ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.53

DOI: 10.21822/2073-6185-2025-52-3-183-190 Обзорная статья / Review article

Основные подходы к оценке защищенности информационных систем и перспективы их применения в органах внутренних дел Российской Федерации

А.И. Янгиров[1], А.С. Черкасова[2], А.О. Ефимов[2], Е.А. Рогозин[2], С.Б. Ахлюстин[2]
[1] ФКУ «НИЦ «Охрана» Росгвардии,
[1] 111539, г. Москва, Реутовская, 12Б, Россия,
[2]Воронежский институт МВД России,
[2]394065, г. Воронеж, проспект Патриотов, 53, Россия

Резюме. Цель. В статье проведен анализ основных подходов к оценке защищенности информационных систем, выделены их преимущества и недостатки, рассмотрена их применимость для органов внутренних дел Российской Федерации. Целью исследования является определение перспектив развития методологических подходов к оценке защищенности органов внутренних дел Российской Федерации. **Метод.** Исследование опирается на изучение различных методов оценки защищенности информационных систем, а также на анализ научной литературы и публикаций по данной теме. **Результат.** Предложен подход к дальнейшему развитию методов оценки защищенности информационных систем с учетом специфики органов внутренних дел Российской Федерации. **Вывод.** Отмечается перспективность исследований в рамках создания специализированного программного обеспечения, объединяющего в себе экспертные знания и количественные алгоритмы, которое могло бы упростить оценку защищенности информационных систем органов внутренних дел, обеспечив точность, доступность и адаптивность к специфике правоохранительной деятельности. Такое программное обеспечение стало бы ценным инструментом для повышения безопасности данных органов внутренних дел, минимизации рисков и оптимизации ресурсов, открывая новые возможности для защиты критически важных информационных систем.

Ключевые слова: информационная система, методы оценки, органы внутренних дел, программное обеспечение

Для цитирования: А.И. Янгиров, А.С. Черкасова, А.О. Ефимов, Е.А. Рогозин, С.Б. Ахлюстин. Основные подходы к оценке защищенности информационных систем и перспективы их применения в органах внутренних дел Российской Федерации. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(3): 183-190. DOI:10.21822/2073-6185-2025-52-3-183-190

Basic approaches to assessing the Security of Information Systems and prospects for their application in the internal affairs agencies of the Russian Federation

A.I. Yangirov[1], A.S. Cherkasova[2], A.O. Efimov[2], E.A. Rogozin[2], S.B. Akhlyustin[2]
[1] FSI «SRC «Okhrana» of the Federal Service of National Guard of Russia,
[1]12 B Reutovskaya Str., Moscow 111539, Russia,
[2]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[2]53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. The article analyzes the main approaches to assessing the security of information systems, highlights their advantages and disadvantages, and considers their applicability to the internal affairs bodies of the Russian Federation. The aim of the study is to determine the prospects for the development of methodological approaches to assessing the security of internal affairs bodies of the Russian Federation. **Method**. The present study is based on the study of various methods for assessing the security of information systems, as well as on the analysis of scientific literature and publications on this topic. **Result**. The authors propose an approach to the

further development of methods for assessing the security of information systems, taking into account the specifics of the internal affairs bodies of the Russian Federation. **Conclusion**. The authors note the prospects of research in the framework of creating specialized software that combines expert knowledge and quantitative algorithms, which could simplify the assessment of the security of information systems of law enforcement agencies, ensuring accuracy, accessibility and adaptability to the specifics of law enforcement activities. Such software would be a valuable tool for improving the data security of law enforcement agencies, minimizing risks and optimizing resources, opening up new opportunities to protect critical information systems.

