НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2025 Том 25 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
Jule–August 2025 Vol. 25 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2025-25-4-727-736
УДК 004.094

Применение современных методов оценивания рисков информационной безопасности объекта критической информационной инфраструктуры

Илья Иосифович Лившиц✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Livshitz.il@yandex.ru✉, https://orcid.org/0000-0003-0651-8591

Аннотация
Рассмотрена практика оценивания рисков информационной безопасности объектов критической информационной инфраструктуры. Выполнено сравнение методов анализа дерева событий, дерева отказов и международного стандарта ISO/IEC 27005:2022, устанавливающего принципы управления рисками. Показаны пути дополнения существующих методических требований Российской Федерации в области безопасности объектов критической информационной инфраструктуры современными методами оценивания рисков информационной безопасности. Выполнено сопоставление современных методов оценивания рисков информационной безопасности на примере системы управления водоснабжением. Обосновано применение необходимого перечня мер защиты, обеспечивающих заданный уровень остаточных рисков информационной безопасности. Продемонстрирована возможность применения современных методов оценивания рисков информационной безопасности объектов критической инфраструктуры в дополнение к существующим методическим требованиям Российской Федерации.

Ключевые слова
критическая инфраструктура, объекты критической информационной инфраструктуры, информационная безопасность, стандарт, риск, оценивание рисков, меры защиты, остаточный риск

Ссылка для цитирования: Лившиц И.И. Применение современных методов оценивания рисков информационной безопасности объекта критической информационной инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 4. С. 727–736. doi: 10.17586/2226-1494-2025-25-4-727-736

Application of modern methods for information security risks evaluation of a critical information infrastructure facility

Ilya I. Livshitz✉

ITMO University, Saint Petersburg, 197101, Russian Federation
Livshitz.il@yandex.ru✉, https://orcid.org/0000-0003-0651-8591

Abstract
The practice of assessing IT-security risks of Critical Information Infrastructure (CII) facilities is considered. The methods of Event Tree Analysis (ETA), Fault Tree Analysis (FTA), and the International Standard ISO/IEC 27005:2022, which establishes the principles of risk management, were compared. The ways of supplementing the existing methodological requirements of the Russian Federation in the field of IT-security of CII facilities with modern methods of assessing IT-security risks are shown. A comparison of modern methods for assessing IT-security risks is carried out using the example of a water supply management system. The application of the necessary list of protection measures providing a given level of residual IT-security risks is justified. The possibility of using modern methods for assessing the IT-security risks of CII facilities in addition to the existing methodological requirements of the Russian Federation is demonstrated.

Keywords
critical infrastructure, critical information infrastructure facilities, information security, standard, risk, risk assessment, protection measures, residual risk

For citation: Livshitz I.I. Application of modern methods for information security risks evaluation of a critical information infrastructure facility. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 4, pp. 727–736 (in Russian). doi: 10.17586/2226-1494-2025-25-4-727-736

Введение

Проблема обеспечения безопасности объектов критической информационной инфраструктуры (КИИ) не является новой. В Российской Федерации известны требования, разработанные различными регуляторами (Приказ ФСТЭК № 235[1], Приказ ФСТЭК № 239[2] и другие). Однако в актуальной нормативной базе практически не рассмотрен полный цикл управления рисками, в частности в «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России 5 февраля 2021 г. (п. 2.3, ж, п. 2.7, а; п. 3.2, д), указано неоднозначное и сложно определенное «замещение» термина «ущерб» термином «риск». При этом практики оценивания результативности мер защиты и расчета остаточных рисков в полном замкнутом цикле не приведено. В методическом документе «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[3], утвержденном ФСТЭК России 2 мая 2024 г., приведен перечень частных показателей безопасности, их наименования и максимальные значения, но только применительно к обеспечению безопасности объектов КИИ от актуальных угроз безопасности информации (УБИ). К сожалению, в рассматриваемом документе риски (остаточные риски) не рассматриваются.

Объективно наблюдается неполнота оценки безопасности объектов КИИ из-за пропуска этапа оценивания рисков после определения актуальных УБИ и перехода сразу к выбору средств защиты. Представляется целесообразным повысить точность и скорость оценивания актуального уровня информационной безопасности объектов КИИ за счет дополнения существующих методических требований подходящими методами оценки рисков.

Анализ известных методов менеджмента рисков

В современной научной литературе приведено достаточно примеров применения современных национальных и международных стандартов менеджмента рисков на практике, в том числе и для защиты объектов КИИ. Например, известны работы в области строительства [1, 2], судостроения [3], анализа геологических данных для предупреждения катастроф [4], в ядерной отрасли [5], на железнодорожном транспорте [6]. Помимо общего [7] и специального отраслевого анализа [8], известны публикации по оценке рисков применительно к области обеспечения информационной безопасности (ИБ), в частности, описан инцидент с атакой SolarWind [9]. В отечественной научной практике [2, 7, 10, 11], а также в зарубежных публикациях [4–6, 12, 13] рассматриваются различные аспекты применения современных стандартов управления рисками. Крайне важно, что в указанных публикациях предоставляется именно «инженерный» уровень применения множества методов управления рисками (например, в IEC 31010:2019[4] их более 40), а не обобщенные «наукообразные» конструкции [14, 15].

Для оценивания рисков ИБ на объектах КИИ рассмотрим кратко доступную статистику по причинам, источникам и факторам появления таких рисков. Например, в обзоре российской компании «СёрчИнформ»[5] представлены данные за 2024 г., структурированные по нескольким аналитическим разрезам, что будет далее востребовано при оценивании рисков ИБ. В частности, в указанном обзоре предоставляются данные по статистике утечки данных сотрудниками (рис. 1) и, как можно видеть, доля компаний, которые сталкивались с утечками («сливом») в течение последних двух лет, примерно одинаковая.

