DOI: 10.18137/RNU.V9187.25.02.P.104 УДК 004.056.53

Рыленков Давыд Андреевич
аспирант, Московский финансово-юридический университет МФЮА, Москва. SPIN-код: 9488-6720
Электронный адрес: davyd.rylenckov@yandex.ru
Davyd A. Rylenkov
Postgraduate, Moscow University of Finance and Law, Moscow. SPIN-code: 9488-6720
E-mail address: davyd.rylenckov@yandex.ru

РАЗРАБОТКА МЕТОДА ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ МНОГОКОМПОНЕНТНЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. Для любой современной компании необходимо обеспечивать качественное управление процессами информационной безопасности в связи с распространением кибератак на организации и появлением новых угроз. Для этого требуется использование наиболее точного набора метрик для оценки показателей защищенности компонентов информационной системы и информационной системы в целом. Информационные системы, применяемые в компаниях, являются многокомпонентными и включают в себя значительное число объектов и связей, что необходимо учитывать при проведении оценки защищенности и проектировании системы защиты информации. Существующие методы оценки не учитывают в полной мере особенности структуры информационной системы, фокусируясь только на реализацию отельных мер защиты и наличие в анализируемой системе конкретных средств защиты без учета вариантов конфигурации связей между элементами системы. В статье рассматривается реализация метода оценки уровня защищенности многокомпонентных корпоративных информационных систем с учетом их структуры и конфигурации отдельных элементов защиты. Предлагаемый метод оценки может быть реализован для компаний различного масштаба и широкого спектра сфер деятельности, имеющих распределенную корпоративную информационную инфраструктуру.

Ключевые слова: информационная безопасность, защита данных, информационные системы, методика оценки, кибербезопасность.

Для цитирования: *Рыленков Д.А.* Разработка метода оценки уровня защищенности многокомпонентных корпоративных информационных систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2025. № 2. С. 104 – 110. DOI: 10.18137/RNU.V9187.25.02.P.104

DEVELOPMENT OF A METHOD FOR ASSESSING THE LEVEL OF SECURITY OF MULTI-COMPONENT CORPORATE INFORMATION SYSTEMS

Abstract. Any modern company needs to ensure high-quality management of information security processes due to the spread of cyberattacks on organizations and the emergence of new threats. This requires the use of the most accurate set of metrics to assess the security indicators of the information system. components Information systems used in companies are multicomponent and include dozens of objects and a significant number of links between them. These implementation features must be taken into account when assessing security and designing an information security system. The existing security assessment methods do not fully take into account the features of the structure of the information system, focusing only on the implementation of individual data protection measures and the presence of specific security tools in the

analyzed systems without taking into account the configuration options for the links between each of the elements of the particular system. This article discusses the implementation of a method for assessing the security level of multicomponent corporate information systems, taking into account their structure and configuration of individual security elements. The proposed assessment method can be implemented for companies of various sizes and a wide range of areas of activity, as well as for companies with a distributed corporate information infrastructure.

Keywords: information security, data protection, information systems, assessment methodology, cybersecurity.

For citation: Rylenkov D.A. (2025) Development of a method for assessing the level of security of multicomponent corporate information systems. *Vestnik of Russian New University. Series: Complex Systems: Models, analysis, management*. No. 2. Pp. 104 – 110. DOI: 10.18137/RNU.V9187.25.02.P.104 (In Russian).

Для обеспечения качественного процесса управления необходимо осуществлять функции комплексного контроля параметров исследуемой системы [1–5]. При осуществлении задач управления информационной безопасностью (далее – ИБ) предприятия необходимо формирование набора метрик для оценки уровня защищенности всех компонентов информационной системы организации [6–9].

В корпоративной информационной инфраструктуре организации основными объектами защиты могут выступать:

- рабочие станции пользователей;
- используемые серверы;
- мобильные устройства, подключаемые к корпоративной сети организации;
- сетевое оборудование.

В Таблице 1 показаны конкретные примеры объектов защиты в пределах каждой из рассматриваемых групп.

Таблица 1

Примеры объектов защиты в рамках корпоративной информационной инфраструктуры организации

Группа объектов защиты	Конкретные примеры
Рабочие станции пользователей	Рабочие станции под управлением операционных систем Windows, Linux, macOS
Серверы	Сервер баз данных Web-сервер Сервер мониторинга Контроллер домена DNS-сервер Файловый сервер Сервер централизованной аутентификации
Мобильные устройства	Смартфоны и планшетные компьютеры под управлением мобильных операционных систем iOS и Android
Сетевое оборудование	Маршрутизаторы Коммутаторы Беспроводные точки доступа Межсетевые экраны

Источник: здесь и далее таблицы составлены автором.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 2 за 2025 год

Конфигурацию связей между компонентами защиты можно представить в общем случае двумя способами – параллельным и последовательным соединением.

