DOI: 10.37791/2687-0649-2025-20-5-100-120

# Многокритериальная оценка угроз информационной безопасности на основе технологий цифровых двойников и разведки угроз

***И.В. Котенко***[1*]***, И.Б. Саенко***[1]***, Е.С. Митяков***[2]
[1]*Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Россия*
[2]*МИРЭА – Российский технологический университет, Москва, Россия*
[*]*ivkote@comsec.spb.ru*

**Аннотация.** В настоящее время проблема обеспечения информационной безопасности критической информационной инфраструктуры неуклонно возрастает и приобретает стратегическое значение, что вызвано взрывным ростом сложных целевых атак на инфраструктурные объекты. Решение этой проблемы требует разработки новых подходов к оценке угроз информационной безопасности, сочетающих актуальность данных, предоставляемых технологией разведки угроз, с глубоким пониманием специфики защищаемых систем. Анализ состояния проблемы показывает, что существующие подходы к оценке угроз информационной безопасности для объектов критической информационной инфраструктуры обладают такими недостатками, как разрыв между данными разведки угроз и контекстом конкретной системы, субъективность качественных оценок и сложность ранжирования угроз с учетом множества противоречивых критериев. Для преодоления этих недостатков в статье предложен метод многокритериальной оценки угроз информационной безопасности объектов критической информационной инфраструктуры, интегрирующий технологии разведки угроз и цифровых двойников, в котором технология цифровых двойников призвана обеспечить необходимое понимание объектной специфики. Разработана система показателей, структурированная по пяти проекциям оценки угроз: тяжесть последствий, возможности нарушителя, уязвимость объекта, сложность атаки и эффективность защиты. Разработана концептуальная модель системы оценки угроз информационной безопасности, основанной на применении технологий цифровых двойников и разведки угроз. Представлена методика многокритериальной оценки угроз, в которой производятся расчеты интегрального индекса угрозы и Парето-оптимальных рангов угроз по совокупности критериев. Экспериментальное апробирование на синтетических данных подтвердило согласованность результатов этих расчетов. Практическое применение предложенного метода позволяет проводить анализ угроз как в целом, так и в рамках отдельных проекций системы показателей.

**Ключевые слова:** угроза информационной безопасности, разведка угроз, цифровое моделирование, цифровые двойники, многокритериальный анализ, информационная безопасность

**Для цитирования:** *Котенко И.В., Саенко И.Б., Митяков Е.С.* Многокритериальная оценка угроз информационной безопасности на основе технологий цифровых двойников и разведки угроз // Прикладная информатика. 2025. Т. 20. № 5. С. 100–120. DOI: 10.37791/2687-0649-2025-20-5-100-120

# Multi-criteria assessment of information security threats based on the technologies of digital twins and threat intelligence

***I. Kotenko*[1*], *I. Saenko*[1], *E. Mityakov*[2]**
[1]*Saint Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia*
[2]*MIREA – Russian Technological University, Moscow, Russia*
[*]*ivkote@comsec.spb.ru*

**Abstract.** Currently, the problem of ensuring information security of critical information infrastructure is steadily increasing and acquiring strategic importance, which is caused by the explosive growth of complex targeted attacks on infrastructure facilities. The solution to this problem requires the development of new approaches for assessing information security threats that combine the relevance of data provided by threat intelligence technology with a deep understanding of the specifics of the protected systems. An analysis of the state of the problem shows that existing approaches for assessing information security threats to critical information infrastructure facilities have such shortcomings as a gap between threat intelligence data and the context of a specific system, subjectivity of qualitative assessments, and the complexity of ranking threats given many conflicting criteria. To overcome these shortcomings, the article proposes a method for multi-criteria assessment of information security threats to critical information infrastructure facilities that integrates threat intelligence and digital twin technologies, where the digital twin technology is designed to provide the necessary understanding of object specifics. A system of indicators has been developed, structured according to five projections of threat assessment: severity of consequences, intruder capabilities, vulnerability of the facility, complexity of the attack, and effectiveness of protection. A conceptual model of an information security threat assessment system based on the technologies of digital twins and threat intelligence has been developed. A multi-criteria threat assessment methodology is presented, in which the integral threat index and Pareto-optimal threat ranks are calculated based on a set of criteria. Experimental testing on synthetic data confirmed the consistency of the results of these calculations. Practical application of the proposed method allows for threat analysis both as a whole and within individual projections of the indicator system.

**Keywords:** information security threat, threat intelligence, digital modeling, digital twins, multi-criteria analysis, information security

**For citation:** Kotenko I., Saenko I., Mityakov E. Multi-criteria assessment of information security threats based on the technologies of digital twins and threat intelligence. *Prikladnaya informatika*=Journal of Applied Informatics, 2025, vol.20, no.5, pp.100-120 (in Russian). DOI: 10.37791/2687-0649-2025-20-5-100-120



## Введение

Экспоненциальный рост сложных целевых атак на объекты критической информационной инфраструктуры (КИИ) требует разработки новых подходов к оценке угроз, сочетающих актуальность данных разведки угроз (РУ, Threat Intelligence – TI) с глубоким пониманием специфики защищаемых систем. Существующие подходы к оценке угроз информационной безопасности (ИБ) для объектов КИИ сталкива-