответственный редактор, С.А. Вызулин, Е.В. Михайленко, Ю.Н. Сопильняк. – Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования "Краснодарский университет Министерства внутренних дел Российской Федерации", 2013. – С. 305-307. – EDN YTBIAH.
15. Родин, С.В. Моделирование систем защиты информации в информационных системах вневедомственной охраны : специальность 05.13.18 "Математическое моделирование, численные методы и комплексы программ", 05.13.19 "Методы и системы защиты информации, информационная безопасность" : автореферат

диссертации на соискание ученой степени кандидата технических наук / Родин Сергей Владимирович. – Воронеж, 2009. – 17 с. – EDN NKXWRJ.

16. Сумин, В.И. Разработка сетевой модели целевых установок сложных организационных систем специального назначения / В.И. Сумин, А.С. Кравченко, С.В. Родин // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 79-87. – DOI 10.12737/2219-0767-2024-77-85. – EDN QIRWOK.
17. ФСТЭК России. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. – Утв. 28 октября 2022 г. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (дата обращения: 04.10.2024).
18. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. – 2013. – № 2(101). – С. 36–43. – EDN QAVHRX.
19. Forum of Incident Response and Security Teams. Common Vulnerability Scoring System version 4.0: Specification Document [Электронный ресурс]. – URL: https://www.first.org/cvss/specification-document (дата обращения: 16.01.2025).
20. Lin G., Wen S., Han Q.-L., Zhang J., Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey // Proceedings of the IEEE. – 2020. – Vol. 108, no. 10. – P. 1825–1848. – DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.
21. OWASP Foundation. OWASP Risk Rating Methodology [Электронный ресурс]. – URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (дата обращения: 16.01.2025).
22. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning // 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. – 2018. – P. 757–762. – DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
23. Serdechny A. L., Tarelkin M. A., Lomov A. A., Simonov K. V. Карты источников, содержащих сведения об уязвимостях программного обеспечения // Информация и безопасность. – 2019. – Т. 22, № 3. – С. 411–422. – EDN ZOUMGN.
24. Wang T., Wei T., Gu G., Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection // IEEE Symposium on Security and Privacy, Oakland, CA, USA. – 2010. – P. 497–512. – DOI: http://dx.doi.org/10.1109/SP.2010.37.
25. Ефимов, А.О. Об осуществлении управления уязвимостями автоматизированных систем //Вестник Воронежского института МВД России. – 2023. – № 3. – С. 186-196.EDN MAYURS.
26. Ефимов, А.О. Оценка уровня защищенности (безопасности функционирования) автоматизированных систем на основе их уязвимостей, формализованная при помощи теории систем массового обслуживания/ А.О. Ефимов, Е.А. Рогозин//Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 2. – С. 83-89.DOI 10.21822/2073-6185-2023-50-2-83-89.
27. Ефимов, А.О. Прогнозирование количества выявляемых уязвимостей информационной безопасности на основе теории «серых систем» / А.О. Ефимов, С.А. Мишин, Е.А. Рогозин // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50, № 3. – С. 72-82. – DOI 10.21822/2073-6185-2023-50-3-72-82. – EDN JEDBYH.

References:

1. Avetisyan A.I., Belevantsev A.A., Chuklyaev I.I. Technologies of Static and Dynamic Analysis of Software Vulnerabilities. *Cybersecurity Issues*. 2014;3(4): 20–28. – EDN SSYPXV.
2. Bokova O.I., Drovnikova I.G., Etepnev A.S. [et al.] Methods for Assessing the Reliability of Information Security Systems against Unauthorized Access in Automated Systems. *SPIIRAS Proceedings*. 2019;18(6): 1301–1332. – DOI 10.15622/sp.2019.18.6.1301-1332. – EDN YBHXOB.
3. GOST R 53114-2008. Information Technology. Information Security. Basic Terms and Definitions. – Effective from 2009-01-01. – Moscow: Standartinform, 2009. – 14 p.
4. GOST R 56546-2015. Information Security. Information Protection. Security Indicators of Information Systems. – Effective from 2016-01-01. – Moscow: Standartinform, 2016. – 12 p.
5. GOST R 58142-2018. Information Security. Methods and Means of Information Protection. General Provisions. – Effective from 2018-12-01. – Moscow: Standartinform, 2018. – 24 p.
6. Doinikova E.V., Chechulin A.A., Kotenko I.V. Assessment of Computer Network Security Based on CVSS Metrics. *Information and Control Systems.* 2017;6(91):76–87. DOI 10.15217/issn1684-8853.2017.6.76. – EDN ZXWUWH.
7. Drovnikova I.G., Etepnev A.S., Rogozin E.A. Main Types of Vulnerabilities and the Relationship of Security Components in Justifying the Reliability Indicators of Information Protection Systems against Unauthorized Access in Automated Systems*. Devices and Systems. Control, Diagnostics*. 2019;3:59–64. EDN VWGOHY.
8. Efimov A.O., Livshits I. I., Meshcheryakova T.V., Rogozin E.A. Conceptual Framework for Assessing the Security Level of Automated Systems Based on Their Vulnerabilities // Information Technology Security. – 2023. – Vol. 30, No. 2. – P. 63–79. – DOI 10.26583/bit.2023.2.04. – EDN LGPQZP.
9. Konovalenko S.A., Korolev I.D. Detection of Vulnerabilities in Information Systems Using a Combined Method of Analyzing Parametric Data Determined by Computer Network Monitoring Systems. *Almanac of Modern Science and Education.* 2016;11(113): 60–66. – EDN XEEDXH.
10. Kravchenko A.S., Rodin S.V., Smolentseva TE. Hardware and Software Tools and Information Processes for Protecting Systems Providing Users with Access to Software Resources. *Modern Problems of Science and Education.* 2015;1-1:357. – EDN VIDYLR.