На Рисунке 1 графически показано последовательное соединение компонентов.

Рисунок 1. Структурная схема последовательного соединения компонентов
Источник: здесь и далее рисунки выполнены автором.

На Рисунке 2 показано параллельное соединение компонентов.

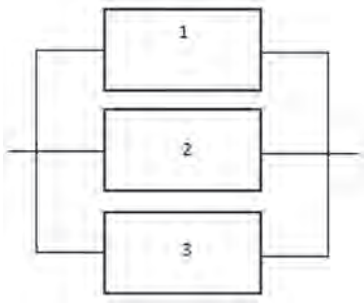

Рисунок 2. Структурная схема параллельного соединения компонентов

Допустимы также более сложные структуры с одновременным включением последовательного и параллельного типов связности [10; 11].

При последовательном соединении компонентов уровень защищенности Z будет рассчитываться по формуле

$$Z = \prod_{i=1}^{n} R_i .$$

При параллельном соединении компонентов будет действовать формула

$$Z = 1 - \prod_{i=1}^{n} \left[1 - R_i\right],$$

где R – значение уровня защищённости отдельного компонента инфраструктуры.

При этом значение R рассчитывается на основе выражения

$$R = \sum_{i=1}^{n} F_i K_i .$$

Здесь K – вес конкретного требования ИБ; F – степень его реализации; n – общее число требований ИБ.

Область значений для параметров $F \in [0;1] u K \in [0;1]$. При этом

$$\sum_{i=1}^{n} K_i = 1 .$$

Набор требований ИБ для серверной инфраструктуры включает следующие пункты [12–15]:

1) ограничение на подключение к серверным службам с ограниченным перечнем диапазонов IP-адресов;

2) выделение изолированной сети управления серверной инфраструктурой;

3) мониторинг серверных приложений;

4) ведение журналов событий активных сервисов;

5) выполнение регулярного резервного копирования данных;

6) внедрение систем бесперебойного питания;

7) отказоустойчивая кластеризация эксплуатируемых систем;

8) резервирование на уровне систем хранения данных;

9) активация шифрования в протоколах управления;

10) реализация централизованной политики обновления программного обеспечения серверных систем.

В качестве примера структуры с последовательным соединением компонентов можно представить многоуровневую архитектуру web-приложения, где выделяются три ключевых звена:

- web-сервер;
- сервер приложений;
- сервер баз данных.

Пусть общая защищенность компонента web-сервера $R1 = 0,7$, для сервера приложений $R2 = 0,9$, для сервера баз данных $R3 = 0,9$. Согласно алгоритму расчета для конфигурации с последовательным соединением компонентов общий уровень защищенности

$$Z = \prod_{i=1}^{n} R_i = 0,7 \cdot 0,9 \cdot 0,9 = 0,57.$$

В Таблице 2 отображена интерпретация значений показателя уровня защищённости Z. Полученное значение Z = 0,57 относится к среднему уровню защищенности.

Таблица 2

Интерпретация значений показателя уровня защищенности

Значение Z	**Уровень защищенности**
0,7 … 1	Высокий
0,4 … 0,69	Средний
0 … 0,39	Низкий

Для верификации разработанного метода был проведен анализ граничных условий состояния оцениваемой системы. Для варианта последовательного соединения компонентов: если один компонент из набора имеет уровень защищенности, равный нулю, вся рассматриваемая система также имеет низкий уровень защищенности:

$$Z = \prod_{i=1}^{n} R_i = R_1 R_2 \cdot 0 = 0.$$

Если уровень защищённости каждого из компонентов системы равен 1, то итоговый показатель защищенности системы будет максимальным:

$$Z = \prod_{i=1}^{n} R_i = 1 \times \ldots \times 1 = 1.$$

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 2 за 2025 год

Аналогичные расчеты выполнены для параллельной структуры:

$$Z = 1 - \prod_{i=1}^{n} [1 - 0] = 0;$$

$$Z = 1 - \prod_{i=1}^{n} [1 - 1] = 1.$$

Таким образом, предложен метод оценки уровня защищенности многокомпонентных корпоративных информационных систем, показан пример расчета для участка инфраструктуры организации, выполнен анализ разработанного метода на основе выделения граничных условий состояния оцениваемой системы. Возможно масштабирование данного метода с учетом особенностей реализации конкретной информационной системы и возможности интеграции информационных систем разного уровня. Разработанный метод может быть использован для организаций различного масштаба и специализации.

Литература

1. *Вовик А.Г.* Подход к управлению информационной безопасностью на основе комплексной формальной модели // Автоматизация процессов управления. 2024. № 3 (77). С. 55–66. DOI: 10.35752/1991-2927_2024_3_77_55. EDN OQVSGM.

