НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2023 Том 23 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2023 Vol. 23 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2023-23-3-519-529
УДК 004.056

Обзор национальных и международных стандартов для категорирования объектов критической информационной инфраструктуры

Илья Иосифович Лившиц✉

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

Аннотация
Обеспечение безопасности объектов критической информационной инфраструктуры — активно развивающееся направление в сфере информационной безопасности на национальном и мировом уровне. Категорирование объектов критической инфраструктуры является составной частью общего процесса обеспечения безопасности. При динамично изменяющемся уровне угроз процесс определения категории объекта все еще недостаточно оптимален. На основе существующих требований российских и международных стандартов оценивание объектов критической инфраструктуры проводится не всегда оперативно и корректно. Также не формируются численные оценки, не обеспечивается объективность оценки и последующей переоценки со стороны независимых экспертов. В работе представлен анализ актуальных требований в области категорирования объектов критической инфраструктуры, применяемых в Российской Федерации. Выполнен сравнительный анализ национальных нормативных правовых актов Российской Федерации и системы международных стандартов в области информационной безопасности. Рассмотрено регулирование процессов категорирования объектов критической инфраструктуры. Обоснована необходимость формирования численных значений критериев значимости для корректного определения и последующей независимой оценки (переоценки) категории объектов критической инфраструктуры. Представлены рекомендации по совершенствованию процесса категорирования объектов критической инфраструктуры и формированию численных оценок. Реализация приложенных рекомендаций позволит повысить точность, объективность и достоверность процесса создания современных систем обеспечения информационной безопасности.

Ключевые слова
критическая информационная инфраструктура, категорирование объектов критической информационной инфраструктуры, критерии значимости, информационная безопасность, система управления информационной безопасности, риски, остаточные риски

Ссылка для цитирования: Лившиц И.И. Обзор национальных и международных стандартов для категорирования объектов критической информационной инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23, № 3. С. 519–529. doi: 10.17586/2226-1494-2023-23-3-519-529

Review of national and international standards for categorizing of critical information infrastructure objects

Ilya I. Livshitz✉

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

Abstract
Ensuring the security of critical information infrastructure facilities is an actual developing area of information security both at the national and global level. Categorization of critical infrastructure objects is an integral part of the common and holistic security process. With a dynamically changing threats level, the process of determining the category of an object is still not optimal enough. Based on the existing requirements both of Russian and International standards, the assessment of critical infrastructure facilities not always be carried out promptly and correctly, in addition, numerical

estimates are not formed, the objectivity of the assessment and subsequent reassessment by independent experts is not ensured. This article presents an analysis of the current requirements in the field of categorization of critical infrastructure objects used in the Russian Federation. A comparative analysis of the national regulatory legal acts of the Russian Federation and the system of International standards in the field of IT-security is presented. Regulation of categorization processes of critical infrastructure objects is considered. The necessity of forming numerical values of significance criteria for the correct determination and subsequent independent evaluation (reassessment) of the category of critical infrastructure objects is substantiated. Recommendations for improving the process of categorizing critical infrastructure objects and the formation of numerical estimates are presented. The implementation of the recommendations made will improve the accuracy, objectivity and reliability of the process of creating modern information security systems.

Keywords
critical information infrastructure, categorization of critical information infrastructure objects, significance criteria, information security, information security management system, risks, residual risks

For citation: Livshitz I.I. Review of national and international standards for categorizing of critical information infrastructure objects. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 3, pp. 519–529 (in Russian). doi: 10.17586/2226-1494-2023-23-3-519-529

Введение

Значимым результатом отражения существенных изменений в процессах обеспечения информационной безопасности (ИБ) в Российской Федерации стала Доктрина информационной безопасности[1] 2016 г. С помощью доктрины были обновлены концепция и задачи обеспечения защиты информации, а также уточнены важные понятия, например, «критическая информационная инфраструктура» (КИИ). В результате были приняты Федеральный закон от 26.07.2017 N 187-ФЗ[2] «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ) и Постановление Правительства РФ от 08.02.2018 N 127[3] «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (ПП-127). Указанная система требований, во-первых, ввела в Российской Федерации понятие КИИ, которое заменило ранее применявшееся устаревшее понятие — «ключевые системы информационной инфраструктуры», предложенные в 2014 г. ФСТЭК России, и определила новые требования по защите: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 21 декабря 2017 г. N 235[4] «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и Приказ ФСТЭК от 25 декабря 2017 г. N 239[5] «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. Приказов ФСТЭК России от 9 августа 2018 г. N 138, от 26 марта 2019 г. N 60, от 20 февраля 2020 г. N 35).