Keywords: information system, assessment methods, internal affairs agencies, software

For citation: A.I. Yangirov, A.S. Cherkasova, A.O. Efimov, E.A. Rogozin, S.B. Akhlyustin. Basic approaches to assessing the Security of Information Systems and prospects for their application in the internal affairs agencies of the Russian Federation. Herald of Daghestan State Technical University. Technical Sciences. 2025;52(3):183-190. (In Russ) DOI:10.21822/2073-6185-2025-52-3-183-190

Введение. Современный мир, пронизанный цифровыми технологиями, ставит перед организациями и государственными институтами задачу обеспечения надежной защиты информационных систем. В эпоху, когда данные становятся стратегическим ресурсом, их безопасность определяет не только экономическую устойчивость предприятий, но и стабильность общественных процессов. ОВД, ответственные за поддержание правопорядка и защиту граждан, особенно остро ощущают необходимость в эффективных инструментах оценки и усиления информационной безопасности. Утечка конфиденциальных сведений, кибератаки или сбои в работе информационных систем могут привести к серьезным последствиям, включая утрату доверия общества, нарушение оперативной деятельности и угрозу национальной безопасности. В этом контексте разработка и применение методов оценки защищенности информационных систем приобретают существенное значение, требуя подходов, которые сочетали бы точность, практичность и адаптивность к специфическим условиям правоохранительной деятельности.

Одной из ключевых проблем в области информационной безопасности является сложность достижения баланса между глубиной анализа и доступностью инструментов оценки. С одной стороны, информационные системы становятся все более сложными, интегрируя облачные технологии, распределенные сети и большие объемы данных, что требует детального технического анализа уязвимостей. С другой стороны, организации, в том числе ОВД, нуждаются в методиках, которые можно оперативно внедрять в условиях ограниченных временных и финансовых ресурсов.

Постановка задачи. В данных обстоятельствах возникает необходимость создания универсальных подходов, способных учитывать как технические, так и организационные аспекты безопасности. Качественные методы оценки, ориентированные на нормативные документы, часто оказываются недостаточными для выявления скрытых уязвимостей, в то время как количественные подходы, предоставляющие числовые показатели, могут быть сложными в реализации без специализированных инструментов.

Методы исследования. Данное исследование основано на анализе различных подходов к оценке защищенности информационных систем, а также различных источников научной литературы и публикаций.

Обсуждение результатов. Вопросы анализа методов оценки защищенности информационных систем рассматривались в следующих исследованиях [1 - 3].

Авторы [4] выделяют два основных подхода к оценке защищенности информационных систем: качественный и количественный. Каждый подход включает несколько методов, которые применяются в зависимости от контекста, целей и доступных ресурсов.

Качественные методы, ориентированы на оценку информационной системы с точки зрения соответствия нормативным документам, организационных мер и субъективных факторов.

Типовая методика качественной оценки обычно включает:

1) Оценку уровня информационной безопасности;

2) Оценку рисков;

3) Тестирование систем информационной безопасности.

В процессе оценки уровня информационной безопасности в основном анализируется архитектура системы, политики доступа, организационные меры. Оценка проводится на основе чек-листов и нормативных требований.

Оценка рисков, прежде всего, направлена на выявление угроз и уязвимостей, присваивая им приоритет на основе вероятности и потенциального ущерба. Обычно используются такие методы, как SWOT-анализ, матрицы рисков или экспертные обсуждения, для классификации рисков (например, несанкционированный доступ, утечка данных).

В рамках тестирования систем информационной безопасности осуществляется практическая проверка защитных механизмов с помощью аудита, пентестинга или имитации атак. Тестирование систем информационной безопасности позволяет выявить реальные уязвимости, дает практическое понимание эффективности защиты, а также может быть адаптировано под конкретные сценарии атак.

К преимуществам качественных методов относят: простоту реализации для организаций с ограниченными техническими знаниями, а также фокус на организационных аспектах (политики, процедуры и тому подобное) и наиболее критических угрозах.

Вместе с тем, качественные методы субъективны из-за отсутствия числовых метрик, в полной мере не учитывают технические уязвимости информационных систем, а также зависимы от нормативной базы, которая может быть устаревшей. Эти методы подходят для первоначальной оценки, соответствия нормативным требованиям и формирования общей картины безопасности. Они эффективны в организационном контексте, но их субъективность и ограниченная техническая глубина снижают точность при анализе сложных информационных систем.

Эффективность тестирования сопряжена с высокой стоимостью проведения работ, необходимостью квалифицированных специалистов. В связи с этим тестирование обычно проводится ограниченно (тестируется только часть сценариев), что не позволяет судить о защищенности системы в целом.

Для ОВД Российской Федерации, где важна стандартизация процедур, качественные методы полезны для проверки соответствия регламентам, но недостаточны для детального анализа технических уязвимостей.

