УДК 004.056.53
DOI: 10.26102/2310-6018/2025.49.2.025

Метод числового расчета уровня защищенности компонентов информационной инфраструктуры

Ю.В. Беликов✉

Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону, Российская Федерация

Резюме. Одним из ключевых вопросов в процессе организации информационной безопасности является оценка соответствия предъявляемым требованиям по защите инфраструктуры, а также реагирование на актуальные угрозы и риски. Данная оценка обеспечивается проведением соответствующего аудита. В отечественных и международных стандартах указываются различные методики по проведению аудита информационной безопасности, а также приводятся концептуальные модели построения процесса оценки. Однако к недостаткам этих стандартов можно отнести невозможность их углубленной адаптации в рамках отдельных информационных систем, а также частичное или полное отсутствие числовой оценки параметров безопасности, что в негативной форме может влиять на объективность оценки применяемых параметров и не отражать реальных угроз. В свою очередь адаптация числовых методов при анализе уровня зрелости процессов информационной безопасности позволяет решить ряд важных задач, например, автоматизацию процесса оценки, обеспечение более точного показателя выявления уязвимых компонентов информационной инфраструктуры, а также возможность интеграции полученных значений с иными процессами, направленными на нейтрализацию актуальных угроз безопасности со стороны злоумышленников. Целью настоящей работы являются анализ возможности применения числовой оценки уровня зрелости информационной безопасности, а также использование аппарата нечетких множеств при проведении аудита.

Ключевые слова: информационная безопасность, аудит, оценка уровня зрелости, средства защиты информации, численная оценка, нечеткие множества, нечеткая логика, критерии безопасности, риски.

Для цитирования: Беликов Ю.В. Метод числового расчета уровня защищенности компонентов информационной инфраструктуры. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1884 DOI: 10.26102/2310-6018/2025.49.2.025

Method of numerical calculation of the security level of information infrastructure components

Yu.V. Belikov✉

Rostov State University of Economics, Rostov-on-Don, the Russian Federation

Abstract. One of the key issues in the process of organizing information security is the assessment of compliance with the requirements for infrastructure protection, as well as response to current threats and risks. This assessment is ensured by conducting an appropriate audit. Domestic and international standards specify various methods for conducting an information security audit, and also provide conceptual models for constructing the assessment process. However, the disadvantages of these standards include the impossibility of their in-depth adaptation within individual information systems, as well as the partial or complete lack of a numerical assessment of security parameters, which can negatively affect the objectivity of the assessment of the parameters used and not reflect real threats. In turn, the adaptation of numerical methods in the analysis of the maturity level of information security processes allows solving a number of important problems, for example, automation of the assessment

process, providing a more accurate indicator of identifying vulnerable components of the information infrastructure, as well as the ability to integrate the obtained values with other processes aimed at neutralizing current security threats from intruders. The purpose of this work is to analyze the possibility of using a numerical assessment of the maturity level of information security, as well as the use of fuzzy sets in the audit.

Keywords: information security, audit, maturity level assessment, information security tools, numerical assessment, fuzzy sets, fuzzy logic, security criteria, risks.

For citation: Belikov Yu.V. Method of numerical calculation of the security level of information infrastructure components. *Modeling, Optimization and Information Technology*. 2025;13(2). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1884 DOI: 10.26102/2310-6018/2025.49.2.025

Введение

В международном стандарте ISO 19011:2018 «Guidelines for auditing management systems», IDT (ГОСТ Р ИСО 19011-2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента. Conformity assessment. Guidelines for auditing management systems») аудитом информационной безопасности являются процессы объективного оценивания параметров и методов защиты инфраструктуры в соответствии с установленными критериями нормативных документов. В связи с этим можно считать, что целью проведения аудита информационной безопасности организации является общая оценка уровня зрелости процессов защиты информационных активов, а также выработка стратегии, направленной на снижение потенциального риска наступления негативных событий вследствие реализации угроз [1]. Основанием для проведения аудита могут быть следующие факторы:

1) регулярное выявление инцидентов информационной безопасности, повлекших финансовые и репутационные ущербы;
2) развитие инфраструктуры организации;
3) общее снижение уровня информационной безопасности организации;
4) добровольное проведение аудита с целью проверки уровня зрелости процессов информационной безопасности.

