УДК 004.056.53
DOI: 10.26102/2310-6018/2025.49.2.013

Метод количественной оценки опасности реализации угроз безопасности информации объектов критической информационной инфраструктуры потенциальными нарушителями

Д.В. Чернов✉

Тульский государственный университет, Тула, Российская Федерация

Резюме. В условиях нарастающей информатизации различных производственных сфер, когда большинство технологических процессов и информационных потоков автоматизируются и управляются средствами вычислительной техники, выбор мер по обеспечению безопасности информации (БИ) объектов критической информационной инфраструктуры (ОКИИ) становится актуальной проблемой. В статье рассматриваются существующие методы и подходы к оценке опасности реализации угроз БИ ОКИИ, к которым относятся автоматизированные системы управления технологическими процессами, информационные системы и информационно-телекоммуникационные сети. Указанные подходы помогают специалистам в области БИ оценить риски, связанные с возможными кибератаками и утечками данных. Предложен метод количественной оценки степени опасности реализации угроз БИ, основанный на интеллектуальном анализе данных, хранящихся в подсистеме журналирования ОКИИ. Метод позволяет количественно оценить степень опасность реализации угроз БИ потенциальными нарушителями применительно к конкретному ОКИИ. Разработанный метод дополняет располагаемые оценки специалистов в области БИ путем формирования экспертных оценок со стороны дополнительно привлекаемых специалистов – профессионалов в области технологических процессов и информационных потоков КИИ. Результаты исследования рекомендованы для использования при моделировании угроз БИ и разработке требований к средствам защиты информации в ОКИИ.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, автоматизированная система управления, технологический процесс, угроза, нарушитель, потенциал, опасность реализации угроз, риск, ущерб.

Для цитирования: Чернов Д.В. Метод количественной оценки опасности реализации угроз безопасности информации объектов критической информационной инфраструктуры потенциальными нарушителями. *Моделирование, оптимизация и информационные технологии.* 2025;13(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1870 DOI: 10.26102/2310-6018/2025.49.2.013

A method for quantifying the danger of implementing threats to the information security of objects of critical information infrastructure by potential violators

D.V. Chernov✉

Tula State University, Tula, the Russian Federation

Abstract. In the context of increasing informatization of various production areas, when most technological processes and information flows are automated and controlled by computer technology, the choice of measures to ensure the security of information (SI) of critical information infrastructure objects (CIIO) becomes a pressing issue. The article discusses existing methods and approaches to assessing the risk of implementing SI threats to CIIO, which include automated process control systems, information systems, and information and telecommunication networks. These approaches help SI

specialists assess the risks associated with possible cyberattacks and data leaks. A method is proposed for quantitatively assessing the degree of danger of implementing SI threats based on the intelligent analysis of data stored in the CIIO logging subsystem. The method allows for a quantitative assessment of the degree of danger of implementing SI threats by potential violators with respect to a specific CIIO. The developed method complements the available assessments of SI specialists by forming expert assessments from additionally involved specialists - professionals in the field of technological processes and information flows of CIIO. The results of the study are recommended for use in modeling SI threats and developing requirements for information security tools in the CIIO.

Keywords: information security, critical information infrastructure, automated control system, technological process, threat, violator, potential, danger of threat realization, risk, damage.

For citation: Chernov D.V. A method for quantifying the danger of implementing threats to the information security of objects of critical information infrastructure by potential violators. *Modeling, Optimization and Information Technology.* 2025;13(2). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1870 DOI: 10.26102/2310-6018/2025.49.2.013

Введение

Аналитические отчеты ведущих отечественных и зарубежных производителей систем и средств защиты информации указывают на возрастающую активность потенциальных нарушителей режима информационной безопасности (ИБ) (хакеров и представителей разведывательных сообществ), направленную на хищение информации и подрыв работоспособности промышленных систем, относящиеся в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ[1] к объектам критической информационной инфраструктуры (ОКИИ), в отношении которых необходимо выполнять комплекс мероприятий, направленных на обеспечение безопасности информации (БИ).

В условиях стремительного развития технологий и увеличения объемов обрабатываемых данных, угрозы ИБ становятся все более сложными и разнообразными. Современные кибератаки на ОКИИ могут иметь серьезные последствия не только для отдельных организаций, но и для национальной безопасности в целом. В связи с этим, актуальность разработки и внедрения эффективных методов оценки опасности реализации возможных угроз ИБ потенциальными нарушителями возрастает.