Для объектов КИИ важно оперативно и корректно выполнить оценку критерия значимости информационной системы (ИС) в зависимости от обрабатываемых типов информации [1, 2]. Определение критерия значимости ИС зависит от применяемых категорий информации и регламентируется формальным процессом категорирования. С учетом последующей «стоимости» ошибок при создании некорректной системы обеспечения информационной безопасности (СОИБ) при неточном (неполном) категорировании, можно обоснованно полагать, что этап категорирования является ключевым, поскольку безопасность объектов КИИ крайне важна практически для всех сфер современной экономики и государственного управления [3, 4]. Актуальность рассматриваемой проблемы точного численного и корректного категорирования объектов КИИ с учетом новых рисков и требования повышения уровня обеспечения ИБ для стратегически важных отраслей подтверждена дополнительно в Указе Президента Российской Федерации от 01.05.2022 № 250[6] «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Непринятие мер по защите на объектах КИИ может привести к серьезным инцидентам, например, в области топливно-энергетического комплекса: нефтяной терминал SaudiAramco[7], нефтяной завод Oil

[1] Указ Президента Российской Федерации от 05.12.2016 г. № 646 [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/41460, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] Федеральный закон от 26.07.2017 г. N 187 [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/?ysclid=l8d73e934i5010228, свободный. Яз. рус. (дата обращения: 20.10.2022).

[3] Постановление Правительства РФ от 08.02.2018 г. N 127 [Электронный ресурс]. Режим доступа: https://base.garant.ru/71876120/?ysclid=l8d75l1svw618900114, свободный. Яз. рус. (дата обращения: 20.10.2022).

[4] Приказ ФСТЭК России от 21 декабря 2017 г. N 235 [Электронный ресурс]. Режим доступа: https://fstec.ru/normotvorcheskaya/ akty/53-prikazy/1589-?ysclid=l8d7t834hy284363961, свобод- ный. Яз. рус. (дата обращения: 20.10.2022).

[5] Приказ ФСТЭК России от 25 декабря 2017 г. N 239 [Электронный ресурс]. Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239?ysclid=l8d7u36shh579968999, свободный. Яз. рус. (дата обращения: 20.10.2022).

[6] Указ Президента Российской Федерации от 01.05.2022 г. № 250 [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/47796, свободный. Яз. рус. (дата обращения: 20.10.2022).

[7] Хуситы зажигают нефть ракетами [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4584906?, сво-

India[1], нефтеперерабатывающий завод Petro Rabigh[2], трубопровод Colonial Pipeline[3] и др. Актуальность проблемы защиты объектов КИИ не вызывает сомнения, и для снижения ущерба и минимизации рисков возникает необходимость создания корректного СОИБ для объектов КИИ. Известно, что каждая ИС, работающая с определенной «чувствительной» информацией, требует применения определенного набора мер и средств защиты (иногда называемых «контролями», *IT-security controls*), обеспечивающих поддержание безопасного функционирования на заданном уровне (степень результативности, *effectiveness*) в соответствии с определенным множеством требований или критериев (*criteria*). В качестве критериев могут быть приняты известные национальные и международные стандарты, которые предоставляют рекомендации по выполнению процессов оценки соответствия (*conformity assessment*). Соответственно, корректный процесс категорирования позволяет рационально установить критерии, далее выбрать оптимальный набор средств и мер защиты (*controls*) и обеспечить заданный результат — создание, внедрение и развитие СОИБ для конкретного объекта КИИ [5, 6]. В развитие новизны данной темы примем во внимание еще один параметр — экономическую эффективность СОИБ применительно к оптимальной совокупности средств и мер защиты, позволяющих обеспечить заданный результат в определенных граничных условиях (время, деньги, персонал и прочее). Пример расчета оптимальности различных наборов средств и мер защиты и сопоставления их по показателю чистого дисконтированного дохода (Net Present Value, NPV), полученный автором при проведении курсов в Университете ИТМО, представлен на рис. 1.

На рисунке показано наглядное сопоставление двух и более вариантов набора мер и средств обеспечения безопасности, дающих различные экономические расчетные значения по показателю NPV. Видно, что вариант *2* выглядит более предпочтительным, поскольку проходит точку окупаемости раньше, чем вариант *1* при одинаковых граничных условиях (лабораторные расчетные условия) [7, 8].