Проводя аудит информационной безопасности с целью получения оценки уровня зрелости процессов защиты данных в инфраструктуре специалистам необходимо определить основные направления анализа информационных систем в соответствии с наиболее вероятными рисками нарушения конфиденциальности, целостности и доступности информации [2]. К данным направлениям оценки уровня безопасности относятся следующие цели:

– анализ актуальных рисков компонентов информационной инфраструктуры;
– выявление менее защищённых компонентов или направлений ИТ-технологий в инфраструктуре;
– оценка соответствия требованиям по информационной безопасности;
– выработка стратегии развития информационной безопасности.

Однако, исходя из существующих методов проведения аудита, а также анализируя существующие стандарты, можно отметить, что оценка уровня зрелости процессов информационной безопасности зачастую проводится в форме анкетирования с формализованными вариантами ответа: положительными или отрицательными. Несмотря на высокую степень проработанности международных стандартов, а также фундаментальность приводимых методов, их применение на практике не всегда может показать высокую степень эффективности, особенно в контексте информационных активов с ограниченным финансированием информационных технологий и, в частности, информационной безопасности. Кроме того, рекомендательный характер большинства

международных стандартов ограничивает их универсальность и снижает эффективность их использования в процессах оценки уровня зрелости процессов обеспечения информационной безопасности. Данная особенность не позволяет получить объективной картины о состоянии информационной безопасности как отдельных информационных (автоматизированных) систем или их компонентов, так и о процессах по защите данных в организации в целом [3]. Для проведения максимально объективной оценки необходимо проводить четкую декомпозицию аудируемых параметров и применять численный анализ данных.

Применение метода численной оценки критериев безопасности

С точки зрения оценки зрелости процессов обеспечения информационной безопасности рассматриваемые меры защиты можно разделять на организационные, технические, инженерные и прочие. Анализ международных стандартов в области аудита безопасности показывает, что процедура оценивания защищенности инфраструктуры зачастую представляет собой анкетирование, подразумевающее либо положительный, либо отрицательный ответ. Данная форма проверки соответствия требованиям по безопасности может являться эффективной в том случае, если оценке подлежат организационные меры защиты или технические меры, представляющие ключевые механизмы безопасности. Например, на вопрос аудитора о наличии в организации локального акта, описывающего парольную политику, можно дать однозначный ответ. Аналогичные ответы можно дать в отношении наличия в организации системы SIEM. Классический подход в оценке уровня зрелости процессов информационной безопасности описан в следующих международных стандартах [4]:

– Trusted Computer System Evaluation Criteria – «оранжевая книга» один из первых стандартов в области оценки защищенности информационной инфраструктуры. Разработанный в США в 1980-х годах в рамках задач Министерства обороны США, стандарт описывал процесс классификации информационных систем по уровням безопасности. Несмотря на то, что стандарт был разработан и введен более 40 лет назад, специалисты по информационной безопасности до сих пор руководствуются политиками «оранжевой книги»;

– Information Technology Security Evaluation Criteria – данный Европейский стандарт стал развитием Trusted Computer System Evaluation Criteria. Более гибкие подходы к оценке процессов информационной безопасности и четкое разделение функциональных требований и требований к уровню доверия позволили оценивать безопасность систем с учетом их конкретного назначения и контекста применения. Настоящий стандарт стал важным этапом в эволюции оценки защищенности и оказал значительное влияние на создание современного универсального стандарта ISO/IEC 15408;

– Рекомендации X.800 – настоящий стандарт определяет общую архитектуру безопасности для открытых телекоммуникационных систем, устанавливая базовые принципы, услуги и механизмы обеспечения информационной безопасности. Документ предлагает универсальную модель, охватывающую ключевые аспекты защиты, такие как контроль доступа, конфиденциальность, целостность, аутентификацию и управление безопасностью. X.800 служит теоретической основой для построения комплексных систем защиты и стандартизации подходов в области телекоммуникационной и информационной безопасности, обеспечивая согласованность при разработке и внедрении защитных мер в гетерогенных сетевых средах;