Количественный подход ориентирован на числовые показатели, позволяющие объективно измерить уровень защищенности. К количественным методам оценки защищенности информационных систем относятся [1-11]:

1) Метод экспертных оценок;

2) Метод информационных потоков;

3) Графовый метод;

4) Методы весовых коэффициентов;

5) Оценка уязвимостей применяемого программного обеспечения.

Метод экспертных оценок основан на стандартах ГОСТ Р ИСО/МЭК 15408 [5-10] и использует экспертные суждения для оценки рисков с помощью профилей защиты.

Точно определить вероятности конкретных угроз, атак и эффективность отдельных политик безопасности достаточно сложно. Поэтому для количественной оценки риска используются экспертные оценки, которые базируются на использовании кластера исходов. Например, кластер на рис. 1 представлен в виде иерархического дерева с вершинами Z1,..., Zi,..., Zn, где каждая вершина соответствует элементу множества значений анализируемого показателя {Ti}, {Vi}, {SPi}, {RAi}.

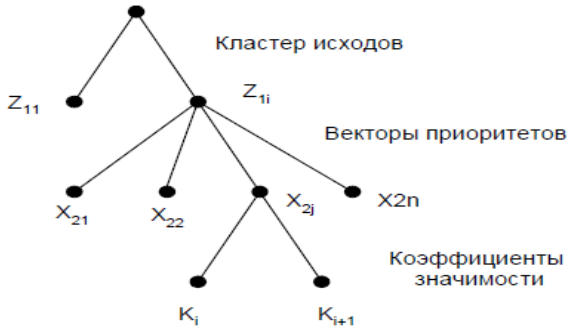

Рис. 1 - Иерархия кластеров
Fig. 1 - Cluster hierarchy

В дальнейшем экспертами оцениваются вероятности угроз (P_T), политика безопасности (P_{SP}) и значимости активов (P_{RA}). Риск рассчитывается как длина вектора:

$$R = \sqrt{P_T^2 + P_{SP}^2 + P_{RA}^2} \quad (1)$$

После выбора целей безопасности риск корректируется с учетом нейтрализации угроз. К преимуществам метода экспертных оценок могут быть отнесены: структурированный подход, опирающийся на международные стандарты, учет сложных взаимосвязей между угрозами и мерами защиты, гибкость в адаптации к различным системам. Вместе с тем, данный метод зависим от квалификации экспертов, субъективен при оценке, несмотря на формализацию, а также требует значительных знаний стандартов и архитектуры информационных систем.

Метод информационных потоков основан на анализе коммуникационных потоков. Обычно этот метод применяется при проектировании архитектуры безопасности, включающую средства, реализующие соответствующую функцию (функции) защиты с необходимым набором параметров, их размещение в вычислительной сети и связь друг с другом. Например (рис. 2), в процессе оценки распределённой сети моделируется топология сети (с межсетевыми фильтрами и серверами), определяются потоки (внутренние, внешние) и матрицы доступа.

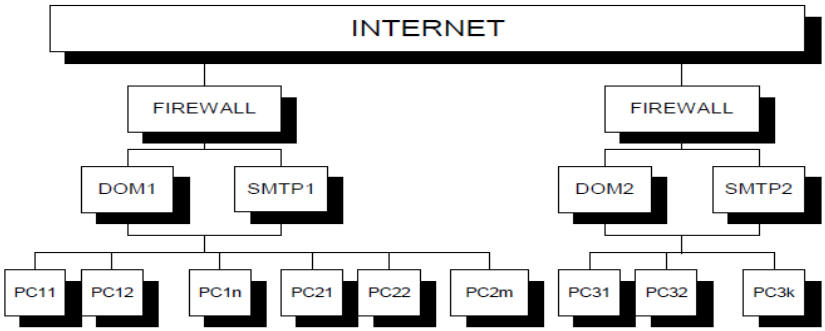

Рис. 2 - Примерная топология сети
Fig. 2 - Approximate network topology

Для реализации функций управления доступом составляется матрица разрешенных связей, определяющих права доступа (p_k, i, j) пользователей к тем или иным сетевым ресурсам:

$$U = \langle p_k, 1, j, \dots, p_k, n, j \rangle \quad (2)$$

В формуле 2 j - обозначает тип доступа (например, доступ на чтение, доступ на запись и тому подобное.), k - порядковый номер пользователя, а n – число пользователей.