Соответственно, при анализе данного риска могут быть приняты во внимание как объем финансирования

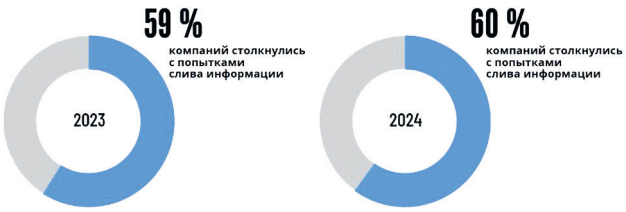

Рис. 1. Статистика утечки данных по вине сотрудников[6]

Fig. 1. Statistics on data leaks caused by employees

[1] [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235?ysclid=m7ltp57ouk63751815 (дата обращения: 03.06.2025).

[2] [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239?ysclid=m7ltpaukr2631376170 (дата обращения: 03.06.2025).

[3] [Электронный ресурс]. Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g?ysclid=m832n4zdm5637837561 (дата обращения: 03.06.2025).

[4] [Электронный ресурс]. Режим доступа: IEC 31010:2019. Risk management – Risk assessment techniques (https://www.iso.org/standard/72140.html) (дата обращения: 03.06.2025).

[5] [Электронный ресурс]. Режим доступа: https://searchinform.ru/news/company-news/2024/11/22/a-study-of-the-level-of-information-security-in-moscow-companies-in-2024/?utm_source=seclab&utm_medium=media_p&utm_campaign=post_survey_msk&utm_content=polza (дата обращения: 03.06.2025).

[6] [Электронный ресурс]. Режим доступа: https://searchinform.ru/news/company-news/2024/11/22/a-study-of-the-level-of-information-security-in-moscow-companies-in-2024/?utm_source=seclab&utm_medium=media_p&utm_campaign=post_survey_msk&utm_content=polza (дата обращения: 03.06.2025).

мер защиты (в частности, Data Loss Prevention решений), так и их результативность. Доступна статистика категорий вины сотрудников при утечке информации (рис. 2).

Оценка «чистой» умышленной утечки — 21 % (отдельная категория), но если учесть еще 1/2 по категории «Одинаково часто» (38 %), то общая статистика злого умысла достигнет уже 40 %, что объективно приводит к необходимости переоценки всей системы безопасности на объектах КИИ — комплекса как организационных, так и технических мер. В этом аналитическом аспекте представляется уместным сопоставить действующую методическую базу и стандарты управления рисками, которые предусматривают периодическую оценку рисков, результативности мер защиты и пересмотр остаточных рисков [16, 17].

В дополнение к отчету компании «СёрчИнформ» рассмотрим зарубежный отчет[1], который показывает «классическую» для стандартов ISO прослеживаемость «от актива» (рис. 3).

Ценность данного примера заключается в удельных значениях, присвоенных каждой категории («Актив», «Действия», «Нарушители»). Весьма важно сопоставление различных отчетов (национального и зарубежного), в частности, точность определения категорий «внутренние нарушители», «внешние нарушители», «партнеры» и «прочие».

Также следует отметить полезное детальное распределение по видам действий, что в целом соответствует стандарту ISO/IEC 27005:2022[2] и может быть практически применимо при оценивании рисков для объектов КИИ (например, воздействия партнеров на окружение и/или физическое состояние). Несмотря на

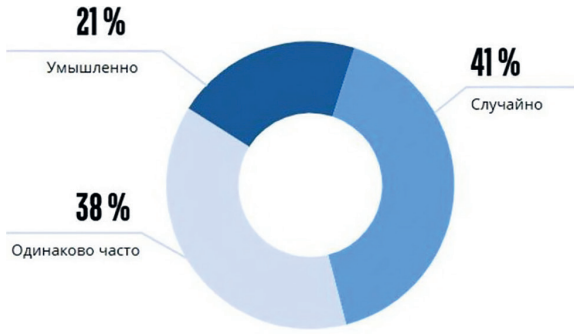

Рис. 2. Статистика категорий вины сотрудников при утечках[3]

Fig. 2. Statistics on employee guilt categories in leaks

минимальные уровни статистического воздействия (по 1 % каждый) именно такие атаки, как показала мировая практика крупнейших вторжений (например, Schneider Electric[4], Colonian Pipeline[5]), приводят к существенному ущербу.

Среди новаций в области управления рисками ИБ представляется возможным отметить два интересных практических предложения.

В Великобритании предложена классификация киберинцидентов по аналогии с природными катастрофами. Классификация[6] будет строиться на двух основных критериях: число «затронутых» инцидентом организаций и финансовые убытки, превышающие 1.000 фунтов стерлингов. Ключевые факторы анализа включают время простоя бизнеса, стоимость восстановления данных, расходы на реагирование и прочее. Тем не менее, штрафы, компенсации и иные платежи не учитываются при базовой оценке.

В Европейском союзе[7] вступил в силу первый этап регулирования искусственного интеллекта (ИИ), соответственно, со 2 февраля 2025 г. запрещены системы, которые несут «неприемлемый риск». К «неприемлемому риску» относят, в частности, реализацию уязвимостей для работников, социальный скоринг для частных (публичных) целей, индивидуальную предиктивную аналитику на базе профилирования сотрудников, биометрическое категорирование на базе национальности, членства в профсоюзах, политической приверженности, религии и прочее.

Весьма примечательно, что в области ИИ Еврокомиссия предполагает введение специальных мер стандартизации, которые должны обеспечить гармонизацию ряда стандартов (в частности, CEN и CENELEC[8]). В целом, эта практика известна, как для стандартов семейства ISO, так и для иных методических документов, например Cobit [8, 18]. Предполагается, что после публикации новых стандартов в официальном издании Official Journal будет введена «презумпция соответствия» всех разрабатываемых ИИ-систем установленным требованиям.

Примеры анализа ИБ объектов КИИ различными методами

Для оценивания рисков ИБ для конкретного объекта КИИ применены три количественных метода:

— метод анализа дерева событий (Event Tree Analysis, ETA) по требованиям IEC 31010:2019;

[1] [Электронный ресурс]. Режим доступа: https://www.orangecyberdefense.com/global/security-navigator (дата обращения: 03.06.2025).