– BSI – стандарты безопасности, разработанные Федеральным ведомством по информационной безопасности Германии (BSI) являются комплексными методическими

подходами к обеспечению информационной безопасности. Эти стандарты ориентированы на практическое внедрение и поддержание системы управления информационной безопасностью с учетом типовых угроз и мер защиты. BSI обеспечивает структурированную и масштабируемую модель, подходящую как для крупных организаций, так и для малых предприятий. Методология BSI оказала значительное влияние на развитие европейских и международных стандартов, включая ISO/IEC 27001, и активно используется в государственных и частных секторах Германии и за ее пределами;

– BS 7799-3:2006 – представляет собой часть британской серии стандартов в области информационной безопасности и дополняет ранее разработанные BS 7799-1 и BS 7799-2. Основное внимание в BS 7799-3 уделяется управлению рисками информационной безопасности. Он предоставляет методологию идентификации, оценки и управления рисками, лежащими в основе построения эффективной системы управления информационной безопасностью (СУИБ). Стандарт гармонизирован с принципами ISO/IEC 27001 и служит основой для интеграции процессов управления рисками в общую систему корпоративного управления безопасностью. BS 7799-3:2006 способствует системному и обоснованному подходу к снижению рисков и принятию решений в сфере защиты информации;

– ISO/IEC 17799:2000 «Information technology. Code of practice for security management» – международный стандарт, содержащий свод передовой практики по управлению информационной безопасностью. Он основан на британском стандарте BS 7799-1 и охватывает широкий спектр аспектов защиты информации – от организационных до технических, включая политику безопасности, управление доступом, физическую защиту, обеспечение непрерывности бизнеса и другие ключевые направления. Стандарт служит практическим руководством для организаций при создании, внедрении и поддержании системы управления информационной безопасностью. ISO/IEC 17799 стал основой для дальнейшего развития серии стандартов ISO/IEC 27000 и сыграл важную роль в формировании международных подходов к построению безопасной информационной среды;

– ISO/IEC 15408-1:2009 «Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model»;

– Control Objectives for Information and related Technology – это методология и фреймворк, разработанный ISACA для управления ИТ и обеспечения информационной безопасности в организациях. COBIT предоставляет структуру для выстраивания, мониторинга и совершенствования процессов управления ИТ, акцентируя внимание на согласовании ИТ-целей с бизнес-целями, управлении рисками и контроле за эффективностью.

Однако, когда речь заходит о количественной оценке параметров безопасности становится невозможным получение объективных данных на основе элементарных бинарных ответов. Другими словами, процесс аудита безопасности не может быть сведен к формальным положительным или отрицательным ответам на вопросы, указанные в программе аудита [5]. В случае, когда оцениваются критерии технической безопасности информационной инфраструктуры необходимо интерпретировать численное (процентное) соответствие предъявляемым требованиям.

Исходя из данных фактов перед специалистами по информационной безопасности, участвующим в аудите, встает ключевая задача – декомпозиция оцениваемых параметров на числовую и качественную оценку соответствия требованиям. Для этого необходимо определить, какие параметры можно рассчитать

числовым методом. К наиболее популярным численным параметрам оценки уровня зрелости информационной безопасности могут относится:

– покрытие вычислительных устройств антивирусными средствами защиты информации;

– покрытие вычислительных устройств средствами предотвращения утечки информации;

– покрытие вычислительных устройств средствами предотвращения вторжений;

– количество вычислительных устройств, подключенных к единой системе сбора и корреляции событий;

– количество веб-сервисов, защищаемых WAF;

– количество устройств, управляемых групповыми политиками;

– и т. д.

Для оценки параметров зрелости, связанных с количественным покрытием средствами защиты информации вычислительных устройств, необходимо выяснить процентное соотношение защищенных устройств к общему числу эксплуатируемой техники [6]. Исходя из этого формула оценки представленных выше критериев в общем виде будет иметь следующий вид:

$$P = \frac{P_x}{P_y} \cdot 100\%,$$

где P – общая оценка исследуемого параметра, P_x – реальные показатели покрытия, P_y – общее количество устройств.