Возможный тип доступа определяется используемой информационной системой. В общем случае, матрица разрешенных связей является трехмерной и заполняется в соответствии с действующей политикой безопасности, которая считается заданной. В дальнейшем функции защиты (аудит, целостность) распределяются по узлам сети.

Метод информационных потоков подходит для сложных сетевых систем, обеспечивает систематическое размещение защитных мер и учитывает реальную топологию сети.

Одновременно, данный метод сложен в реализации для среднестатистических специалистов, требует детального анализа сети, а также ограничен только сетевыми сценариями.

Графовый метод представляет информационную систему в виде графа, где вершины - модули защиты и объекты, а рёбра - возможные пути нарушителя (рис. 3).

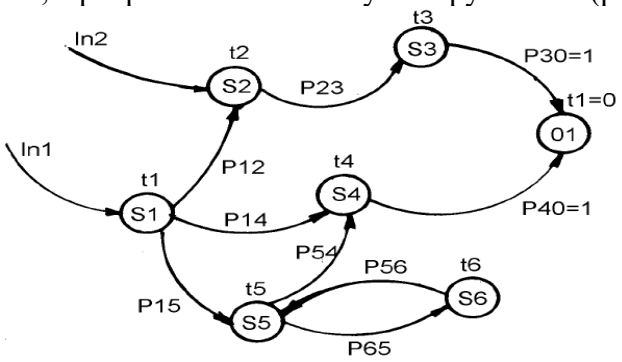

Рис. 3 - Представление информационной системы в виде упрощенного графа
Fig. 3 - Representation of the information system in the form of a simplified graph

В процессе оценки рассчитывается время взлома ($t_{взл}$) и сравнивается с временем обнаружения (t_p). Относительный оценочный параметр L отображает достаточность системы защиты:

$$L = \frac{t_{\text{взл}}}{t_p} \tag{3}$$

Если $L \geq 1$, защита адекватна; если $L < 1$, требуется принятие мер по повышению защищенности наиболее уязвимых направлений. Графовый метод имеет следующие преимущества:

1) Интуитивно понятная визуализация путей атак;

2) Позволяет количественно оценить временные характеристики;

3) Гибкость в моделировании различных систем.

При этом к ограничениям графового метода можно отнести: снижение точности оценки защищенности из-за упрощения модели информационной системы, сложность получения данных о временных параметрах, а также сложность анализа для крупных систем.

Метод весовых коэффициентов использует анкетирование для определения приоритетов угроз, уязвимостей и атак, присваивая им веса. В процессе оценки составляется матрица взаимосвязей, где коэффициент опасности атаки ($K_{оп}$) рассчитывается как произведение весов угроз ($K_{угр}$) и источников ($K_{ист}$):

$$K_{\text{оп}} = K_{\text{угр}} K_{\text{ист}} \tag{4}$$

Основными преимуществами метода весовых коэффициентов являются: простота сбора данных через опросы, учет человеческого фактора и организационных аспектов. Представленный метод подходит для начального анализа рисков различных информационных систем. Вместе с тем, сам метод может быть ограничен глубиной технического анализа, а также зависим от качества анкет (анкетирование обладает некоторой субъективностью ответов респондентов).

Более практико-ориентированным подходом является использование стандарта CVSS (Common Vulnerability Scoring System) [11-20], который позволяет определить критичность уязвимостей на основе множества параметров.

Оценка CVSS агрегирует технические характеристики уязвимости в количественное значение в диапазоне: 0…10. Это значение может быть использовано для автоматизированной сортировки и приоритезации уязвимостей в рамках защиты автоматизированных систем.

Замечание – CVSS по своей сути является экспертной системой оценки, поскольку её параметры, хотя и стандартизированы, формируются и калибруются на основе профессиональных суждений разработчиков стандартов и экспертов по безопасности. Это означает, что методика в значительной мере опирается на формализованный, но всё же субъективный анализ, принятый в профессиональном сообществе.

Объединяя оценку достаточности защиты, веса угроз и источников, а также базовую оценку уязвимости по стандарту CVSS, в рамках комплексного подхода получим показатель Z – безразмерный комплексный показатель защищенности:

$$Z = LK_{\text{оп}}V \quad (5)$$

где, V – базовая оценка критичности уязвимости по стандарту CVSS [11].