В октябре 2023 года иранская хакерская группа CyberAv3ngers объявила о взломе очистного сооружения сточных вод в городе Нетания, Израиль [1]. В своем телеграм-канале хакеры опубликовали скриншоты, на которых видно, что они получили доступ к системам управления и мониторинга КИИ завода, управляемых автоматизированными системами управления технологическими процессами (АСУ ТП). Указанные действия привели к возникновению угрозы нарушения работы очистных сооружений. Таким образом, была проведена целенаправленная кибератака на целую отрасль критической инфраструктуры государства.

Анализ тенденций[2,3] реализации кибератак с 2020 года показывает, что подходы к нарушению режима БИ ОКИИ и АСУ ТП существенно изменились. Если в 2020 году основными методами проникновения были использование внешних устройств (24 % от

[1] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=3&nd=102439340 (дата обращения: 22.03.2025).

[2] Экспертно-аналитический центр InfoWatch. Тенденции развития киберинцидентов АСУ ТП. Аналитический отчет за 2024 год. InfoWatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/tendentsii-razvitiya-iberintsidentov-asu-tp-za-dve-tysyachi-dvadtsat-chetyvertiy-god.pdf (дата обращения: 22.03.2025).

[3] Ландшафт угроз для систем промышленной автоматизации. Четвертый квартал 2024 – регионы. Kaspersky ICS CERT. URL: https://ics-cert.kaspersky.ru/publications/reports/2025/03/17/threat-landscape-for-industrial-automation-systems-regions-q4-2024/ (дата обращения: 24.03.2025).

общего количества киберинцидентов), фишинг (22 %) и компрометация устройств удаленного доступа (14 %), то к 2024 году структура угроз изменилась: Компрометация учетных данных – (20 %) Атаки на цепочки поставок (15 %). Использование устройств с доступом в интернет (13 %). Чаще всего нарушители получают доступ через автоматизированные рабочие места (30 % атак), SCADA-серверы (25 %) и программируемые логические контроллеры (ПЛК) (21 %). В 70 % случаев атаки сопровождаются заражением троянским ПО, предназначенным для вымогания денежных средств у организации – владельца АСУ ТП. Рост количества киберинцидентов (атак) к началу 2025 года это локальная (в пределах Российской Федерации) и глобальная динамика для всей мировой ИТ-индустрии. В течение последних двух лет число атак на отечественные АСУ ТП выросло на 160 %, в то время как в мире аналогичный показатель увеличился лишь на 17 %. Наибольшее количество атак фиксируется в следующих отраслях: машиностроение (38 % атак в России и 32 % в мире); транспорт (24 % в России и 28 % в мире); производственные предприятия и добыча (19 % и 22 %); энергетика (19 % и 18 % соответственно).

Общая динамика выявленных киберинцидентов ИБ на ОКИИ, эксплуатирующих АСУ ТП в период с 2018 по 2024 годы представлена на Рисунке 1.

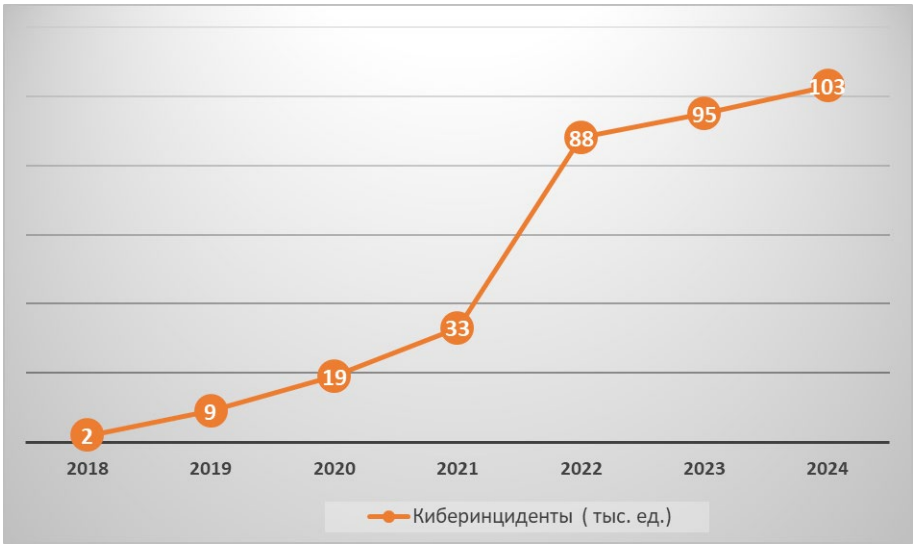

Рисунок 1 – Общая динамика выявленных инцидентов ИБ АСУ ТП
Figure 1 – General dynamics of identified information security incidents