При оценке критериев покрытия информационной инфраструктуры средствами защиты крайне важно учитывать архитектуру защищаемого программного обеспечения. Для этого следует провести дополнительную декомпозицию по ключевым характеристиками объектов инфраструктуры. Так, например, при определении оценки покрытия средствами класса DLP не рационально учитывать устройства, в том числе виртуальные, используемые в технологических процессах, доступ к которым ограничен для пользователей [7]. Также примером корректной оценки является расчет покрытия средствами антивирусной защиты устройств разных классов функциональности: рабочие места пользователей («тонкие» и «толстые» клиенты), серверные операционные системы, файловые хранилища, системы управления базами данных, системы виртуализации, докеры и т. д.

Указанный подход позволяет наиболее точно определить возможное несоответствие требованиям по безопасности, а также оценить гипотетические риски при реализации угроз безопасности информации [8].

Пример реализации предложенного метода

В частном случае оценку покрытия вычислительных устройств антивирусными средствами защиты информации следует рассчитывать по формуле:

$$P_{av} = \frac{P_{hav}}{P_{hm}} \cdot 100\%,$$

где P_{av} – оценка покрытия вычислительных устройств антивирусными средствами защиты информации, P_{hav} – количество устройств с установленными средствами антивирусной защиты информации, P_{hm} – общее количество устройств.

Например, в организации функционирует 4321 автоматизированное рабочее место. Всего под защитой антивирусной программы находятся 3589 устройств, тогда:

$$P_{av} = \frac{3589}{4321} \cdot 100\% \approx 83\ \%.$$

Значит, процентное покрытие устройств антивирусным программным обеспечением составляет 83 %. Исходя из данной оценки аудитор может принять решение о соответствии или несоответствии предъявляемым требованиям.

Формула оценки покрытия вычислительных устройств средствами предотвращения утечки информации:

$$P_{dlp} = \frac{P_{hdlp}}{P_{hm}} \cdot 100\ \%,$$

где P_{dlp} – оценка покрытия вычислительных устройств средствами предотвращения утечки информации, P_{hdlp} – количество устройств с установленными средствами предотвращения утечки информации, P_{hm} – общее количество устройств.

Формула оценки покрытия вычислительных устройств средствами предотвращения вторжений:

$$P_{ips} = \frac{P_{hips}}{P_{hm}} \cdot 100\%,$$

где P_{ips} – оценка покрытия вычислительных устройств средствами предотвращения вторжений, P_{hips} – количество устройств с установленными средствами предотвращения вторжений, P_{hm} – общее количество устройств.

Формула оценки покрытия вычислительных устройств, подключенных к единой системе сбора и корреляции событий:

$$P_{edr} = \frac{P_{hedr}}{P_{hm}} \cdot 100\ \%,$$

где P_{edr} – оценка подключения устройств к единой системе сбора и корреляции событий, P_{hedr} – количество устройств, подключенных единой системе сбора и корреляции событий, P_{hm} – общее количество устройств.

Аналогичным образом возможно проведение расчетов и для других компонентов информационных систем или количества используемых средств защиты информации.

Исходя из проведенных расчетов, возможна консолидация результатов в графическом виде для формирования отчета по аудиту информационной безопасности и определению процессов, наиболее подверженных риску. Наиболее применимым в данном случае является диаграмма паука, как система логических утверждений, использующая экзистенциальные точки в процессе построения [9].

В качестве примера обратимся к ранее приведенным показателям оценки безопасности автоматизированных рабочих мест:

- покрытие антивирусными средствами защиты P_{av} = 83 %;
- покрытие агентами DLP P_{dlp} = 34 %;
- покрытие устройств системами предотвращения вторжений P_{ips} = 83 %;
- покрытие устройств средствами EDR P_{edr} = 91 %.