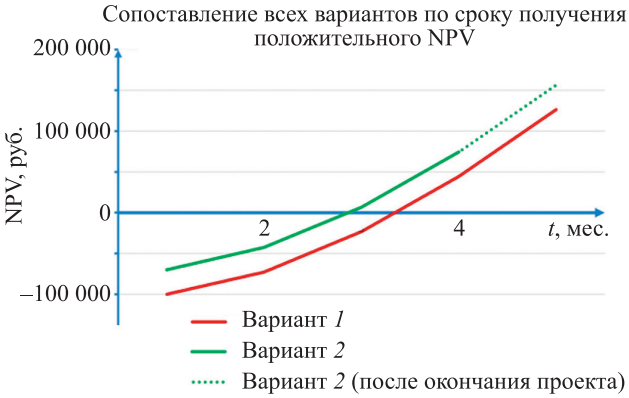

Рис. 1. Пример сопоставления вариантов мер и средств обеспечения безопасности [7]

Fig. 1. An example of comparing various security controls combinations [7]

Анализ российского законодательства для категорирования объектов КИИ

Как было показано в разделе «Введение», в Российской Федерации в законодательство введено понятие КИИ, к обязательной области применения которого относятся организации, функционирующие в закрытом перечне 14 сфер деятельности (ст. 2 п.8 187-ФЗ) и имеющие ИС, информационно-телекоммуникационные сети или автоматизированные системы управления технологическими процессами, являющиеся объектами КИИ. Основные юридические схемы обеспечения процесса защиты объектов КИИ регламентирует 187-ФЗ. Обобщенно, процесс категорирования объектов КИИ, в соответствии со ст. 7 187-ФЗ, заключается в установлении эквивалентности конкретного объекта КИИ критериям значимости (всего определено 14 критериев по 5 группам) и показателям их значений, которые определены в ПП-127. Указанный этап обязывает субъектов КИИ объективно определить критичные процессы организации, и на их основе обоснованно выделить конкретные объекты, относящиеся к КИИ.

Существующей нормативной правовой базой в Российской Федерации в сфере обеспечения безопасности КИИ не определены «целевые» конкретные показатели для критериев ключевых процессов, ответственность за их определение полностью ложится на субъекты КИИ. Показатели критериев значимости 3-х категорий значимости, от 1-й (наивысшей) до 3-й (наименьшей), определены конкретными диапазонами исчисляемых единиц и показателями нарушений штатной работоспособности относительно установленного официального фиксированного значения. Строгие фиксированные ограничения могут приводить к определению категории значимости, не отражающей в полной мере реальность функционирования и (или) непрерывные процессы технической модернизации, функционального развития и (или) переконфигурирования. Например, в настоящее время не в полной мере определен порядок проведения категорирования сложных современных объектов, оснащенных блоками электроники под управлением микропроцессоров — станков с числовым программным управлением[4], меди-

бодный. Яз. рус. (дата обращения: 20.10.2022).

[1] Хакеры потребовали $7,5 млн у индийского нефтяного завода Oil India [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/531297.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] Аварийная ситуация: как противостоять атакующему системы ПАЗ вредоносу Trisis [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/analytics/523661.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[3] Colonial Pipeline предупреждает клиентов об утечке данных в результате атаки DarkSide [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/news/523424.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[4] Автоматический или автоматизированный? Все равно ОКИИ! Транспорт [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/blog/personal/valerykomarov/349793.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

цинских информационных мониторинговых системы[1], тепловозов, судов с цифровыми блоками управления[2]. Отметим, что процесс обеспечения безопасности объектов КИИ в Российской Федерации был существенно модернизирован в 2018 г., как в рамках соответствия определенным важным задачам «Стратегии национальной безопасности Российской Федерации»[3], так и при смене применявшегося еще в 2014 г. подхода защиты ключевой системы информационной инфраструктуры, предложенного ФСТЭК России[4] и отмененного в 2018 г. В существующем варианте жесткие установленные нормативы не допускают вариации исходя из актуальных (или планируемых при последующей модернизации) изменений технических характеристик и (или) технологических изменений объектов КИИ. В отличие от известного подхода управления рисками в технических системах (ГОСТ Р ИСО серии 31000[5], ГОСТ Р МЭК серии 31010[6]), в существующих условиях владельцы объектов КИИ не выполняют переоценку показателей по ПП-127, не поддерживают и не обновляют файлы рисков (не учитываются остаточные риски) и не пересматривают состав мер и средств защиты, применяемых в каждый конкретный момент.

Анализ международной законодательной базы для категорирования объектов КИИ

Анализ международной нормативной базы начнем с рассмотрения наиболее известного, практически применяемого и периодически обновляемого стандарта ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management[7]. Данный стандарт считается во всем мире ключевым для расчета рисков (остаточных рисков) ИБ и формирования системы для точно определяемых требований при категорировании защищаемых активов различного назначения. Заметим, что в октябре 2022 г. вышла новая версия стандарта ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks[8].