Отмечается общая тенденция на повышение киберинцидентов именно в области промышленной автоматизации. В статье предлагается более подробно рассмотреть оценку опасности реализации угроз БИ для АСУ ТП ввиду их многоуровневой структуры.

Постановка задачи

Потенциал нарушителя ИБ – это совокупность возможностей, которыми обладает потенциальный злоумышленник для проведения атак на информационные системы организации. Потенциал включает в себя знания, опыт, ресурсы, инструменты и мотивацию нарушителя и определяется в следующих целях:

– Оценка рисков: Знание потенциала позволяет лучше оценить вероятность и возможные последствия реализации угроз ИБ. Чем больше ресурсов и знаний у нарушителя, тем большее количество угроз БИ он сможет реализовать в ИТ-инфраструктуре.

− Разработка мер защиты: Понимание уровня подготовки и мотивации нарушителей помогает разрабатывать адекватные меры защиты: от базовых антивирусных решений до сложных систем мониторинга и предотвращения вторжений.

− Планирование бюджета на безопасность: Оценка потенциала нарушителя помогает определить, сколько ресурсов нужно выделить на защиту информационных активов ИТ-инфраструктуры.

− Реагирование на инциденты: Если уже произошел инцидент, понимание потенциала нарушителя поможет быстрее локализовать проблему и минимизировать ущерб, наносимый потенциальным нарушителем БИ.

− Обучение персонала: Важно понимать, какие именно нарушители могут представлять угрозу, чтобы правильно организовать обучение сотрудников правилам БИ в ИТ-инфраструктуре.

Таким образом, определение потенциала нарушителя является важным этапом управления рисками в области ИБ.

Потенциал нарушителя позволяет оценить степень усилий, которые он прилагает для осуществления угроз ИБ. Однако указанная характеристика не отражает уровень опасности, связанной с реализацией угроз БИ в контексте конкретной АСУ ТП. Оценка опасности действий нарушителя, направленных на осуществление угроз БИ, будет варьироваться для разных систем, поскольку механизмы их реализации и применяемые меры по обеспечению БИ различаются.

Основные подходы и методики, используемые для указанной оценки, а также их сравнительная характеристика и отличительные особенности представлены в Таблице 1.

Таблица 1 – Сравнительная характеристика
Table 1 – Comparative characteristics

Методика	Отличительные особенности
Анализ рисков	Один из ключевых методов, который предполагает систематическое выявление, оценку и управление вероятностью возникновения угроз. В рамках анализа рисков предпринимаются действия по: идентификации возможных угроз; определению уязвимостей в информационных системах; анализу последствий, связанных с реализацией каждой угрозы БИ; оценке вероятности возникновения угроз; ранжированию угроз по степени критичности [2].
Методика FAIR (Factor Analysis of Information Risk)	Структурированный подход к оценке риска (опасности) реализации угроз, основанный на количественном анализе. Он рассматривает различные факторы, влияющие на риск, такие как частота событий, уровень потерь и возможности управления рисками. Методика позволяет оценить финансовые потери, которые могут возникнуть вследствие реализации угроз [3].
Октава (OCTAVE)	Методология оценки рисков, разработанная SEI (Software Engineering Institute). Фокусируется на трех основных этапах: выявление наиболее важных активов и угроз; оценка текущего состояния безопасности; разработка стратегий для минимизации рисков [4].
CVSS (Common Vulnerability Scoring System)	Используется для оценки степени критичности уязвимостей в информационных системах. Система присваивает каждому уязвимому месту рейтинг, который учитывает такие параметры, как сложность эксплуатации, влияние на конфиденциальность, целостность и доступность данных [5].