2. *Тоичкин Н.А.* Проектирование архитектуры информационной системы диагностики состояний и управления безопасностью технологических процессов // Научно-технический вестник Поволжья. 2023. № 3. С. 128–132. EDN RMHINJ.

3. *Филяк П.Ю., Мильков А.О.* Подходы к управлению рисками информационной безопасности для обеспечения защиты информации в организациях // Информация и безопасность. 2016. Т. 19. № 4. С. 583–586. EDN WXCUXJ.

4. *Левина В.И.* Информационная безопасность и угрозы информационной безопасности в коммерческих организациях // Вопросы образования и науки : Сборник научных трудов по материалам международной научно-практической конференции. Тамбов, 30 ноября 2017 г. Ч. 2. Тамбов : Юком, 2017. С. 53–54. EDN YOXCXR.

5. *Болдырев А.Н.* Информационная безопасность. Виды угроз информационной безопасности // Современные тенденции развития гуманитарных, правовых и экономических исследований Республики Калмыкия: теория и практика : Сборник материалов III Республиканской студенческой научно-практической конференции, Элиста, 18 марта 2021 г. Элиста : Калмыцкий филиал Московского государственного гуманитарно-экономического университета, 2021. С. 137–140. EDN IWIEGE.

6. *Баранкова И.И., Михайлова У.В., Афанасьева М.В.* Минимизация рисков информационной безопасности на основе моделирования угроз безопасности // Динамика систем, механизмов и машин. 2019. Т. 7. № 4. С. 60–66. EDN XRTAUD.

7. *Кравцов Н.К.* Информационная безопасность как одна из составляющих экономической безопасности предприятий сферы электронной торговли // Академическая публицистика. 2021. № 11-2. С. 180–184. EDN SZIIJP.

8. *Комаров И.С.* Использование сканеров безопасности для увеличения уровня безопасности информационной системы // Новая наука: Опыт, традиции, инновации. 2016. № 4-2(77). С. 130–132. EDN VVCOER.

9. *Поколявин А.И.* Обеспечение информационной безопасности в условиях цифровизации // Татищевские чтения: актуальные проблемы науки и практики : Материалы XX Международной научно-практической конференции : В 2 т. Тольятти, 18–19 апреля 2024 г. Тольятти : Волжский университет им. В.Н. Татищева, 2024. С. 241–246. EDN NULQRC.

10. *Азарычева М.А.* Методы корреляции событий в системах управления инцидентами информационной безопасности // Актуальные тенденции и инновации в развитии российской науки : Сборник научных статей. Ч. XIII. Москва : Перо, 2022. С. 27–32. EDN THEOXJ.

11. *Благовещенский А.Н.* Организация системы обеспечения информационной безопасности предприятия // Современные проблемы безопасности жизнедеятельности: настоящее и будущее : Материалы III Международной научно-практической конференции в рамках форума «Безопасность и связь», Казань, 27–28 февраля 2014 г. Ч. 1. Казань : Научный центр безопасности жизнедеятельности, 2014. С. 73–80. EDN YUXHAD.

12. *Рыленков Д.А., Карпов Д.С.* Интегральный метод оценки уровня защищенности информационной системы // Системы автоматизации (в образовании, науке и производстве) AS'2024 : Труды Всероссийской научно-практической конференции (с международным участием), Новокузнецк, 10–12 декабря 2024 г. Новокузнецк : Сибирский государственный индустриальный университет, 2024. С. 316–318. EDN EDPLHP.

13. *Басыня Е.А.* Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия // Безопасность информационных технологий. 2018. Т. 25. № 4. С. 42–51. DOI: http://dx.doi.org/10.26583/bit.2018.4.04. EDN YQNKOD.

14. *Михно А.В., Кумратова А.М.* Обеспечение информационной безопасности облачных вычислений // Информационное общество: современное состояние и перспективы развития : Сборник материалов X международного студенческого форума. Краснодар, 25–29 декабря 2017 г. Краснодар : Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. С. 308–310. EDN YOHGLV.

15. *Савельев И.А., Боровская О.Е.* Современные подходы к комплексному обеспечению информационной безопасности в облаке // Правовая информатика. 2023. № 3. С. 89–96. EDN SCDBVL.

References

1. Vovik A.G. (2024) An approach to information security management based on a comprehensive formal model. *Automation of Control Processes*. No. 3 (77). Pp. 55–66. DOI: 10.35752/1991-2927_2024_3_77_55 (In Russian).

2. Toichkin N.A. (2023) Designing the process safety management system architecture for industrial productions. *Scientific and Technical Volga Region Bulletin*. No. 3. Pp. 128–132. (In Russian).

3. Filyak P.Yu., Mil'kov A.O. (2016) Approaches to Risk Management Information Security to Protect Information in Organizations. *Informatsiya i bezopasnost'* [Information and security]. Vol. 19. No. 4. Pp. 583–586. (In Russian).