Рассмотрим наиболее важные требования, установленные в ISO/IEC 27005:2022:

— определение критериев воздействия (*Impact criteria*). Критерии разработаны и конкретизированы с точки зрения степени ущерба или затрат для организации, вызванных событием ИБ, с учетом уровня классификации затронутого информационного ресурса;
— оценка последствий (*Assessment of consequences*). Оценка активов начинается с классификации активов в соответствии с их критичностью с точки зрения их важности для достижения бизнес-целей организации. Далее оценка определяется с использованием двух показателей: восстановительная стоимость актива (стоимость восстановления, очистки и замены информации, если это возможно); деловые последствия потери или компрометации актива, такие как потенциальные неблагоприятные деловые и (или) правовые или нормативные последствия раскрытия, модификации, отсутствия и (или) уничтожения информации и других информационных активов.

Отметим, что в ПП-127 четко указано, что исходными данными для категорирования являются угрозы безопасности информации (УБИ) в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа. В результате виден общий методический подход для определения объективных свидетельств (статистики), на базе которой возможно выполнение оценки рисков и выбора наиболее эффективных мер противодействия актуальным УБИ. В качестве примера рассмотрим отчет «Анализ мошеннических звонков с территории Украины. Участники и цифры (ноябрь 2022)»[9], в котором приведены данные статистики Сбера за 2022 г. В отчете отмечено, что мошенники сделали 1,5 млрд попыток позвонить клиентам банков с целью похитить денежные средства. Также приведены данные по опе-

---

[1] Краткий обзор новой методики оценки угроз ФСТЭК [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/blog/personal/Business_without_danger/350381.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] Сегодня АСУ ТП не защищают ни воздушный зазор, ни проприетарные протоколы [Электронный ресурс]. Режим доступа: https://www.securitylab.ru/blog/company/solarsecurity/347320.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[3] Указ Президента Российской Федерации от 02.07.2021 г. № 400 О Стратегии национальной безопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/acts/bank/47046, свободный. Яз. рус. (дата обращения: 20.10.2022).

[4] Информационное сообщение ФСТЭК России от 4 мая 2018 г. N 240/22/2339 [Электронный ресурс]. Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie-fstek-rossii-ot-4-maya-2018-g-n-240-22-2339, свободный. Яз. рус. (дата обращения: 20.10.2022).

[5] ГОСТ Р ИСО 31000-2019 Национальный стандарт Российской Федерации. Менеджмент риска. Принципы и руководство. [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200170125?ysclid=lgxkri97tj944205707 свободный. Яз. рус. (дата обращения: 20.10.2022).

[6] ГОСТ Р ИСО 31010-2021 Национальный стандарт Российской Федерации. Надежность в технике. Методы оценки риска. [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200180987?ysclid=lgxkvbc8ut371018586 свободный. Яз. рус. (дата обращения: 20.10.2022).

[7] ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management [Электронный ресурс]. Режим доступа https://www.iso.org/standard/75281.html, свободный. Яз. рус. (дата обращения: 20.10.2022).

[8] ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks [Электронный ресурс]. Режим доступа: https://www.iso.org/standard/80585.html, свободный. Яз. рус. (дата обращения: 20.10.2022).

[9] Анализ мошеннических звонков с территории Украины. Участники и цифры [Электронный ресурс]. Режим доступа: https://promo.sber.ru/kibrary, свободный. Яз. рус. (дата обращения: 20.10.2022).

раторам, которые безнаказанно пропускают мошеннический трафик с установочными данными.

Важно обратить внимание на логику стандарта ISO/IEC 27005:2018, в котором особое внимание отдано на определение бизнес-целей. Далее выполнена классификация необходимых активов исходя из их уровня критичности по отношению к определенным ранее бизнес-целям, и выбран наиболее оптимальный состав мер для противодействия с учетом важной экономической оценки «восстановительной стоимости» (*replacement value of the asset*), насколько это практически возможно. В Приложении B (Annex B) дано описание состава первичной информации, которое включает: жизненно важную информацию (*vital information*) для осуществления миссии или бизнеса организации; личную информацию (*personal information*), в соответствии с национальными законами о конфиденциальности; стратегическую информацию (*strategic information*), необходимую для достижения целей, определенных стратегическими целями; дорогостоящую информацию (*high-cost information*), сбор, хранение, обработка и передача которой требует длительного времени и (или) сопряжена с высокой стоимостью приобретения.