Таблица 1 (продолжение)
Table 1 (continued)

OWASP Top 10	Публикует список десяти наиболее распространенных уязвимостей веб-приложений. Организации используют этот перечень для выявления и устранения потенциальных проблем, связанных с безопасностью приложений и соответственно не могут удовлетворить потребностей в оценке опасности реализации угроз для АСУ ТП.
Тестирование на проникновение (Penetration Testing)	Этот метод подразумевает проведение симуляции атаки на информационную систему с целью выявления слабых мест. Специалисты в области ИБ имитируют действия реальных злоумышленников, чтобы проверить устойчивость системы к различным видам атак. Отсутствует единый алгоритм количественной оценки опасности реализации угроз БИ [6].
Модель STRIDE	Используется для классификации и моделирования угроз. Не позволяет количественно оценить опасность, исходящую от нарушителей ИБ, однако выделяет шесть типов актуальных угроз БИ: Spoofing Identity (подмена личности); Tampering with Data (манипуляция данными); Repudiation (отказ от ответственности); Information Disclosure (разглашение информации); Denial of Service (отказ в обслуживании); Elevation of Privilege (повышение привилегий) [7].
Сценарии нападений (Attack Trees) TRIKE	Методика построения деревьев атак помогает визуализировать и проанализировать возможные пути проникновения злоумышленника в систему. Каждый узел дерева представляет собой действие, которое ведет к компрометации системы. Также не позволяет количественно оценивать опасность реализации угроз [7].

Каждая из перечисленных в Таблице 1 методик имеет свои преимущества и недостатки, и выбор конкретного метода зависит от выполняемых технологических процессов в АСУ ТП, типа обрабатываемых данных и целей оценки опасности реализации угроз БИ.

Для количественной оценки опасности, исходящей от потенциального нарушителя, необходимо разработать метод, который учтет технические особенности АСУ ТП, их многоуровневую структуру, а также ущерб, который могут причинить деструктивные действия нарушителя в результате вывода из строя средств и мер защиты информации при реализации угроз БИ.

Материалы и методы

В основу разработанного метода положены нечеткие оценки защищенности ИС предложенные в [8].

Пусть возможные комбинации угроз БИ для некоторой АСУ ТП представлены множеством $H = \{h_1, h_2, h_3 \dots h_\tau\}$, где $h_i \in H$ – совокупность угроз, которая может быть реализована потенциальным нарушителем ИБ, с некоторой вероятностью. Следовательно, можно говорить о множестве вероятностей $P = \{P_{h_1}, P_{h_2}, P_{h_3} \dots P_{h_\tau}\}$, при этом справедливо $\sum P_{h_\tau} = 1$.

Величина ущерба от реализации угроз БИ представлена множеством $N_h = \{N_{h_1}, N_{h_2}, N_{h_3} \dots N_{h_\tau}\}$, при этом справедливо выражение: $0 \le N_{h_\tau} \le N_{max}$. По отношению к АСУ ТП могут быть реализованы наборы угроз множества $\tilde{H} = \{\tilde{H}_1 = H_1 \vee H_3, \tilde{H}_2 = H_2 \vee H_4, \tilde{H}_3 = H_1 \vee H_2 \vee H_i \dots \tilde{H}_\tau\}$ с вероятностями их реализации $\tilde{P} = \{\tilde{P}_1, \tilde{P}_2, \tilde{P}_3 \dots \tilde{P}_\tau\}$ при

выполнении условия $\sum_{i=1}^{\tau} \tilde{P}_i = 1$. В таком случае суммарный ущерб от реализации наборов угроз будет определяться на основании выражения:

$$\sum_{i=1}^{\tau} \widetilde{N}_i = N_{max}, \quad (1)$$

которое соответствует правилу:

$$\widetilde{N}_i = \frac{N_i}{N_{max}}. \quad (2)$$

Величина ущерба N_h не является постоянной величиной и отличается в зависимости от конкретных угроз из множества H, вероятности P возникновения указанных угроз БИ и выполняемых технологических процессов из множества $Q = \{q_1, q_2, q_3 \dots q_m\}$. Тогда общую величину ущерба от реализации всех угроз потенциальным нарушителем ИБ можно представить в виде функции:

$$N_{\sum} = f(H, P, Q). \quad (3)$$

Выражение (3) не учитывает характеристики выполняемых технологических процессов в системе и многоуровневую структуру АСУ ТП. Указанные характеристики предложено определять в рамках вычисления ущерба $N_{h_i}(k, t)$ от реализации каждой из множества угроз в момент времени *t* при их выполнении на каждом из k уровней системы в соответствии с функцией:

$$N_{\Sigma} = f(H, P, N_{h_i}(k, t)). \quad (4)$$

Пусть количественная оценка опасности реализации угроз БИ $0 \le L(t) \le 1$ будет зависеть от суммарной величины ущерба N_{Σ}, наносимого АСУ ТП в результате реализации множества угроз H. Тогда вероятность того, что угрозы БИ не будут реализованы в АСУ ТП, может быть определена как степень защищенности системы в соответствии с выражением:

$$\overline{P} = \prod_{i=1}^{\tau}(1 - P_{h_i}), 0 \le P_{h_i} \le 1. \quad (5)$$

В случае нанесения ущерба от реализации всех угроз N_{h_i}, при условии $0 \le N_{h_i} \le N_{max}$, АСУ ТП понесет суммарный ущерб, взвешенный с учетом вероятности:

$$N_{\sum} = \sum_{i=1}^{\tau} N_{h_i} P_{h_i}, 0 \le N_{\sum} \le N_{max}. \quad (6)$$

Таким образом, выражение (6) определяет уровень потенциального ущерба в случае невозможности выполнения технологического процесса, а уровень максимального возможного ущерба определяется как $N \sum N_{h_{i_{max}}}$ при суммарной вероятности $\sum P_{h_\tau} = 1$.

Количественная оценка опасности реализации угроз БИ нарушителями заключается в определении суммарного ущерба от реализации каждой угрозы в отношении технологических процессов в АСУ ТП. При этом суммарный ущерб определяется в условиях негативного воздействия на каждом из ее уровней угрозообразующих факторов, таких как критичность нарушения технологического процесса и критичность выполняемых технологических процессов для достижения целей эксплуатации АСУ ТП, которые, в наихудшем случае, приводят к максимальному возможному ущербу.

В работе [9] автором предложено определять ущерб от реализации конкретного деструктивного действия $N_{h_i}(t) < 1$ без учета уровней АСУ ТП на основе эвристических оценок пользователей системы в разные моменты времени. Указанный способ определения ущерба корректен для оценки реализации угроз БИ отдельных файлов в

памяти информационных систем и не применим для АСУ ТП, поскольку не учитывает следующих важных особенностей автоматизации технологических процессов, критичности и значимости выполняемых технологических процессов.

В предлагаемом методе ущерб $N_{h_i}(t)$ предложено вычислять на основе оценок критичности технологического процесса с учетом роли в общей организации производственного процесса в соответствии с выражением (7) на каждом из уровней АСУ ТП.

$$N_{h_i}(t) = \sum_{q=1}^{q} R_{kq}(t), \quad (7)$$

где $R_{kq}(t)$ – оценка критичности нарушения технологического процесса q потенциальным нарушителем ИБ на каждом из k-уровней АСУ ТП.

Оценку критичности нарушения технологического процесса предложено определять в соответствии с выражением (8), свойственным методике анализа видов и последствий потенциальных дефектов (Potential Failure Mode and Effects Analysis, FMEA) [10].

$$R_{kq}(t) = \prod_{n=1}^{3} O_{nq}(t), R_{kq} \in [0; 1]. \quad (8)$$

В подсистеме журналирования большинства современных SCADA – систем верхнего уровня АСУ ТП содержатся следующие значения необходимые для получения критичности нарушения технологического процесса $R_{kq}(t)$:

– $O_{1q}(t)$ – вероятность нарушения технологического процесса q, т. е. количество срабатывания типа «отказ в обслуживании» за рассматриваемый промежуток времени;

– $O_{2q}(t)$ – вероятность невыявления нарушения технологического процесса q до его появления, т. е. узел был недоступен, однако причина отказа не была выявлена;

– $O_{3q}(t)$ – вероятность прекращения технологического процесса q, т. е. общее количество итераций опроса оборудования, при которых за рассматриваемый промежуток времени узел АСУ ТП в сети был недоступен.