[2] [Электронный ресурс]. Режим доступа: https://www.iso.org/standard/80585.html (дата обращения: 03.06.2025).

[3] [Электронный ресурс]. Режим доступа: https://searchinform.ru/news/company-news/2024/11/22/a-study-of-the-level-of-information-security-in-moscow-companies-in-2024/?utm_source=seclab&utm_medium=media_p&utm_campaign=post_survey_msk&utm_content=polza (дата обращения: 03.06.2025).

[4] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/549300.php (дата обращения: 03.06.2025).

[5] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/520905.php (дата обращения: 03.06.2025).

[6] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/556206.php (дата обращения: 03.06.2025).

[7] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/556096.php?ysclid=m6uivplqj9626198927 (дата обращения: 03.06.2025).

[8] [Электронный ресурс]. Режим доступа: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1683?utm_source=se%D1%81uritylabru (дата обращения: 03.06.2025).

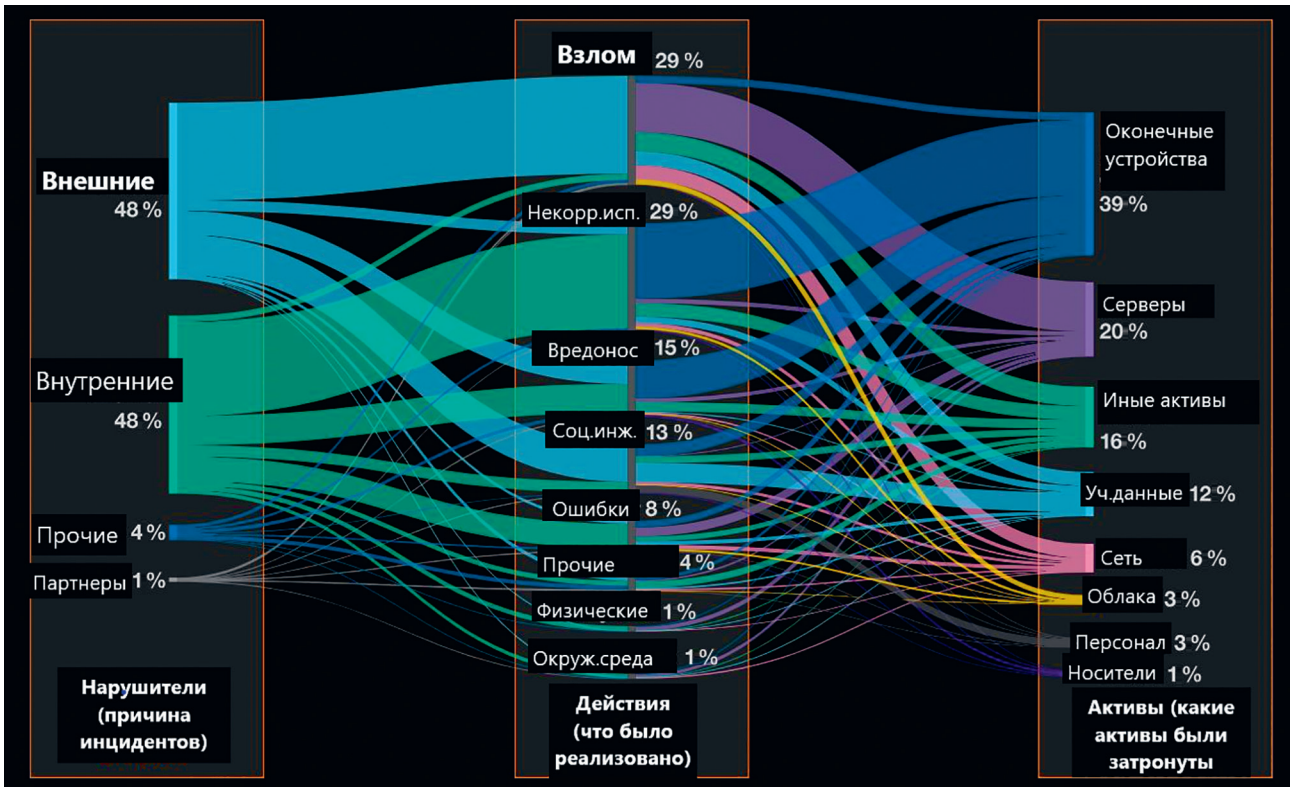

Рис. 3. Статистика по злоумышленникам, действиям и затронутым активам[1]

Fig. 3. Statistics on intruders, actions, and affected assets

— метод анализа дерева отказов (Fault Tree Analysis, FTA) по требованиям IEC 31010:2019;
— метод оценивания рисков по требованиям ISO/IEC 27005:2022.

Кратко поясним выбор именно этих методов для решения поставленной практической задачи оценивания рисков ИБ для конкретного объекта КИИ.

Существующие численные методы (например, марковский анализ, метод Монте-Карло), оперирующие с количественными оценками риска (стандарт IEC 31010:2019), больше ориентированы на оценивание вероятностей, требуют существенно больших затрат на экспертизу и обработку.

Предложенные в настоящей работе методы обеспечивают возможность получения количественных оценок рисков ИБ. Однако такие оценки удобно сопоставлять с размером потенциального ущерба, бюджетом на средства обеспечения безопасности и критериями принятия (обработки) рисков ИБ. Такие методы гарантируют воспроизводимость и повторяемость результатов процесса, что крайне важно для выполнения тестирования собственной командой экспертов ИБ и сопоставления с численными результатами внешнего тестирования.

Рассмотрим задачу сравнения нескольких методов оценивания рисков ИБ системы управления водоснабжением промышленного предприятия, реализованного на базе промышленного логического контроллера (ПЛК). Проблема безопасности систем управления водоснабжением как объекта КИИ признана актуальной[1]. Подобные объекты, как правило, характеризуются высокой сложностью (например, свыше 512 параметров на один технологический блок)[2].