Примем во внимание, что информация, которая не была идентифицирована как «чувствительная» (*sensitive*) после проведения общей оценочной процедуры в первом цикле, может не иметь классификации, следовательно, даже если такая информация будет скомпрометирована, организация все равно сможет успешно выполнить свою миссию. С другой стороны, необходимо принять во внимание, что в случае ошибочной и (или) неполной классификации первичной информации, возможны серьезные инциденты ИБ в случае компрометации, поскольку для ошибочно пропущенной информации для конкретного объекта (ИС) в СОИБ не были предусмотрены соответствующие меры защиты. В результате необходимо учесть, что исключительно важно выполнение последующего обязательного цикла переоценки с учетом остаточных рисков в отношении объекта защиты (ИС) [9–12].

Анализ федерального законодательства ФРГ для категорирования объектов КИИ

Рассмотрим два актуальных стандарта (BSI-Standard 200-2 IT-Grundschutz Methodology (BSI 200-2[1] и BSI 200-3[2]) в системе федеральных стандартов BSI (ФРГ), которые определяют процесс управления рисками ИБ, в том числе порядок работы с активами применительно к объектам КИИ. Перед началом фактического анализа рисков ИБ по BSI 200-3 выполним процедуру в соответствии с BSI 200-2, включающую: регламентацию и внедрение процесса обеспечения ИБ в организации, в том числе путем утверждения концепции безопасности; определение области применения концепции безопасности и формирование соответствующего перечня ценных информационных активов; определение и внедрение базовых и стандартных мер по обеспечению ИБ определенных активов.

В результате данного оценивания (по аналогии со стандартом ISO/IEC 27005) получим перечень информационных активов, в отношении которых необходимо выполнить анализ рисков. Стандарт BSI 200-2 допускает объединение активов в группы с целью сохранения разумности при выполнении оценки значительного количества типовых активов (однотипных программируемых промышленных контроллеров, рабочих станций и др.) и определение в дальнейшем приоритетов для такой оценки: «стандартная защита» — приоритет отдается высокоуровневой оценке бизнес-процессов и всей ИТ-инфраструктуры. Полученная оценка выступает как ориентир для управления рисками в отношении активов более низких уровней; «защита ядра» — приоритет отдается оценке ключевых активов, которым должны быть предъявлены самые высокие требования к внедряемым мерам защиты; «базовая защита» — сначала выполняются обязательные базовые требования из BSI 200-2, затем — мероприятия по оценке рисков.

Заметим, что стандарт BSI 200-2 при реализации варианта «базовой защиты» требует сначала выполнить базовые требования и затем «включить» данный состав информационных активов в контекст общего процесса управления рисками с последующей оптимизаций состава применяемых мер защиты. В п. 8.2.1 «Определение категорий потребностей в защите» определено, что «потребности в защите обычно не поддаются количественной оценке». Следует полагать данное ограничение существенным недостатком, негативно влияющем на возможность применения различных шкал (дискретных оценок) и иных численных показателей в отношении конкретного объекта оценивания. По этой причине BSI 200-2 ограничивается только квалифицированным заявлением, подразделяя потребности в защите на три категории последствий ущерба: «нормальная» (*normal*) — ограничены и поддаются управлению; «высокие» (*high*) — могут быть значительными; «очень высокие» (*very high*) — могут достигать катастрофического уровня.

Рассмотрим в качестве примера одну из категорий — «нормальную» защиту, определенную в стандарте BSI 200-2. Для рассматриваемой категории потребность в защите определяется при следующих факторах: нарушение законов (нормативных актов) с незначительными последствиями; незначительные нарушения контракта (*Minor breaches of contract*) с максимально низкими штрафными санкциями; нарушение прав (*Impairment of the right*) обработки персональных данных с неблагоприятными последствиями; ухудшение способности (*Impairment of the ability*) выполнять задачи (оцениваемое как приемлемое, максимально допустимое время простоя составляет от 24 до 72 ч); финансовые последствия (*Financial consequences*) признаются приемлемыми.

[1] BSI-Standard 200-2 [Электронный ресурс]. Режим доступа https://www.bsi.bund.de/SharedDocs/Downloads/EN/ BSI/Grundschutz/International/bsi-standard-2002_en_pdf. pdf?blob=publicationFile&v=2, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] Немецкое качество или как оценивать риски ИБ по BSI-Standard 200-3 [Электронный ресурс]. Режим доступа https://www.securitylab.ru/blog/company/USSC/352337.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

Анализ федеральных стандартов NIST по категорированию

На международном уровне для категорирования объектов КИИ, кроме ISO (IEC), наиболее известными являются стандарты:

— FIPS (Federal Information Processing Standards, Федеральные стандарты обработки информации) серии 199 «Standards for Security Categorization of Federal Information and Information Systems» (Стандарты категорирования безопасности информации и информационных систем) (FIPS 199[1]);
— NIST (National Institute of Standards and Technology, Национальный институт стандартов и технологий) серии SP 800-60 «Guide for Mapping Types of Information and Information Systems to Security Categories Special Publication» (Специальное издание. Руководство по сопоставлению типов информации и информационных систем с категориями безопасности);
— FISMA (Federal Information Security Management Act, Федеральный закон США об управлении информационной безопасностью), 2002 г.