По результатам определения оценок критичности каждого из уровней АСУ ТП выбирается максимальное значение $R_{kq}(t)$. Получение указанной оценки не требует профильных знаний в области ИБП, поскольку расчетные данные для нее доступны по умолчанию оператору и администратору АСУ ТП.

Таким образом, выражение для определения оценки опасности реализации угроз БИ АСУ ТП принимает следующий вид:

$$L(t) = \frac{\sum_{i=1}^{\tau}([\prod_{n=1}^{3} O_{nq}(t)])P_{h_i}}{N_{max}}. \quad (9)$$

Количественная оценка опасности реализации угроз БИ, позволяет осуществить переход к минимизации рисков ИБ и проектированию адекватной системы защиты информации. К основным действиям для выполнения вышеуказанных мероприятий следует отнести:

– разработку и внедрение мер по снижению рисков, направленных на устранение или минимизацию угроз, выявленных в ходе оценки опасности их реализации. Это могут быть технические меры (например, обновление программного обеспечения, установка межсетевых экранов) и организационные (например, изменение политик безопасности);

– укрепление подсистемы контроля доступа АСУ ТП в части внедрения дополнительных механизмов контроля доступа к критически важной информации и узлам системы. В том числе внедрение систем контроля действий привилегированных пользователей и средств многофакторной аутентификации;

– внедрение средств мониторинга сетевой активности и аудита ИТ-инфраструктуры АСУ ТП, а также проведение регулярного аудита (пентест/тестирование на проникновение) систем безопасности для оценки их эффективности.

Данный перечень действий не является исчерпывающим, однако даже их выполнение поможет не только снизить количественные оценки опасности реализации угроз БИ потенциальными нарушителями, но и снизить общее количество актуальных угроз БИ в АСУ ТП в целом.

Результаты

В результате математического моделирования (Таблица 2) метода оценки опасности реализации 16 угроз БИ, представленных в БДУ ФСТЭК России (УБИ.003 – УБИ.018) для внешнего нарушителя, реализующего атаку на АСУ ТП, с высоким потенциалом были получены следующие ключевые результаты:

1. Оценка опасности реализации угроз потенциальным нарушителем: Моделирование показало, что наиболее опасными угрозами являются УБИ.004 (Угроза аппаратного сброса пароля BIOS) и УБИ.014 (Угроза длительного удержания вычислительных ресурсов пользователями), с оценкой опасности реализации 0,15 и 0,35 соответственно. Эти угрозы требуют особого внимания при разработке мер защиты.

2. Уровень ущерба: Наибольший уровень ущерба, согласно моделированию, был зафиксирован для угрозы УБИ.008 (Угроза восстановления и/или повторного использования аутентификационной информации), где уровень ущерба оценивался в 9 по 10-балльной шкале. Это подчеркивает необходимость усиления подсистемы аутентификации в целях минимизации негативных последствий от реализации актуальных угроз БИ, ассоциированных в том числе с утечкой ключевой информации. Однако указанные мероприятия не являются первоочередными ввиду низких показателей оценки вероятности возникновения указанной угрозы.

4. Рекомендации по снижению рисков: На основе полученных данных были разработаны рекомендации по снижению рисков, включая внедрение многоуровневой системы защиты, регулярное обновление программного обеспечения и обучение сотрудников по вопросам кибербезопасности.

Таблица 2 – Результаты математического моделирования
Table 2 – Results of mathematical modeling

№	h_i	P_{h_τ}	$N_{h_i}(t)$	$O_{1q}(t)$	$O_{2q}(t)$	$O_{3q}(t)$	$R_{kq}(t)$	$L_h(t)$
1	УБИ.003	0,3990	0,7255	0,6232	0,1323	0,4521	0,0373	0,0205
2	УБИ.004	0,0876	0,0903	0,6489	0,3262	0,7437	0,1574	0,1527
3	УБИ.005	0,0806	0,6864	0,2474	0,6914	0,9845	0,1684	0,0198
4	УБИ.006	0,0850	0,5921	0,5716	0,2645	0,7211	0,1090	0,0156
5	УБИ.007	0,7073	0,4397	0,1047	0,1335	0,2998	0,0042	0,0067
6	УБИ.008	0,1490	0,8741	0,4714	0,8762	0,6076	0,2510	0,0428
7	УБИ.009	0,0167	0,6894	0,3056	0,0201	0,7709	0,0047	0,0001
8	УБИ.010	0,0309	0,0899	0,0281	0,6936	0,4222	0,0082	0,0028
9	УБИ.011	0,0009	0,5414	0,8604	0,3456	0,8060	0,2397	0,0004
10	УБИ.012	0,0321	0,1528	0,3848	0,9489	0,2161	0,0789	0,0166
11	УБИ.013	0,0590	0,2732	0,9692	0,8413	0,2266	0,1848	0,0399
12	УБИ.014	0,5652	0,3307	0,2966	0,8703	0,7938	0,2049	0,3503
13	УБИ.015	0,0623	0,1669	0,4826	0,8401	0,6171	0,2502	0,0934