Методы количественной оценки защищенности выделяются своей способностью предоставлять числовые показатели (например, время взлома, вероятность атаки или экономические потери). В отличие от качественных методов, которые фокусируются на организационных аспектах и соответствии нормативной документации, количественные методы позволяют измерить эффективность защиты в конкретных сценариях. Это особенно важно для ОВД, где информационные системы обрабатывают конфиденциальные данные (например, оперативные сведения, личные данные граждан), и любая уязвимость может привести к критическим последствиям.

Экспертная оценка является наиболее формализованным из количественных методов, но имеет существенные ограничения, особенно в контексте ОВД. Экспертная оценка требует глубокого понимания стандартов информационной безопасности, таких как ГОСТ Р ИСО/МЭК 15408 [5,6,7], и способности анализировать сложные взаимосвязи между угрозами, политиками и активами. Эксперты должны уметь интерпретировать профили защиты и рассчитывать векторы риска, что предполагает специализированное образование и опыт. В ОВД такие специалисты встречаются редко, поскольку большинство профильного персонала – это сотрудники и работники с общей технической подготовкой, а не узкие специалисты в области кибербезопасности. В отличие от метода экспертной оценки другие количественные методы (граф-метод, метод информационных потоков, метод весовых коэффициентов) менее требовательны к подготовке специалистов.

Несмотря на формализацию, итоговые оценки зависят от субъективных суждений экспертов, что может привести к расхождениям. В ОВД, где важно единообразие процедур, субъективность создаёт риск несогласованности в оценках между подразделениями.

Проведение экспертной оценки требует значительного времени на сбор данных, обсуждения и анализ, а также привлечения внешних консультантов, что увеличивает затраты на проведение работ и дальнейшее принятие оперативных решений.

Вывод. Каждый из представленных подходов обладает своими достоинствами и недостатками. В данных обстоятельствах для ОВД представляется перспективным разработка комбинированного метода, объединяющего качественные и количественные подходы. При разработке такого метода возможно привлечение экспертов, которые на первоначальном этапе могли бы сформировать общие подходы, подготовить базу данных для учёта типичных угроз и уязвимостей, актуальных для информационных систем ОВД. Для упрощения работы специалистов, задействованных при реализации мер информационной безопасности на местах, с разработанным методом возможно создание программного обеспечения в целях:

- автоматизации расчётов (например, рисков по методу весовых коэффициентов или времени взлома по графовому методу);
- включения базы данных, разработанной экспертами, для учёта типичных угроз и уязвимостей в информационных системах ОВД;
- предоставления интерфейса, доступного для специалистов среднего уровня, с пошаговыми инструкциями и визуализацией.

Экспертное участие на этапе разработки метода обеспечит точность, а программное обеспечение, разработанное на основе метода, сделает инструмент доступным для широкого круга пользователей.

Библиографический список:

1. Маковский К.Е. Сопоставление методов оценки защищенности корпоративных информационных систем // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2021. – № 4. – С. 124–127. – DOI: 10.37882/2223-2966.2021.04.27. – EDN: XUKXKX.
2. Титов Д.В., Филипова Е.Е. Использование метода экспертных оценок при определении уровня защищенности информационной системы // Вопросы защиты информации. – 2022. – № 2(137). – С. 51–53. – DOI: 10.52190/2073-2600_2022_2_51. – EDN: KYSIHX.
3. 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. – EDN: OBDQBR.
4. Полянский Д.А. Комплексная защита объектов информатизации. Книга 10. Оценка защищённости: учебное пособие. – Владимир: Изд-во Владим. гос. ун-та, 2005. – 80 с.
5. ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200101777 (дата обращения: 13.04.2025).
6. ГОСТ Р ИСО/МЭК 15408-2–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные компоненты безопасности [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200105710 (дата обращения: 13.04.2025).
7. ГОСТ Р ИСО/МЭК 15408-3–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Требования доверия к безопасности [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200105711 (дата обращения: 13.04.2025).
8. Родин, С.В. Математическое моделирование политики безопасности автоматизированной информационной системы вневедомственной охраны / С.В. Родин // Вестник Воронежского института МВД России. – 2009. – № 1. – С. 174-181. – EDN JXUTPX.
9. 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.
10. Родин, С.В. Анализ влияния уровневого распределения информации на характеристики контроля целостности в автоматизированных информационных системах информационных центров МВД / С.В. Родин, М.А. Жукова // Вестник Воронежского института МВД России. – 2011. – № 2. – С. 80-85. – EDN NUZWEF.
11. Common Vulnerability Scoring System v4.0: Specification Document [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/specification-document (дата обращения: 13.04.2025).
12. Scarfone K., Mell P. An analysis of CVSS version 2 vulnerability scoring // 2009 3rd International Symposium on Empirical Software Engineering and Measurement. – IEEE, 2009. – P. 516–525.
13. Spring J. et al. Time to Change the CVSS? // IEEE Security & Privacy. – 2021. – Vol. 19, № 2. – P. 74–78.
14. Houmb S.H., Franqueira V.N.L., Engum E.A. Quantifying security risk level from CVSS estimates of frequency and impact // Journal of Systems and Software. – 2010. – Vol. 83, № 9. – P. 1622–1634.
15. Spring J. et al. Towards improving CVSS // SEI, CMU, Tech. Rep. – 2018.
16. Figueroa-Lorenzo S., Añorga J., Arrizabalaga S. A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS // ACM Computing Surveys (CSUR). – 2020. – Vol. 53, № 2. – P. 1–53.
17. Fruhwirth C., Mannisto T. Improving CVSS-based vulnerability prioritization and response with context information // 2009 3rd International Symposium on Empirical Software Engineering and Measurement. – IEEE, 2009. – P. 535–544.
18. Khazaei A., Ghasemzadeh M., Derhami V. An automatic method for CVSS score prediction using vulnerabilities description // Journal of Intelligent & Fuzzy Systems. – 2015. – Vol. 30, № 1. – P. 89–96.
19. Costa J. C. et al. Predicting CVSS metric via description interpretation // IEEE Access. – 2022. – Vol. 10. – P. 59125–59134.
20. Franklin J. et al. CVSS implementation guidance // National Institute of Standards and Technology, NISTIR-7946. – 2014.
21. Wang R. et al. An improved CVSS-based vulnerability scoring mechanism // 2011 Third International Conference on Multimedia Information Networking and Security. – IEEE, 2011. – P. 352–355.
22. Gallon L., Bascou J.J. Using CVSS in attack graphs // 2011 Sixth International Conference on Availability, Reliability and Security. – IEEE, 2011. – P. 59–66.
23. Aksu M.U. et al. A quantitative CVSS-based cyber security risk assessment methodology for IT systems // 2017 International Carnahan Conference on Security Technology (ICCST). – IEEE, 2017. – P. 1–8.

References:

1. Makovsky K.E. Comparison of Methods for Assessing the Security of Corporate Information Systems. *Modern Science: Current Problems of Theory and Practice. Series: Natural and Technical Sciences*. 2021; 4:124-127. - DOI: 10.37882/2223-2966.2021.04.27. - EDN: XUKXKX. (In Russ)
2. Titov D.V., Filipova E.E. Using the Expert Assessment Method in Determining the Level of Security of an Information System. *Information Security Issues*. 2022;2(137):51-53. DOI: 10.52190/2073-2600_2022_2_51. - EDN: KYSIHX. (In Russ)
3. Borzenkova S.Yu., Kazarina E.E. Analysis of methods for assessing the level of security of information systems during their operation. *Bulletin of Tula State University. Technical sciences*. 2020; 5:93-97. EDN: OBDQBR. (In Russ)
4. Polyansky D.A. Comprehensive protection of information technology objects. Book 10. Security assessment: a tutorial. - Vladimir: Publishing house of Vladimir. state University, 2005; 80 p. (In Russ)
5. GOST R ISO/IEC 15408-1–2012. Information technology. Methods and means of security. Criteria for assessing the security of information technology. Part 1. Introduction and general model [Electronic resource]. – Available at: https://docs.cntd.ru/document/1200101777 (Accessed: 13.04.2025). (In Russ)