В стандартах NIST предложено осуществлять как категорирование обрабатываемой (и защищаемой) информации, так и ИС в целом [13]. Категорирование ИС является первым шагом для создания СОИБ, последующие этапы создания которой описаны в цикле RFM[2] (Risk Management Framework, Структура управления рисками) [14, 15]. Подробное описание процесса категорирования, которое относится к этапу планирования СОИБ, в соответствии с требованиями NIST SP 800-53[3], представлено на рис. 2.

Корректное определение категории значимости ИС — результат адекватно установленной категории критичности различных типов информации, обрабатываемой в рассматриваемой ИС [16, 17]. В соответствии с FIPS 199, категория безопасности ИС — наивысшее значение критичности из всех типов информации, функционирующей в рассматриваемой ИС. Таким образом, изначально рассматриваются и оцениваются все типы информации, которые есть в ИС [18, 19]. Следующим этапом оценивается уровень потенциального воздействия на каждый тип информации и определяется лишь качественное значение: низкое, среднее, высокое или отсутствует.

К сожалению, в рассматриваемых федеральных стандартах NIST допускаются только качественные оценки, и этот недостаток, отчасти, нивелирует применимость предлагаемого аппарата для современного использования в процессе создания эффективной СОИБ. Потенциальное воздействие определяется оценкой ущерба для каждого объекта по свойствам безопасности (конфиденциальность, целостность, доступность). И в данном случае — фиксированная «триада» свойств ИБ, и этот недостаток, также не дает основания применения методического аппарата для современного практического использования. На последнем шаге для оценки воздействия на каждый объект ИБ для ИС выбирается максимальное воздействие из всех типов информации в ИС [16, 17]. В публичных ресурсах доступны примеры применения методики FIPS 199, что позволяет строить простейшие записи для оценивания категории безопасности (КБ) для ИС:

$$КБ_{ИС} = \{(К, воздействие); (Ц, воздействие); (Д, воздействие)\}, \quad (1)$$

где К — конфиденциальность; Ц — целостность; Д — доступность.

При данном наборе «триады» свойств ИБ критичность ИС — $КБ_{ИС}$ определяется в соответствии с FIPS 199 следующим образом (табл. 1).

В развитии новизны по данной теме учтем несколько дополнительных свойств ИБ, например: подотчетность, неотказуемость, аутентичность (в соответствии с требованиями п. 3.28). Тогда запись (1) обеспечит более расширенный перечень свойств ИБ, например:

$$КБ_{ИС} = \{(К, воздействие); (Ц, воздействие); (Д, воздействие); (П, воздействие); (Н, воздействие); (А, воздействие)\}, \quad (2)$$

где П — подотчетность; Н — неотказуемость; А — аутентичность.

При расширенном, по сравнению с базовым набором свойств ИБ (FIPS 199) на основании записи (2) $КБ_{ИС}$, определим критичность ИС в соответствии с новой комбинацией FIPS 199 и ISO/IEC 27001[4] (табл. 2). Видно, что расширенный метод обеспечивает явное улучшение точности КБИС (по расширенному набору свойств, но все же оценки по-прежнему применяются только качественные, не формируются численные оценки и не обеспечивается объективность оценки и переоценки со стороны независимых экспертов. Напомним, что рассматриваемые недостатки объективно могут повлечь негативные и необратимые последствия при создании СОИБ и в открытых источниках, только за 2022 г. приведены примеры противодействия для современных векторов атак и конкретных уязвимостей промышленных систем[5].

[1] Промышленные компании: векторы атак [Электронный ресурс]. Режим доступа https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] Risk Management Framework for Information Systems and Organizations [Электронный ресурс]. Режим доступа https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, свободный. Яз. рус. (дата обращения: 20.10.2022).

[3] Обзор NIST SP 800-53 [Электронный ресурс]. Режим доступа https://www.altx-soft.ru/upload/iblock/d76/%D0%9E%D0%B1%D0%B7%D0%BE%D1%80%20SP%20800-53_v4.pdf?ysclid=l8eiqe5gxr92836019, свободный. Яз. рус. (дата обращения: 20.10.2022).