Таблица 2 (продолжение)
Table 2 (continued)

14	УБИ.016	0,0498	0,2588	0,1390	0,7776	0,5135	0,0555	0,0107
15	УБИ.017	0,9307	0,2033	0,0341	0,5521	0,2177	0,0041	0,0188
16	УБИ.018	0,0734	0,3107	0,3768	0,0225	0,5766	0,0049	0,0012
Общая оценка опасности реализации угроз БИ АСУ ТП $L(t)$								**0,7923**

На Рисунке 2 представлены полученные данные зависимости оценки опасности реализации (УБИ.003 – УБИ.018) для внешнего нарушителя с высоким потенциалом от вероятности возникновения указанных угроз и уровня ущерба, полученных в результате математического моделирования реализации разработанного метода.

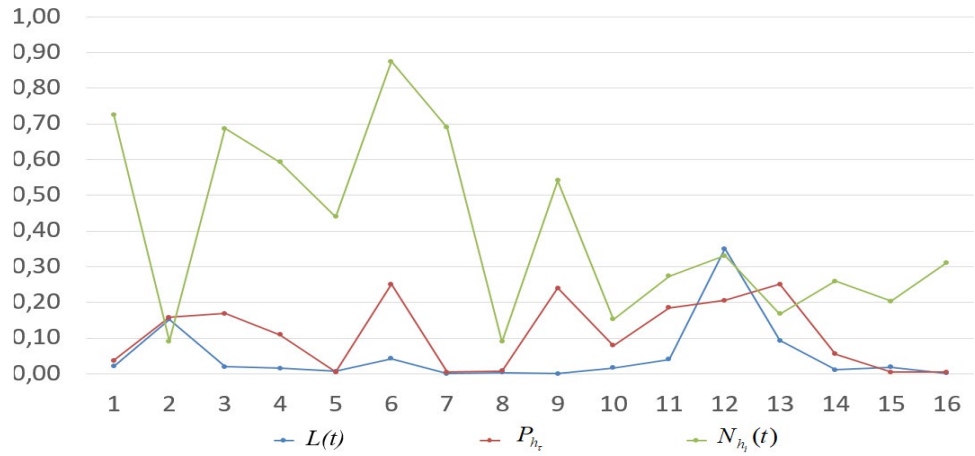

Рисунок 2 – Зависимость оценки опасности реализации угроз БИ $L(t)$
Figure 2 – Dependence of the assessment of the danger of the implementation of threats $L(t)$

Результаты математического моделирования разработанного метода подчеркивают важность комплексного подхода к оценке опасности действий нарушителей даже в тех случаях, когда известны расчетные показатели их потенциалов, поскольку опасность действий нарушителей определяется не только его потенциалом, но и условиями функционирования самого объекта КИИ – АСУ ТП. А поскольку указанные объекты обладают многоуровневой структурой, то и оценки опасности реализации угроз БИ потенциальным нарушителем будут отличаться в зависимости от рассматриваемого уровня АСУ ТП. Результаты указывают на возможность применения разработанного метода для информационных систем и информационно-телекоммуникационных сетей, также относящихся к ОКИИ.