А также предложим дополнительные показатели:

– количество доменных устройств, управляемых политикой безопасности P_{ad} = 95 %;

– количество устройств, использующих для авторизации второй фактор P_{sfa} = 12 %.

На основе данных расчетов становится возможным построение диаграммы для визуализации комплексной оценки уровня зрелости процессов информационной безопасности в части, касающейся технической защиты (Рисунок 1).

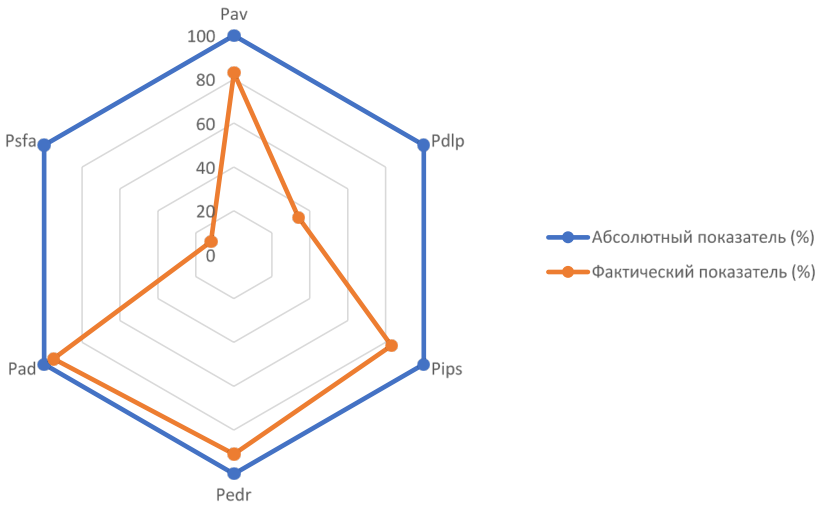

Рисунок 1 – Оценка покрытия средствами защиты информации вычислительных устройств
Figure 1 – Assessment of information security measures coverage for computing devices

Данные, полученные в ходе указанных расчетов, позволяют рассматривать процесс аудита безопасности не только с точки зрения не только классической экспертной, но и числовой оценки [10]. Наиболее эффективным инструментом для подобных расчетов является метод нечетких множеств.

На практике нечеткая логика представляет собой универсальный инструмент для проведения аналитики данных и создания систем поддержки принятия решений в условиях неопределенности [11]. Ее особенности делают теорию нечетких множеств эффективным инструментом в различных областях бизнеса и информационных технологий, таких как анализ рисков, оценка угроз и аудит безопасности [12, 13].

Главным принципом нечеткой логики является концепция применения лингвистических переменных, которые, с помощью заранее определенных лингвистических, описывает абстрактные количественные параметры. Данная переменная характеризуется высокой степенью субъективности и не может быть точно представлена с помощью математических значений. Например, объем сетевого трафика, генерируемого в ходе компьютерной атаки, можно представить как нечеткое множество: интенсивность атаки оценивается по шкале от 1 до 5, где 1 обозначает низкий поток трафика, соответствующий первичной разведке опубликованных сервисов, а 5 – целенаправленную DDoS-атаку, использующую тысячи IP-адресов. В этом примере числовые значения интенсивности атаки ассоциируются с лингвистическими значениями. Шкала включает не только крайние значения, но и промежуточные, называемые интервалами. Эти интервалы описывают параметры интенсивности атаки, при этом различия между соседними интервалами минимальны, и изменение одного значения приводит к изменению всего множества [14, 15].

Анализ научных источников показывает, что теория нечетких множеств активно используется в различных областях информационной безопасности, включая:

– оценку рисков негативных событий, связанных с уязвимостями или инцидентами, которые могут повлиять на конфиденциальность, целостность и доступность информации;
– анализ аномалий в информационной инфраструктуре;
– оценку выбора средств защиты;
– качественную оценку параметров работы сервисов безопасности.

Принцип данного метода заключается в определении алгоритма фаззификации на основе определения нечеткого классификатора и в общем виде сводится к следующим этапам: определение лингвистических переменных (термы) и разработка правил нечеткого вывода.