На публичных ресурсах отечественных разработчиков ПЛК (например, DevLink-C1000[3] НПФ «Круг» или АР-8[4] ООО «НПО «Каскад-ГРУП») приведена техническая информация, однако данных о надежности (наработке на отказ), уровне рисков (уровне полноты безопасности или Safety Integrity Level (SIL)) не приведено. Частично указаны отдельные параметры (например, для Программно-технического комплекса «Торнадо-N»[5] приведена наработка на отказ 150 тыс. часов) или представлена информация о ранее выпол-

[1] [Электронный ресурс]. Режим доступа: https://www.orangecyberdefense.com/global/security-navigator (дата обращения: 03.06.2025).

[1] [Электронный ресурс]. Режим доступа: https://xn--90acqjv.xn--p1ai/wp-content/uploads/2019/03/SHipulin.pdf?ysclid=m7vvbwa9pf47435902 (дата обращения: 03.06.2025).

[2] [Электронный ресурс]. Режим доступа: https://nvtsys.ru/statiya/_06/TEC8_Sargon.pdf (дата обращения: 03.06.2025).

[3] [Электронный ресурс]. Режим доступа: https://www.krug2000.ru/products/ptc/promyshlennye-kontrollery/1331.html (дата обращения: 03.06.2025).

[4] [Электронный ресурс]. Режим доступа: https://kaskad-asu.com/files/controllers/ap-8/re-ap-8.pdf (дата обращения: 03.06.2025).

[5] [Электронный ресурс]. Режим доступа: https://tornado.nsk.ru/integratoram/product_integrator/ptk/ptk-tornado-n/ (дата обращения: 03.06.2025).

ненных проектах на базе иностранных ПЛК[1] (указан только SIL 2). Отметим, что SIL 2 соответствует целевой мере отказов (риску для объекта КИИ) в диапазоне от 10^{-3} до 10^{-2} по IEC серии 61508[2].

Решение практической задачи для конкретного объекта КИИ предлагается обеспечить на базе «общего» стандарта управления рисками ISO 31000:2018[3] и «специального» стандарта IEC 31010:2019[4]. Дополнительные методы расчета SIL для объектов КИИ в настоящей работе не рассматриваются. Подробно методика анализа рисков и формулы расчетов приведены в IEC серии 61508, некоторые примеры расчета приведены в работе [11]. Международные стандарты ISO (IEC) обладают существенной новизной по сравнению с национальными стандартами системы ГОСТ Р в Российской Федерации.

Оценивание рисков для объекта КИИ по методу ETA. В соответствии с описанием метода (п. B.5.6 стандарта IEC 31010:2019) формируется последовательно «инициируемое событие». Далее на основании статистических данных определяются численные значения вероятностей различных исходов с учетом оценки результативности известных мер защиты («контролей»). Результаты оценивания по методу ETA представлены на рис. 4.

Важным преимуществом метода ETA для решения поставленной задачи является как оценивание «сработки» встроенной системы безопасности (например, на базе оценок SIL по IEC серии 61508), зависимость финального состояния объекта КИИ от значения результативности предшествующих рубежей защиты, так и вероятности перехода объекта КИИ в безопасное состояние. Некоторые особенности расчета SIL применительно к объектам КИИ изложены в работе [15]. Для рассматриваемого примера по методу ETA риск для объекта КИИ составляет 0,0115, т. е. находится в интервале 10^{-3}–10^{-2}, что соответствует уровню SIL 2.

Оценивание рисков для объекта КИИ по методу FTA. В соответствии с описанием метода (п. B.5.7 стандарта IEC 31010:2019) определим последовательно нежелательное «топовое» событие. Далее с помощью булевых логических элементов получим зависимости факторов (типов нарушителей, типов атак и прочее), влияющие на основное «топовое» событие. Результаты оценивания по методу FTA показаны на рис. 5. Важным преимуществом метода FTA для решения поставленной задачи является определение как явных (основных) путей реализации нежелательного «топового события», так и иных путей, которые по строгим логическим правилам (в примере на рис. 5 рассмотрены для компактности только логические элементы «или») могут привести к недопустимому инциденту. В соответствии с рекомендациями стандарта IEC 31010:2019 учтена возможность ретроспективного анализа (например, передача выявленных инцидентов для последующего анализа в специальных системах класса Security Information and Event Management (SIEM)). Некоторые особенности анализа инцидентов ИБ применительно к объектам КИИ изложены в работах [12, 13, 16].

[1] [Электронный ресурс]. Режим доступа: https://kaskad-asu.com/press-center/newsfeed/modernizirovannaya-spaz-gd-ooo-hevel-vvedena-v-ekspluatatsiyu.html (дата обращения: 03.06.2025).

[2] [Электронный ресурс]. Режим доступа: https://webstore.iec.ch/en/publication/5515 (дата обращения: 03.06.2025).

[3] [Электронный ресурс]. Режим доступа: ISO 31000:2018. Risk management – Guidelines (https://www.iso.org/standard/65694.html) (дата обращения: 03.06.2025).

[4] [Электронный ресурс]. Режим доступа: IEC 31010:2019. Risk management – Risk assessment techniques (https://www.iso.org/standard/72140.html) (дата обращения: 03.06.2025).