Заключение

Предложен метод количественной оценки опасности реализации угроз БИ ОКИИ. В отличие от существующих методов, предложенный метод имеет в основе оценку вероятностей реализации угроз БИ и ущерба от их реализации. Метод позволяет оценить опасность реализации угроз БИ потенциальным нарушителем по отношению к конкретной рассматриваемой системы, а также позволяет значительно снизить участие экспертов в процессе оценки. Разработанный метод не требует от экспертов профильных знаний в области ИБ, ввиду формирования оценок в отношении технологических процессов, выполняемых АСУ ТП или для ОКИИ в целом. Полученные результаты открывают новые направления для дальнейших исследований, включая более детальное

моделирование воздействия различных факторов на вероятность возникновения угроз и уровень ущерба.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Павлихина А.Н. Простое решение для сложных инфраструктур От чего и как защищать предприятия нефтегазового сектора России? *Деловой журнал Neftegaz.RU*. 2024;(8):20–25.
2. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии. *Современные научные исследования и инновации*. 2020;(1). URL: https://web.snauka.ru/issues/2020/01/90380
3. Одаховская Д.А., Пятков С.В., Черных М.А. Информационные риски: анализ и расчеты. *Прикладные экономические исследования.* 2024;(2):242–247.
   Odakhovskaya D.A., Pyatkov S.V., Chernykh M.A. Information Risk: Analysis and Calculations. *The Applied Economic Researches Journal.* 2024;(2):242–247. (In Russ.).
4. Chernov D., Sychugov A., Sovgir A. Applying a System of Automatic Threat Modeling for APCs at Information Infrastructure Facilities. In: *Advances in Automation IV: Proceedings of the International Russian Automation Conference, RusAutoCon2022, 04–10 September 2022, Sochi, Russia.* Cham: Springer; 2023. P. 374–385. https://doi.org/10.1007/978-3-031-22311-2_36
5. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик CVSS. *Информационно-управляющие системы*. 2017;(6):76–87. https://doi.org/10.15217/issn1684-8853.2017.6.76
   Doynikova E.V., Chechulin A.A., Kotenko I.V. Computer Network Security Evaluation Based on CVSS Metrics. *Information and Control Systems*. 2017;(6):76–87. (In Russ.). https://doi.org/10.15217/issn1684-8853.2017.6.76
6. Макаренко С.И. Тестирование на проникновение на основе стандарта NIST SP 800–115. *Вопросы кибербезопасности*. 2022;(3):44–57.
   Makarenko S. Penetration Testing in Accordance with NIST SP 800–115 Standard. *Voprosy kiberbezopasnosti.* 2022;(3):44–57. (In Russ.).
7. Чернов Д.В. Методики оценки угроз безопасности информации автоматизированных систем управления технологическими процессами. *Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки.* 2021;(9):81–87. https://doi.org/10.37882/2223-2966.2021.09.25
   Chernov D.V. Methods for Assessing Information Security Threats of Automated Process Control Systems. *Modern Science: Actual Problems of Theory and Practice. Series: Natural and Technical Sciences.* 2021;(9):81–87. (In Russ.). https://doi.org/10.37882/2223-2966.2021.09.25
8. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии. *Вопросы кибербезопасности*. 2022;(6):71–82.
   Kostogryzov A. On Models and Methods of Probabilistic Analysis of Information Security in Standardized Processes of System Engineering. *Voprosy kiberbezopasnosti.* 2022;(6):71–82. (In Russ.).
9. Суханов А.В. Нечеткие оценки защищенности информационных систем. *Информация и космос*. 2013;(1):107–110.
   Suhanov A.V. Fuzzy Assessment of Information System Security. *Information and Space.* 2013;(1):107–110. (In Russ.).

10. Babeshko E., Kharchenko V., Gorbenko A. Applying F(I)MEA-technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring. In: *2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, 26–28 June 2008, Szklarska Poreba, Poland.* IEEE; 2008. P. 309–315. https://doi.org/10.1109/DepCoS-RELCOMEX.2008.233

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Чернов Денис Владимирович, старший преподаватель кафедры информационной безопасности Тульского государственного университета, начальник сектора информационной безопасности АО «Центральное конструкторское бюро аппаратостроения», Тула, Российская Федерация.
e-mail: cherncib@gmail.com
ORCID: 0000-0002-7223-8670

Denis V. Chernov, Senior Lecturer at the Department of Information Security, Tula State University, Head of the Information Security Sector of JSC "Central Design Bureau of Apparatus Engineering", Tula, the Russian Federation.

Статья поступила в редакцию 25.03.2025; одобрена после рецензирования 14.04.2025; принята к публикации 24.04.2025.

The article was submitted 25.03.2025; approved after reviewing 14.04.2025; accepted for publication 24.04.2025.