В общем виде задача оценки уровня зрелости сводится с помощью аппарата нечеткой логики к следующему: имеются множество термов $L = \{l_1, l_2, \dots, l_m\}$ и универсальное множество $U = \{u_1, u_2, \dots, u_n\}$. Нечеткое множество $\widetilde{l_j}$, которым описывается лингвистический терм l_j, где $j = \overline{1,m}$, на универсальном множестве U представляется в виде следующей формулы:

$$\widetilde{l_j} = \left(\frac{\mu_{l_j}(u_1)}{u_1}, \frac{\mu_{l_j}(u_2)}{u_2}, \dots, \frac{\mu_{l_j}(u_n)}{n}\right),$$

где $\mu_{l_j}(u_i)$ – степень принадлежности нечеткому множеству, вычисляемая по формуле:

$$\mu_{l_j}(u_i) = \frac{1}{E}\sum_{e=\overline{1,E}} o_{j,i}^{e}, \text{ при } i = \overline{1,n},$$

где E – количество экспертов, $o_{j,i}^{e}$ – мнение e-го эксперта о наличии у элемента u_i свойств нечеткого множества $\widetilde{l_j}$.

Дальнейший алгоритм применения метода нечетких множеств сводится к определению входных и выходных параметров, а также разработке принципа фаззификации и дефаззификации данных параметров. Входные параметры представляют собой совокупность требований информационной безопасности, определенных в ходе аудита, а выходные параметры –это итоговая оценка. При применении нечеткой логики каждому из входных и выходных параметров присваиваются соответствующие лингвистические переменные, называемые термами [16].

В качестве входных параметров могут применяться ранее указанные оцениваемые характеристики. Тогда выходными параметрами может являться оценка уровня покрытия автоматизированных рабочих мест средствами защиты, которая определяется по следующим критериям:

- «низкий» – до 10 % покрытия;
- «ниже среднего» – от 30 % до 50 % покрытия;
- «средний» – от 50 % до 70 % покрытия;
- «выше среднего» – от 70 % до 90 % покрытия;
- «высокий» – от 90 % покрытия.

В данном примере выходные параметры, а также их математические интервалы могут определяться экспертной оценкой или соответствовать требованиям ранее установленных нормативных актов, описывающих процессы информационной безопасности в аудируемой организации [17].

Сама процедура фаззификации представляет собой набор правил в виде X_i: $IF\ (P_1\ IS\ S_1^j)\ AND\ (P_2\ IS\ S_2^j)\ AND \dots AND\ (P_n\ IS\ S_i^j)\ THEN\ Y_i = Z_i^j$, где X_i – номер i-го правила; IF, AND, THEN – логические операторы; P_n – входные лингвистические данные, S_i^j, Z_i^j – нечеткие подмножества, Y_i – выходная переменная *i*-го правила.

Исходя из представленных ранее оценок, а также указанных множеств результирующая оценка составляет 66,3 %, что соответствует «среднему» уровню защищенности автоматизированных рабочих мест.

Заключение

Действующая система отечественных и международных стандартов, регламентирующих оценку уровня зрелости процессов информационной безопасности, предоставляет достаточно проработанную основу для проведения всесторонней оценки применяемых средств защиты и организационных мер. Представленные в настоящей работе стандарты охватывают ключевые аспекты анализа информационной инфраструктуры, позволяя осуществлять комплексный подход к оценке текущего состояния уровня безопасности данных. Однако, учитывая стремительное развитие технологий, появление

новых векторов киберугроз и постоянное совершенствование методов их реализации, становится очевидной необходимость регулярного пересмотра существующих подходов к аудиту и управления рисками в сфере информационной безопасности.

В представленной работе рассматривается усовершенствованный метод расчета показателей эффективности покрытия информационной инфраструктуры средствами защиты на основе применения аппарата нечетких множеств, направленный на повышение точности анализа зрелости процессов информационной безопасности. Предложенный подход обеспечивает высокий уровень объективности полученного результата и позволяет не только оценить текущее состояние реализуемых защитных мер и общий уровень зрелости процессов информационной безопасности, но и выявить уязвимые направления, требующие дополнительного внимания со стороны специалистов.