4. Levina V.I. (2017) Information security and threats to information security in commercial organizations. In: *Voprosy obrazovaniya i nauki* [*Informatsiya I bezopasnost'* [Information and security] : Proceedings of the International Scientific and Practical Conference. Tambov, 30 November 2017. Part 2. Tambov : Yukom Publ. Pp. 53–54. (In Russian).

5. Boldyrev A.N. (2021) Information security. Types of information security threats. In: *Sovremennye tendentsii razvitiya gumanitarnykh, pravovykh i ekonomicheskikh issledovanii Respubliki Kalmykiya: teoriya i praktika* [Modern trends in the development of humanitarian, legal and economic studies of the Re-

public of Kalmykia: Theory and practice] : Proceedings of III Republican student scientific and practical conference. Elista, 18 March 2021. Elista : Kalmyk branch of the Moscow State University of Humanities and Economics Publ. Pp. 137–140. (In Russian).
6. Barankova I.I., Mikhailova U.V., Afanas'eva M.V. (2019) Minimization of information security risks based on security threat modeling. *Dinamika sistem, mekhanizmov i mashin* [Dynamics of systems, mechanisms and machines]. Vol. 7. No. 4. Pp. 60–66. (In Russian).
7. Kravtsov N.K. (2021) Information security as one of the components of economic security of enterprises in the field of electronic commerce. *Akademicheskaya publitsistika* [Academic journalism]. No. 11-2. Pp. 180–184. (In Russian).
8. Komarov I.S. (2016) Using security scanners to increase the security level of an information system. *Novaya nauka: Opyt, traditsii, innovatsii* [New Science: Experience, Tradition, Innovation]. No. 4-2 (77). Pp. 130–132. (In Russian).
9. Pokolyavin A.I. (2024) Ensuring information security in the context of digitalization. In: Tatishchevskie chteniya: aktual'nye problemy nauki i praktiki [Tatishivsky readings: Current problems of science and practice] : Proceedings of the XX International Scientific and Practical Conference : In 2 vols. Tolyatti, April 18–19, 2024. Tolyati : V.N. Tatychev Volzhsky University. Pp. 241–246. (In Russian).
10. Azarycheva M.A. (2022) Event Correlation Methods in Information Security Incident Management Systems. In: Spirina M.L. (Ed) *Aktual'nye tendentsii i innovatsii v razvitii rossiiskoi nauki* [Current trends and innovations in the development of Russian science] : Collection of scientific articles. Part XIII. Moscow : Pero Publ. Pp. 27–32. (In Russian).
11. Blagoveshchenskiy A.N. (2014) Organization of the enterprise information security system. In: Minnikhanov R.N. (Ed) *Sovremennye problemy bezopasnosti zhiznedeyatel'nosti: nastoyashchee i budushchee* [Modern problems of security of life: Present and future] : Proceedings of the III International Scientific-Practical Conference within the forum "Security and communication". Kazan, February 27–28, 2014. Part 1. Kazan : Scientific center for security of life Publ. Pp. 73–80. (In Russian).
12. Rylenkov D.A., Karpov D.S. (2024) Integral method for assessing the level of security of an information system. In: Zimin V.V. (Ed) *Sistemy avtomatizatsii (v obrazovanii, nauke i proizvodstve) AS'2024* [Automation systems (in education, science and production) AS'2024] : Proceedings of the All-Russia Scientific and Practical Conference (with international participation). Novokuznetsk, December 10–12, 2024. Nokuznetsk : Siberian State Industrial University Publ. Pp. 316–318. (In Russian).
13. Basynya E.A. (2018) Distributed system for collecting, processing and analyzing information security events of the enterprise network infrastructure. *IT Security (Russia)*. Vol. 25. No. 4. Pp. 42–51. DOI: http://dx.doi.org/10.26583/bit.2018.4.04 (In Russian).
14. Mikhno A.V., Kumratova A.M. (2018) Ensuring information security of cloud computing. In: *Informatsionnoe obshchestvo: sovremennoe sostoyanie i perspektivy razvitiya* [Information society: Current state and future development] : Proceedings of the X International Student Forum. Krasnodar, December 25–29, 2017. Krasnodar : Kuban State Agrarian University Publ. Pp. 308–310. (In Russian).
15. Savel'ev I.A., Borovskaya O.E. (2023) Modern approaches to complex ensuring of cloud information security. *Legal Informatics*. No. 3. Pp. 89–96. (In Russian).

Поступила в редакцию: 29.03.2025	Received: 29.03.2025
Поступила после рецензирования: 30.04.2025	Revised: 30.04.2025
Принята к публикации: 16.05.2025	Accepted: 16.05.2025