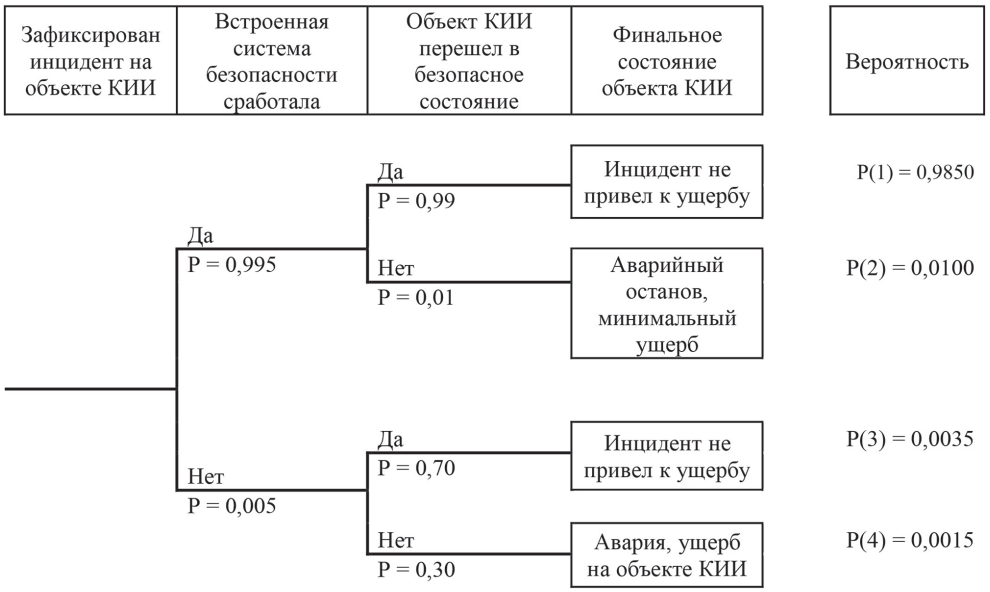

Рис. 4. Пример оценивания рисков для выбранного объекта критической инфраструктуры по методу ETA. P(1)…P(4) — вероятности событий 1…4

Fig. 4. An example of risk assessment for a selected CII facility using the ETA method

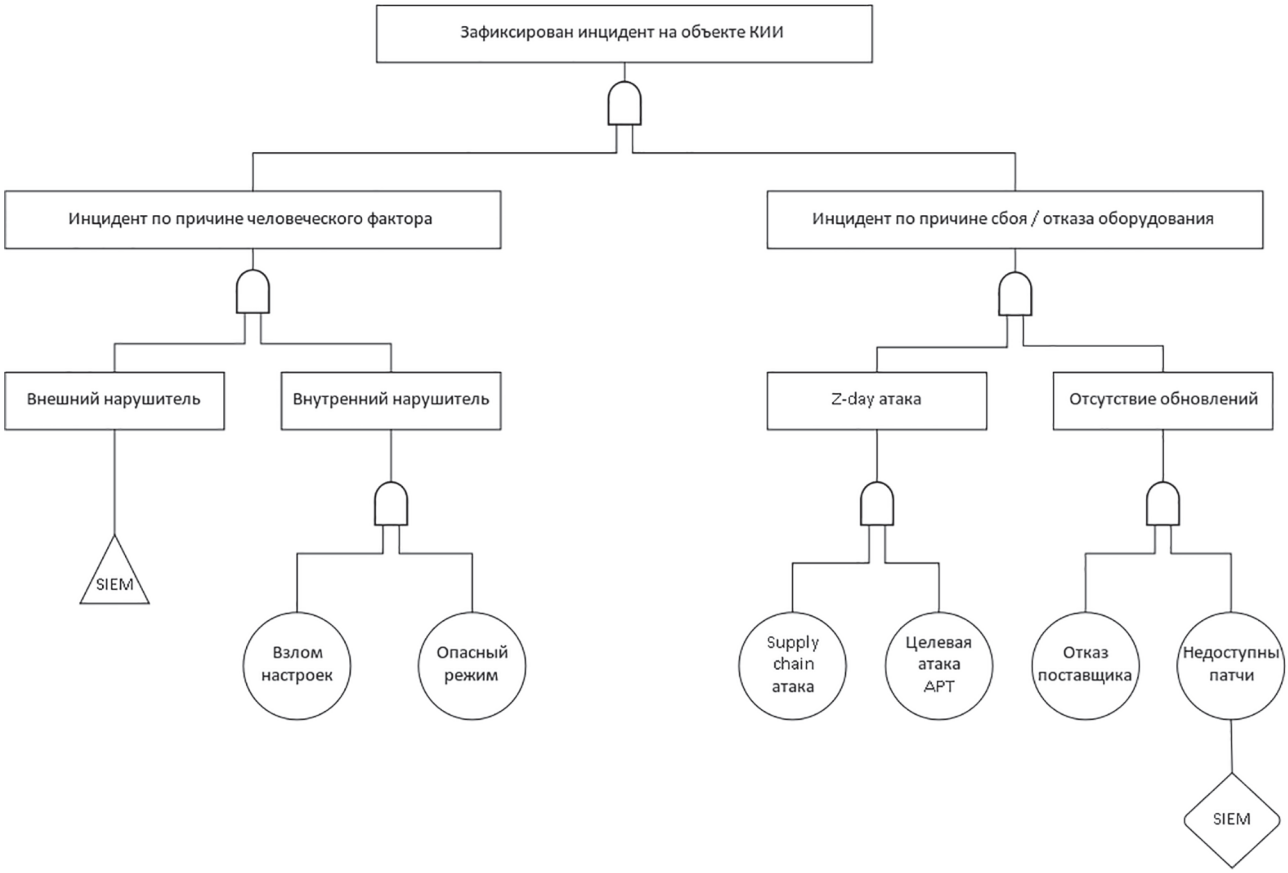

Рис. 5. Пример оценивания рисков для выбранного объекта критической инфраструктуры по методу FTA.
ATP — Advanced Persistent Threat, целевая атака; Z-day — атака «нулевого дня»

Fig. 5. An example of risk assessment for a selected CII facility using the FTA method

С учетом статистики отказов ПЛК (например: DDoS-атаки[1], атаки на встроенное программное обеспечение ПЛК[2], удаленное изменение настроек (9,8 CVSS[3]), обход защиты памяти (9,8 CVSS[4]), атаки серверов SCADA[5] и прочее) для данного примера риск успешной атаки на объект КИИ (при этом встроенная система безопасности не сработала) находится в интервале 10^{-3}–10^{-2}, что соответствует уровню SIL 2.