11. Kubarev A.V. An Approach to the Formalization of Information System Vulnerabilities Based on Their Classification Features. *Cybersecurity Issues*. 2013;2(2): 29–33. – EDN SZEDHH.
12. Lankin O.V., Sumin V.I., Voronova E.V. A System-Complex Cybernetic Approach to the Formation of Methodological Foundations for Intelligent Information Protection against Unauthorized Access. *Bulletin of Voronezh State Technical University*. 2011; 7(8):174–176. – EDN NYIJQT.
13. Livshits I.I. A Method for Assessing the Security of Cloud IT Components According to Existing Standards. *SPIIRAS Proceedings*. 2020;19(2):383–411. – DOI 10.15622/sp.2020.19.2.6. – EDN DPCIDQ.
14. Sumin V.I., Dushkin A.V., Rodin S.V., Zhukova M.A. Mathematical Model of Local Security Policy Considering the Structural Features of an Automated Information System of the Information Center // Mathematical Methods and Information-Technical Tools: Proceedings of the IX All-Russian Scientific and Practical Conference, Krasnodar, June 21–22, 2013 / Editorial Board: I.N. Starostenko (ed.), S.A. Vyzulin, E.V. Mikhailenko, Yu.N. Sopilnyak. – Krasnodar: Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, 2013; 305–307. – EDN YTBIAH.
15. Rodin S.V. Modeling of Information Security Systems in the Information Systems of the Non-Departmental Security Service: Specialty 05.13.18 "Mathematical Modeling, Numerical Methods and Software Complexes", 05.13.19 "Methods and Systems of Information Security, Information Security": Abstract of Dissertation for the Degree of Candidate of Technical Sciences. Rodin Sergey Vladimirovich. Voronezh, 2009;17– EDN NKXWRJ.
16. Sumin V.I., Kravchenko A.S., Rodin S.V. Development of a Network Model of Target Settings of Complex Organizational Systems for Special Purposes. *Modeling of Systems and Processes*. 2024;17(3):79–87. – DOI 10.12737/2219-0767-2024-77-85. – EDN QIRWOK.
17. FSTEC of Russia. Methodology for Assessing the Criticality of Vulnerabilities of Software and Hardware-Software Tools. – Approved on October 28, 2022. https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (accessed: 04.10.2024).
18. Shcheglov K.A., Shcheglov A.Yu. Protection Against Application Vulnerability Attacks. Access Control Models. *Information Security Issues*. 2013;2(101):36–43. – EDN QAVHRX.
19. Forum of Incident Response and Security Teams. Common Vulnerability Scoring System Version 4.0: Specification Document [El.resource]. – URL: https://www.first.org/cvss/specification-document (accessed: 16.01.2025).
20. Lin G., Wen S., Han Q.-L., Zhang J., Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey. *Proceedings of the IEEE*. 2020;108(10):1825–1848. DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.
21. OWASP Foundation. OWASP Risk Rating Methodology [Electronic resource]. – URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (accessed: 16.01.2025).
22. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning // 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. – 2018;757–762. – DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
23. Serdechny A.L., Tarelkin M.A., Lomov A.A., Simonov K.V. Maps of Sources Containing Information on Software Vulnerabilities. *Information and Security.* 2019;22(3):411–422. – EDN ZOUMGN.
24. Wang T., Wei T., Gu G., Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. *IEEE Symposium on Security and Privacy, Oakland, CA, USA.* 2010;. 497–512. – DOI: http://dx.doi.org/10.1109/SP.2010.37
25. Efimov, A.O. On the implementation of vulnerability management of automated systems. *Herald of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2023;3:186-196. EDN MAYURS.
26. Efimov A.O., Rogozin E.A. Assessment of the level of security (safety of functioning) of automated systems based on their vulnerabilities, formalized using the theory of queuing systems. *Herald of Dagestan State Technical University. Technical sciences*. 2023;50():83-89. – DOI 10.21822/2073-6185-2023-50-2-83-89.
27. Efimov, A.O. Forecasting the number of identified information security vulnerabilities based on the theory of "gray systems" / A.O. Efimov, S.A. Mishin, E.A. Rogozin. *Herald of Dagestan State Technical University. Technical sciences.* 2023;50(3):72-82. DOI10.21822/2073-6185-2023-50-3-72-82. EDN JEDBYH.

Сведения об авторах:

Ефимов Алексей Олегович, преподаватель кафедры автоматизированных информационных систем органов внутренних дел; ea.aleksei@yandex.ru

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

Information about authors:

Aleksey O. Efimov, Lecturer, Department of Automated Information Systems of Internal Affairs Bodies; ea.aleksei@yandex.ru

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

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 20.09.2025**.**

Одобрена после рецензирования/Reviced 29.11.2025.

Принята в печать/Accepted for publication 26.12.2025.