[4] ISO/IEC 27001 Системы менеджмента информационной безопасности [Электронный ресурс]. Режим доступа https://www.iso.org/ru/standard/27001, свободный. Яз. рус. (дата обращения: 20.10.2022).

[5] Уязвимости в CodeMeter позволяют атаковать промышленные системы [Электронный ресурс]. Режим доступа https://www.securitylab.ru/news/511888.php?ysclid=la87gkvxjw783700363, свободный. Яз. рус. (дата обращения: 20.10.2022).

Рис. 2. Схема этапа планирования системы обеспечения безопасности [14, 15]
Fig. 2. Scheme of IT-Security planning stage [14, 15]

Таблица 1. Пример определения критичности информационной системы (базовый метод FIPS 199)
Table 1. Example of determining the Information system criticality (FIPS 199 basic method)

Объект	К	Ц	Д	Критичность
База данных	Среднее	Среднее	Низкое	—
Системная информация	Низкое	Среднее	Низкое	—
Оцениваемая система	Среднее	Среднее	Низкое	Средняя

Таблица 2. Пример определения критичности ИС (расширенный метод)
Table 2. Example of determining the Information system criticality (enchased method)

Объект	К	Ц	Д	П	А	Н	Критичность
База данных	Среднее	Среднее	Низкое	Среднее	Низкое	Низкое	—
Системная информация	Низкое	Среднее	Низкое	Среднее	Среднее	Низкое	—
Оцениваемая система	Среднее	Среднее	Низкое	Низкое	Среднее	Низкое	Средняя

Принцип определения $КБ_{ИС}$ в табл. 1 и табл. 2 простой — по достижении более высокого значения ($КБ_{Значение}$) для конкретного свойства ИБ ($КБ_{Свойство}$) вся оцениваемая ИС соответствует автоматически данному значению [18, 19]. Следует отметить, что и ранее действующий защиты ключевой системы информационной инфраструктуры и актуальное ПП-127 придерживаются такого же правила — по достижения высшего значения (ущерба, показателя и др.) вся оцениваемая система (объект оценки) автоматически «наследует» это значение. Например, конкретное свойство ИБ можно определить по факту объективного оценивания текущего значения ($КБ_{Значение}$) и выбранного критерия ($КБ_{Критерий}$):

$$\begin{cases} КБ_{Свойство} = 1;\ КБ_{Значение} \geq КБ_{Критерий} \\ КБ_{Свойство} = 0;\ КБ_{Значение} < КБ_{Критерий} \end{cases}.$$

При этом $КБ_{Значение}$, и $КБ_{Критерий}$ предполагаются численными дискретными в некотором фиксированном и удобном для практического применения в диапазоне, например {0; ¼; ½; ¾; 1}. Заметим, что такие дискретные шкалы могут применяться в соответствии с ГОСТ Р серии 57580[1]. Также в новом методе допускается для повышения скорости формирования оценки $КБ_{ИС}$ дополнительное условие — значение критерия ($КБ_{Критерий}$) может быть одинаковым для некоторого свойства ИБ или для всей совокупности свойств ИБ для конкретного объекта.

[1] ГОСТ Р 57580.1-2017 Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Базовый состав организационных и технических средств [Электронный ресурс]. Режим доступа https://docs.cntd.ru/document/1200146534?ysclid=lgxlkyqwei299336614 свободный. Яз. рус. (дата обращения: 20.10.2022).

Тогда оценка $КБ_{ИС}$ примет следующий вид по совокупности множества свойств ($КБ_{Свойство}$):

$$КБ_{ИС} = \frac{1}{n}\sum_{i}^{n} КБ_{Свойство_i}.$$

В результате задача оптимизации оценки $КБ_{ИС}$ имеет вид (в условиях неравенства $КБ_{Значение}$ и $КБ_{Критерий}$):

$$КБ_{ИС} \xrightarrow{КБ_{Значение} \neq КБ_{Критерий}} \max.$$

Оптимизацию КБ $\xrightarrow{КБ_{Критерий}}$ max выполним в граничных условиях совокупности свойств ИБ («триада» — в базовом варианте и «шести» — в расширенном варианте) и дискретности шкалы оценки. Обратим внимание на актуальный пример — в современных условиях расширение «дискретности» свойств ИБ при оценивании критичности обрабатываемой информации в конкретном объекте может иметь исключительно важное значение — например, для СМИ[1] (в отношении доступности, целостности и подотчетности). Дополнительно рассмотрим дальнейшее совершенствование нового метода категорирования объектов, а именно — как может быть реализована комплексная оценка КБИС с учетом не только оценки собственных экспертов, но и оценки независимых экспертов (например, в рамках аудитов различных типов — внутренних, внешних 2-й стороной или внешних 3-й стороной).