Важнейшим преимуществом разработанного метода является использование теории нечетких множеств для обработки и интерпретации данных. Это обеспечивает более гибкий и точный подход к оценке зрелости процессов безопасности в условиях неопределенности и неполноты информации, что особенно важно при работе с качественными показателями и экспертными оценками. Таким образом, предложенная методика представляет собой эффективный инструмент в арсенале специалистов по информационной безопасности, обеспечивая возможность адаптации к изменяющемуся ландшафту угроз и способствуя принятию обоснованных управленческих решений.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Александров А.В., Велигура А.В., Соколова Я.В. Методика комплексной оценки состояния информационной безопасности предприятия. *Экономический вектор.* 2016;(2):104–112.
   Alexandrov A.V., Veligura A.V., Sokolova Ya.V. Method of Comprehensive Assessment of Information Security of the Companies. *Economic Vector.* 2016;(2):104–112. (In Russ.).
2. Беликов Ю.В. Применение метода нечетких множеств в процессе проведения аудита информационной безопасности. *Инженерный вестник Дона.* 2025;(4). URL: http://ivdon.ru/ru/magazine/archive/n4y2025/9968
   Belikov Yu.V. Application of the Fuzzy Set Method in the Information Security Audit Process. *Engineering Journal of Don.* 2025;(4). (In Russ.). URL: http://ivdon.ru/ru/magazine/archive/n4y2025/9968
3. Иванова Н.В., Коробулина О.Ю. Метод аудита информационной безопасности информационных систем. *Известия Петербургского университета путей сообщения.* 2010;(4):143–153.
   Ivanova N.V., Korobulina O.Yu. Audit Method of Information Security of the Information Systems. *Proceedings of Petersburg Transport University.* 2010;(4):143–153. (In Russ.).
4. Коваленко Б.Б., Вакуленко А.А., Сорокопудов Н.С. Инструменты выбора метода аудита информационной безопасности предприятия. *Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент.* 2019;(3):163–169. https://doi.org/10.17586/2310-1172-2019-12-3-163-169
   Kovalenko B.B., Vakulenko A.A., Sorokopudov N.S. The Selection Tools of Information Security Audit's of the Enterprise Method. *Scientific Journal NRU ITMO. Series: Economics and Environmental Management.* 2019;(3):163–169. (In Russ.). https://doi.org/10.17586/2310-1172-2019-12-3-163-169
5. Никитина Т.О. Аудит систем управления инцидентами информационной безопасности. *Экономика и социум.* 2024;(12–1):954–957.
   Nikitsina T. Audit of Information Security Incident Management Systems. *Ekonomika i sotsium.* 2024;(12–1):954–957. (In Russ.).
6. Воеводин В.А., Маркин П.В., Маркина М.С., Буренок Д.С. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов

значимости свидетельств аудита на основе метода анализа иерархий. *Системы управления, связи и безопасности.* 2021;(2):96–129. https://doi.org/10.24412/2410-9916-2021-2-96-129
Voevodin V.A., Markin P.V., Markina M.S., Burenok D.S. Technique for Developing an Information Security Audit Program Taking into Account the Weight Coefficients Of Certificates Audit Based on the Hierarchy Analysis Method. *Systems of Control, Communication and Security.* 2021;(2):96–129. (In Russ.). https://doi.org/10.24412/2410-9916-2021-2-96-129