Пример оценивания рисков для объекта КИИ по методу ISO/IEC 27005:2022. В соответствии с данным стандартом определяется последовательно перечень активов, присущие им уязвимости, актуальные УБИ, реализуемые риски ИБ, встроенные меры защиты и остаточные риски ИБ. Результаты представлены в табл. 1. Примеры уязвимостей и УБИ приведены в ISO/IEC 27005:2022 (табл. A.10 и A.11), перечень мер защиты — в ISO/IEC 27001:2022 (табл. A.1).

В качестве критериев приемлемости риска и принятия остаточного риска в методе ISO/IEC 27005:2022 применяется интервальное значение риска 10^{-3}–10^{-2}, что эквивалентно уровню SIL 2. Остаточный риск принимается менее 10^{-2}, что эквивалентно уровню SIL 1. Это критериальное значение может быть независимо верифицировано по данным производителя, а в случае отсутствия полных данных — подтверждено по данным независимых испытаний или расчетов по известным формулам (например, IEC серии 61508).

Сопоставление методов оценивания рисков ИБ для объектов КИИ. На основании требований стандартов IEC 31010:2019 (соответственно, ETA и FTA) и ISO/IEC 27005:2022, а также практических результатов работ [10, 15, 16], сопоставление методов оценивания рисков ИБ для конкретного объекта КИИ представлено в табл. 2.

[1] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/498862.php (дата обращения: 03.06.2025).
[2] [Электронный ресурс]. Режим доступа: https://www.ndss-symposium.org/wp-content/uploads/2024-49-paper.pdf?utm_source=se%D1%81uritylabru (дата обращения: 03.06.2025).
[3] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/499700.php (дата обращения: 03.06.2025).
[4] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/520675.php (дата обращения: 03.06.2025).
[5] [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/538973.php ((дата обращения: 03.06.2025).

Таблица 1. Пример оценивания рисков ИБ для выбранного объекта КИИ по методу ISO/IEC 27005:2022
Table 1. An example of risk assessment for a selected CII facility using the ISO/IEC 27005:2022 method

Актив в составе объекта КИИ	Базовые меры защиты	Уязвимости	УБИ	Риск	Уровень риска (SIL)	Критерий приемлемости риска	Решение о принятии риска	Дополнительные меры защиты	Значение остаточного риска (SIL)	Подтверждение принятия остаточного риска
Встроенное ПО ПЛК	A.5.18	Хорошо известные недостатки в ПО	Злоупотребление правами или разрешениями	Отказ ПЛК	Высокий (SIL 2)	Средний (SIL 1)	Обработка	A.5.21	Средний (SIL 1)	Принятие
	A.8.4	Слабый менеджмент паролей						A.5.22		
Электропривод насосов	A.5.29	Недостаточное техническое обслуживание	Неисправность устройства или системы	Отказ водоснабжения	Низкий (SIL 1)	Средний (SIL 1)	Принятие	—	—	—
	A.8.9	Недостаточный контроль за изменением конфигураций								
Персонал (предприятие)	A.5.3	Недостаточный тренинг в области безопасности	Социальный инжиниринг	Недопустимое воздействие	Средний (SIL 1)	Средний (SIL 1)	Принятие	—	—	—
	A.5.20	Недостаточная осведомленность в области безопасности								
Персонала (подрядчик)	A.5.19	Недостаточность или отсутствие механизмов мониторинга	Несанкционированный доступ на объекты	Недопустимое воздействие	Высокий (SIL 2)	Средний (SIL 1)	Обработка	A.5.30	Средний (SIL 1)	Принятие
	A.8.4	Неправильное использование программного и аппаратного обеспечения						A.5.35		
Помещение системы управления водоснабжения	A.7.3	Неадекватное техническое обслуживание	Значительная авария	Отказ водоснабжения	Низкий (SIL 1)	Средний (SIL 1)	Принятие	—	—	—
Помещение насосной станции	A.7.3	Неадекватное техническое обслуживание	Значительная авария	Отказ водоснабжения	Низкий (SIL 1)	Средний (SIL 1)	Принятие	—	—	—
Репутация	A.5.31	Процедуры сообщения об уязвимостях в системе безопасности не разработаны или их внедрение неэффективно	Нарушение законов или нормативных актов	Санкции, штрафы, проверки	Низкий (SIL 1)	Средний (SIL 1)	Принятие	—	—	—

Таблица 2. Сопоставление методов оценивания рисков

Table 2. Comparison of risk assessment methods

Метод	Описание	Преимущества	Недостатки	Воспроизводимость / повторяемость	Практическая применимость
ETA (IEC 31010:2019)	Модель основана на возможных исходах на основе входных событий и статусов мер защиты, которые анализируются по вероятностям и частотам	— Отображает влияние неэффективных мер контроля в виде диаграммы; — выявляет потенциальные сбои, уязвимости и меры защиты с низкой неэффективностью; — учитывает временные рамки и «эффект домино»	— Для проведения полного анализа необходимо определить все возможные исходные события; — обрабатываются только состояния успешной работы и сбоя системы, и трудно учесть частично работающие элементы (меры защиты)	— Обеспечивается другой командой — собственных экспертов или внешних аудитов; — дополнительно возможно сопоставление с данными производителя (SIL), полученными на стенде	— Для категорирования объектов КИИ; — для аудитов ИБ; — для аудитов функциональной безопасности (SIL)
FTA (IEC 31010:2019)	Модель основана на анализе вариантов с использованием булевой логики для описания комбинаций отказов. Варианты включает дерево успеха с приоритетными событиями и дерево причин, применяемое для расследования событий	— Отличается высокой степенью системности, позволяет анализировать множество факторов; — логический анализ деревьев отказов полезен при выявлении путей выхода из строя компонентов в сложной системе	— Метод оперирует только с бинарными состояниями; — метод анализирует одно главное событие и не учитывает вторичные или случайные сбои; — для крупномасштабных систем структура может быть очень сложной	— Обеспечивается другой командой — собственных экспертов или внешних аудитов; — дополнительно возможно сопоставление с данными производителя (SIL), полученными на стенде	— Для категорирования объектов КИИ; — для аудитов ИБ — для аудитов функциональной безопасности (SIL)
Менеджмент рисков (ISO/IEC 27005:2022)	Модель основана на реализации «классической» последовательности: установления контекста (в том числе критериев приемлемости риска и принятия остаточного риска), оценки риска, обработки рисков и принятия рисков	— Предварительно определены каталоги типовых УБИ и уязвимостей; — доступны шкалы оценивания вероятности и ущерба для формирования значения риска; — четкая структура управления рисками с двумя контрольными точками	— Метод не учитывает зависимости (последовательность) контролей; — для крупномасштабных систем результирующие численные оценки могут быть очень сложными и громоздкими	— Обеспечивается другой командой — собственных экспертов или внешних аудитов; — дополнительно возможно сопоставление с данными аудиторов при сертификации по требованиям ISO/IEC 27001	— Для учета инцидентов, УБИ и рисков по требованиям (БДУ ФСТЭК, OWASP, MITRE ATT&CK и прочее); — для категорирования объектов КИИ; — для аудитов ИБ; — для аудитов функциональной безопасности (SIL)