6. GOST R ISO/IEC 15408-2–2013. Information technology. Security methods and tools. Information technology security evaluation criteria. Part 2. Security functional components [Electronic resource]. – Available at: https://docs.cntd.ru/document/1200105710 (Accessed: 13.04.2025). (In Russ)
7. GOST R ISO/IEC 15408-3–2013. Information technology. Security methods and tools. Information technology security evaluation criteria. Part 3. Security assurance requirements [Electronic resource]. – Access mode: https://docs.cntd.ru/document/1200105711 (date accessed: 13.04.2025). (In Russ)
8. Rodin, S.V. Mathematical modeling of the security policy of an automated information system of non-departmental security. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2009;. 1:174-181. - EDN JXUTPX. (In Russ)
9. Sumin, V.I. Development of a network model of target settings of complex organizational systems for special purposes. V.I. Sumin, A.S. Kravchenko, S.V. Rodin. *Modeling of systems and processes.* 2024;17(3): 79-87. – DOI 10.12737/2219-0767-2024-77-85. – EDN QIRWOK. (In Russ)
10. Rodin, S.V. Analysis of the influence of tiered distribution of information on the integrity control characteristics in automated information systems of information centers of the Ministry of Internal Affairs / S. V. Rodin, M. A. Zhukova. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia.* 2011; 2: 80-85. – EDN NUZWEF. (In Russ)
11. Common Vulnerability Scoring System v3.1: Specification Document [Electronic resource]. – Access mode: https://www.first.org/cvss/specification-document (accessed: 13.04.2025).
12. Scarfone K., Mell P. An analysis of CVSS version 2 vulnerability scoring // 2009 3rd International Symposium on Empirical Software Engineering and Measurement. – IEEE, 2009:516–525.
13. Spring J. et al. Time to Change the CVSS?. *IEEE Security & Privacy.* 2021;19(2):74–78.
14. Houmb S.H., Franqueira V.N.L., Engum E.A. Quantifying security risk level from CVSS estimates of frequency and impact. *Journal of Systems and Software*. 2010; 83(9):1622–1634.
15. Spring J. et al. Towards improving CVSS. *SEI, CMU, Tech. Rep.* 2018.
16. Figueroa-Lorenzo S., Añorga J., Arrizabalaga S. A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS. *ACM Computing Surveys (CSUR).* 2020;53(2):1–53.
17. Fruhwirth C., Mannisto T. Improving CVSS-based vulnerability prioritization and response with context information. 2009 *3rd International Symposium on Empirical Software Engineering and Measurement*. – IEEE, 2009;535–544.
18. Khazaei A., Ghasemzadeh M., Derhami V. An automatic method for CVSS score prediction using vulnerabilities description. *Journal of Intelligent & Fuzzy Systems.* 2015; 30(1):89–96.
19. Costa J. C. et al. Predicting CVSS metric via description interpretation. *IEEE Access*. 2022;10:59125–59134.
20. Franklin J. et al. CVSS implementation guidance. *National Institute of Standards and Technology, NISTIR*-7946; 2014.
21. Wang R. et al. An improved CVSS-based vulnerability scoring mechanism. *2011 Third International Conference on Multimedia Information Networking and Securit*y. I*EEE*, 2011: 352–355.
22. Gallon L., Bascou J.J. Using CVSS in attack graphs. *2011 Sixth International Conference on Availability, Reliability and Security. IEEE,* 2011:59–66.
23. Aksu M.U. et al. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. *2017 International Carnahan Conference on Security Technology (ICCST). IEE*E, 2017;1–8.

Сведения об авторах:

Адиль Илдарович Янгиров, начальник отделения лабораторных исследований и испытаний; adil-yan@yandex.ru

Анастасия Сергеевна Черкасова, адъюнкт очной формы обучения; cherkasova.30@yandex.ru

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

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

Сергей Борисович Ахлюстин, кандидат технических наук, начальник кафедры тактико–специальной подготовки; cerg7676@yandex.ru

Information about authors:

Adil I. Yangirov, Head of the Laboratory Research and Testing; adil-yan@yandex.ru

Anastasia S. Cherkasova, full-time Adjunct Student; cherkasova.30@yandex.ru

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

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

Sergey B. Akhlyustin, Cand. Sci. (Eng.), Head of the Department of Tactical and Special Training: cerg7676@yandex.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 20.05.2025**.**

Одобрена после рецензирования/Reviced 29.06.2025.

Принята в печать /Accepted for publication 26.07.2025.