7. Воеводин В.А., Маркина М.С., Маркин П.В. Определение весомости аудиторских свидетельств методом бальных оценок при аудите информационной безопасности. *Computational Nanotechnology.* 2020;7(1):57–62. https://doi.org/10.33693/2313-223X-2020-7-1-57-62
Voevodin V.A., Markina M.S., Markin P.V. Determination of the Weight of Audit Evidence by the Method of Point Ratings in the Information Security Audit. *Computational Nanotechnology.* 2020;7(1):57–62. (In Russ.). https://doi.org/10.33693/2313-223X-2020-7-1-57-62
8. Mynuddin M., Hossain M.I., Khan S.U., Islam M.A., Ahad D.M.A., Tanvir M.Sh. Cyber Security System Using Fuzzy Logic. In: *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 19–21 July 2023, Tenerife, Canary Islands, Spain.* IEEE; 2023. P. 1–6. https://doi.org/10.1109/ICECCME57830.2023.10252778
9. Alali M., Almogren A., Hassan M.M., Rassan I.A.L., Bhuiyan M.Z.A. Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System. *Computers & Security.* 2018;74:323–339. https://doi.org/10.1016/j.cose.2017.09.011
10. Любухин А.С. Методы анализа рисков информационной безопасности: нечеткая логика. *International Journal of Open Information Technologies.* 2023;11(2):66–71.
Lyubukhin A.S. Information Security Risk Analysis Methods: Fuzzy Logic. *International Journal of Open Information Technologies.* 2023;11(2):66–71. (In Russ.).
11. Беликов Ю.В. Разработка нечеткого классификатора входящих заявок на предоставление доступа пользователей к информационной инфраструктуре. *Инженерный вестник Дона.* 2024;(9). URL: http://ivdon.ru/ru/magazine/archive/n9y2024/9472
Belikov Yu.V. Development of a Fuzzy Classifier of Incoming Requests for Providing User Access to the Information Infrastructure. *Engineering Journal of Don.* 2024;(9). (In Russ.). URL: http://ivdon.ru/ru/magazine/archive/n9y2024/9472
12. Ouechtati H., Nadia B.A., Lamjed B.S. A Fuzzy Logic-Based Model for Filtering Dishonest Recommendations in the Social Internet of Things. *Journal of Ambient Intelligence and Humanized Computing.* 2023;14(5):6181–6200. https://doi.org/10.1007/s12652-021-03127-7
13. Yang Ya.L., Zhou Ya.H. A Fuzzy Logic Based Information Security Risk Assessment Method. *Applied Mechanics and Materials.* 2011;130–134:3726–3730. https://doi.org/10.4028/www.scientific.net/AMM.130-134.3726
14. Kerimkhulle S., Dildebayeva Zh., Tokhmetov A., et al. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. *Symmetry.* 2023;15(10). https://doi.org/10.3390/sym15101958
15. Гузаиров М.Б., Машкина И.В., Степанова Е.С. Метод определения ценности информации с использованием аппарата нечеткой логики. *Безопасность информационных технологий.* 2012;19(1):18–29.
Guzairov M.B., Mashkina I.V., Stepanova E.S. The Method of Information Value Estimation Using Fuzzy Logic Tools. *IT Security (Russia).* 2012;19(1):18–29. (In Russ.).

16. Баранова Е.К., Гусев А.М. Методика анализа рисков информационной безопасности с использованием нечёткой логики на базе инструментария MATLAB. *Образовательные ресурсы и технологии.* 2016;(1):88–96.
Baranova E.K., Gusev A.M. The Method of Information Security Risk Analysis Using Fuzzy Logic Based Tools MATLAB. *Educational Resources and Technologies.* 2016;(1):88–96. (In Russ.).
17. Аникин И.В. Нечеткая оценка факторов риска информационной безопасности. *Безопасность информационных технологий.* 2016;23(1):78–87.
Anikin I.V. Fuzzy Assessment of Information Security Risk Factors. *IT Security (Russia).* 2016;23(1):78–87. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THEAUTHORS

Беликов Юрий Владимирович, аспирант, Ростовский государственный экономический университет (РИНХ), Ростов-на-Дону, Российская Федерация
e-mail: belyuvl@gmail.com
ORCID: 0000-0001-8835-795X

Yuri V. Belikov, Postgraduate, Rostov State University of Economics, Rostov-on-Don, the Russian Federation.

Статья поступила в редакцию 21.04.2025; одобрена после рецензирования 12.05.2025; принята к публикации 20.05.2025.

The article was submitted 21.04.2025; approved after reviewing 12.05.2025; accepted for publication 20.05.2025.