Заключение

Рассмотренные методы оценки риска информационной безопасности объектов критической инфраструктуры позволяют объективно обосновать количественные оценки и достоверно сформировать перечень необходимых мер защиты, обеспечивающих заданный уровень остаточных рисков. Полученные результаты могут быть применимы владельцами объектов критической инфраструктуры, заинтересованными в обеспечении заданного уровня безопасности на базе современных методов менеджмента рисков информационной безопасности, предоставляющих сопоставимые и воспроизводимые результаты.

Литература

1. Варламова Д.В., Долженкова А.В., Корочкина С.В. Автоматизация в Риск-менеджменте // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2020. № 4. С. 78–86. https://doi.org/10.17586/2310-1172-2020-13-4-78-86
2. Иващенко И.Н., Гончаров М.А. Безопасность и риск эксплуатируемых сооружений: Методология оперативной оценки // Проблемы анализа риска. 2021. Т. 18. № 6. С. 66–83. https://doi.org/10.32686/1812-5220-2021-18-6-66-83
3. Yusup M.F.B. Application of risk management in shipyards based SNI IEC/ISO 31010:2016 on new shipbuilding projects // Maritime Park: Journal of Maritime Technology and Society. 2022. V. 1. N 2. P. 75–78. https://doi.org/10.62012/mp.v1i2.32646
4. Frantzova A. Comprehensive methodology for geological risk and multy-risk assessment // Review of the Bulgarian Geological Society. 2021. V. 82. Part 3. P. 171–173. https://doi.org/10.52215/rev.bgs.2021.82.3.171
5. Neto A.B.C. Risk to be considered in nuclear reactor decommissioning projects in Brazil // Brazilian Journal of Radiation Sciences. 2022. V. 10. N 4. P. 1–24. https://doi.org/10.15392/2319-0612.2022.2111
6. Lesniak A., Janowiec F., Benavides J.R. The risk of additional branch work in the construction of railway projects // Archives of Civil Engineering. 2024. V. 70. N 2. P. 643–659. https://doi.org/10.24425/ace.2024.149886
7. Никифорова Н.А. Стратегический анализ: Международный стандарт ISO 31000:2018 и ГОСТ Р ИСО 31000-2019 // Финансовый бизнес. 2022. № 4 (226). С. 41–46.
8. Sukmana P.P., Yoga T.P., Habibi Ch. Audit manajemen risiko sistem informasi pada Website Digo.id dengan framework Cobit 5 dan ISO 31000 // Jurnal Accounting Information System (AIMS). 2023. V. 6. N 2. P. 180–201. https://doi.org/10.32627/aims.v6i2.816
9. Lavrnić I., Bašić A., Viduka D. Risk assessment of a solar attack according to ISO 31000 standard // Engineering Review. 2021. V. 41. N 1. P. 120–128. https://doi.org/10.30765/er.1566
10. Лившиц И.И. Практика управления киберрисками в нефтегазовых проектах компаний холдингового типа // Вопросы кибербезопасности. 2020. № 1 (35). С. 42–51. https://doi.org/10.21681/2311-3456-2020-01-42-51
11. Лившиц И.И., Сунцова Д.И. Численный расчет функциональной безопасности компонентов технически сложных промышленных объектов // Автоматизация в промышленности. 2023. № 7. С. 9–15. https://doi.org/10.25728/avtprom.2023.07.02
12. Yuwono M.A., Rachmawati D. Penerapan fraud risk management pada divisi pembelian PT. Lestari menggunakan ISO 31000:2018 // Jurnal Akuntansi Kontemporer. 2023. V. 15. N 3. P. 131–142. https://doi.org/10.33508/jako.v15i3.4629
13. Masita I. Analysis of risk management implementation in the internal audit unit (SPI) Politeknik pelayaran surabaya using ISO 31000 // Robust: Research of Business and Economics Studies. 2022. V. 2. N 2. P. 113–126. https://doi.org/10.31332/robust.v2i2
14. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Kunakov E.P., Drolova E.Y. Implementation and auditing of risk management for the oil and gas company // Proc. of the International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS). 2017. P. 539–543. https://doi.org/10.1109/itmqis.2017.8085881
15. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation - "hybrid" approach and risk of its implementation // Journal of Physics: Conference Series. 2018. V. 1015. N 4. P. 042030. https://doi.org/10.1088/1742-6596/1015/4/042030
16. Беляев Е.А., Емельянова О.А., Лившиц И.И. Анализ методик оценки рисков информационной безопасности кредитно-финансовых организаций // Научно-технический вестник информаци-

References

1. Varlamova D.V., Dolzhenkova A.V., Korochkina S.V. Automation in risk management. *Scientific journal NRU ITMO Series "Economics and Environmental Management"*, 2020, no. 4, pp. 78–86. (in Russian). https://doi.org/10.17586/2310-1172-2020-13-4-78-86
2. Ivashchenko I.N., Goncharov M.A. Safety and Risk of Operating Facilities: Rapid Assessment Methodology. *Issues of Risk Analysis*, 2021, vol. 18, no. 6, pp 66-83. (in Russian). https://doi.org/10.32686/1812-5220-2021-18-6-66-83
3. Yusup M.F.B. Application of risk management in shipyards based SNI IEC/ISO 31010:2016 on new shipbuilding projects. *Maritime Park: Journal of Maritime Technology and Society*, 2022, vol. 1, no. 2, pp. 75–78. https://doi.org/10.62012/mp.v1i2.32646
4. Frantzova A. Comprehensive methodology for geological risk and multy-risk assessment. *Review of the Bulgarian Geological Society*, 2021, vol. 82, part 3, pp. 171–173. https://doi.org/10.52215/rev.bgs.2021.82.3.171
5. Neto A.B.C. Risk to be considered in nuclear reactor decommissioning projects in Brazil. *Brazilian Journal of Radiation Sciences*, 2022, vol. 10, no. 4, pp. 1–24. https://doi.org/10.15392/2319-0612.2022.2111
6. Lesniak A., Janowiec F., Benavides J.R. The risk of additional branch work in the construction of railway projects. *Archives of Civil Engineering*, 2024, vol. 70, no. 2, pp. 643–659. https://doi.org/10.24425/ace.2024.149886
7. Nikiforova N.A. Strategic analysis: international standard ISO 31000:2018 and GOST R ISO 31000-2019. *Finansovyj Biznes*, 2022, no. 4 (226), pp. 41–46. (in Russian)
8. Sukmana P.P., Yoga T.P., Habibi Ch. Audit manajemen risiko sistem informasi pada Website Digo.id dengan framework Cobit 5 dan ISO 31000. *Jurnal Accounting Information System (AIMS)*, 2023, vol. 6, no. 2, pp. 180–201. https://doi.org/10.32627/aims.v6i2.816
9. Lavrnić I., Bašić A., Viduka D. Risk assessment of a solar attack according to ISO 31000 standard. *Engineering Review*, 2021, vol. 41, no. 1, pp. 120–128. https://doi.org/10.30765/er.1566
10. Livshitz I. Practice of cyber-risks management in oil and gas projects of holding companies. *Voprosy Kiberbezopasnosti*, 2020, no. 1 (35), pp. 42–51. (in Russian). https://doi.org/10.21681/2311-3456-2020-01-42-51
11. Livshits I.I., Suntsova D.I. Numerical calculation of functional safety of the components of technically complex industrial plants. *Avtomatizacija v promyshlennosti*, 2023, no. 7, pp. 9–15. (in Russian). https://doi.org/10.25728/avtprom.2023.07.02
12. Yuwono M.A., Rachmawati D. Penerapan fraud risk management pada divisi pembelian PT. Lestari menggunakan ISO 31000:2018. *Jurnal Akuntansi Kontemporer*, 2023, vol. 15, no. 3, pp. 131–142. https://doi.org/10.33508/jako.v15i3.4629
13. Masita I. Analysis of risk management implementation in the internal audit unit (SPI) Politeknik pelayaran surabaya using ISO 31000. *Robust: Research of Business and Economics Studies*, 2022, vol. 2, no. 2, pp. 113–126. https://doi.org/10.31332/robust.v2i2
14. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Kunakov E.P., Drolova E.Y. Implementation and auditing of risk management for the oil and gas company. *Proc. of the International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, 2017, pp. 539–543. https://doi.org/10.1109/itmqis.2017.8085881
15. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation - "hybrid" approach and risk of its implementation. *Journal of Physics: Conference Series*, 2018, vol. 1015, no. 4, pp. 042030. https://doi.org/10.1088/1742-6596/1015/4/042030
16. Belyaev E.A., Emelyanova O.A., Livshitz I.I. An analysis of methods for assessing information security risks of financial institutions.

онных технологий, механики и оптики. 2021. Т. 21. № 3. С. 437–441. https://doi.org/10.17586/2226-1494-2021-21-3-437-441
17. Беззатеев С.В., Елина Т.Н., Мыльников В.А., Лившиц И.И. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 4. С. 553–561. https://doi.org/10.17586/2226-1494-2021-21-4-553-561
18. Ezrahovich A.Y., Vladimirtsev A.V., Livshitz I.I., Lontsikh P.A., Karaseva V.A. Risk-based thinking of ISO 9001:2015 — the new methods, approaches and tools of risk management // Proc. of the International Conference “Quality Management,Transport and Information Security, Information Technologies” (IT&QM&IS). 2017. P. 506–511. https://doi.org/10.1109/itmqis.2017.8085872

Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2021, vol. 21, no. 3, pp. 437–441. (in Russian). https://doi.org/10.17586/2226-1494-2021-21-3-437-441
17. Bezzateev S.V., Elina T.N., Mylnikov V.A., Livshitz I.I. Risk assessment methodology for information systems, based on the user behavior and IT-security incidents analysis. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 4, pp. 553–561. (in Russian). https://doi.org/10.17586/2226-1494-2021-21-4-553-561
18. Ezrahovich A.Y., Vladimirtsev A.V., Livshitz I.I., Lontsikh P.A., Karaseva V.A. Risk-based thinking of ISO 9001:2015 – the new methods, approaches and tools of risk management. *Proc. of the International Conference “Quality Management,Transport and Information Security, Information Technologies” (IT&QM&IS)*, 2017, pp. 506–511. https://doi.org/10.1109/itmqis.2017.8085872

Автор

Лившиц Илья Иосифович — доктор технических наук, профессор практики, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Author

Ilya I. Livshitz — D.Sc., Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 57191569306, https://orcid.org/0000-0003-0651-8591, Livshitz.il@yandex.ru

Статья поступила в редакцию 25.02.2025
Одобрена после рецензирования 05.06.2025
Принята к печати 22.07.2025

Received 25.02.2025
Approved after reviewing 05.06.2025
Accepted 22.07.2025