$$КБ_{Комплексный} = \frac{1}{k}\sum_{i}^{k} КБ_{ИС_j} R_j,$$

где граничные условия для весовых коэффициентов определяются как:

$$\sum_{j}^{k} R_j = 1.$$

Индекс j в общем случае имеет значения от 1 (только внутренний аудит или иногда еще говорят «самооценка») до 3 (добавляется внешний аудит 2-й стороной, например, аттестованной лабораторией ФСТЭК, и внешний аудит 3-й стороной, например, органом по сертификации с необходимой аккредитацией). Безусловно, новый метод нуждается в серьезном контроле беспристрастности (*impartiality*), что является крайне важным в процессе оценки соответствия и занимает первую позицию в перечне принципов, обеспечивающих доверие (ISO/IEC 17021[2]).

Для поддержания доверия необходимо, чтобы решения органа по сертификации основывались на объективных свидетельствах соответствия, и чтобы на его решения не влияли другие интересы или стороны. Дополнительно рассмотрим явное указание угроз сохранения беспристрастности, в частности, финансовый интерес. Необходимо рассмотреть еще один факт, когда сертификат соответствия требованиям международных стандартов ISO одной из крупнейших в Российской Федерации компаний был отозван одним из британских органов по сертификации на основании того, что в составе учредителей есть представитель королевской семьи. В данной ситуации говорить о сохранении беспристрастности не приходится, но данный инцидент в не меньшей степени говорит о важности применения в регулярной практике процедур управления рисками (остаточными рисками). В Российской Федерации регуляторы предпринимают определенные меры для решения данной известной проблемы (например, на уровне Банка России[3] и на уровне экспертного сообщества[4]).

Сравнительный анализ методических подходов для категорирования объектов КИИ

При определении соответствия объектов КИИ установленным критериям значимости, примем во внимание, что существуют ИС, которые в автономном режиме функционирования не будут иметь высокой степени критичности. В то же время на практике в коммерческих и государственных организациях применяется множество ИС, работоспособность которых исходно взаимосвязана — информация различных типов хранится, передается, зашифровывается/расшифровывается и обрабатывается в сложном технологическом «конвейере». Ситуация может значительно усложняться при территориальном (трансграничном) разнесении компонентов КИИ и обеспечения безопасности сложных иерархических систем — например, компоненты автоматизированной системы управления технологическими процессами, работающие в режиме жесткого реального времени. В этом случае потребуется обеспечить анализ соответствия нескольких типов объектов КИИ, функционирующих в разных юрисдикциях, часовых поясах и нормативно-правовом поле трансграничного обмена данными.

В этой связи очень важно определить степень критичности всех типов информации, циркулирующей в технологическом «конвейере». В результате возрастет важность корректной и независимой оценки степени влияния факторов при категорировании объектов КИИ. Другими словами, наиболее существенной задачей является точное и корректное категорирование объекта КИИ для обоснованного отнесения его к категории значимых объектов (или иного решения), поскольку создание СОИБ в последующем опирается именно на

[1] Минцифры планирует повысить кибербезопасность СМИ [Электронный ресурс]. Режим доступа https://www.securitylab.ru/news/534728.php, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] ГОСТ Р ИСО/МЭК 17021-1-2017. Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования [Электронный ресурс]. Режим доступа https://docs.cntd.ru/document/1200146130?ysclid=la6law30im515354401, свободный. Яз. рус. (дата обращения: 20.10.2022).

[3] Банк России не верит «комфортным» аудиторам [Электронный ресурс]. Режим доступа https://www.banki.ru/news/bankpress/?id=3184616&ysclid=la8fhp2o5w364374416, свободный. Яз. рус. (дата обращения: 20.10.2022).

[4] 16 аудиторов, которые проглядели больше всего проблемных банков [Электронный ресурс]. Режим доступа https://www.rbc.ru/finances/16/12/2015/566edbf69a7947200e4430a6?ysclid=la8fikciyz21018617, свободный. Яз. рус. (дата обращения: 20.10.2022).

Таблица 3. Пример оценивания рисков без определения соответствующих активов
Table 3. Example of risk assessment without identifying the relevant assets

Актив	Риск	Вероятность	Последствия	Значимость риска
Не применимо	Запрет производителя в отношении программного обеспечения и оборудования	5	4	20
Не применимо	Прерывание сервисов коммуникаций с контрагентами	3	4	12
Не применимо	Недостаток ключевого ИТ-персонала	2	5	10
Не применимо	Сбои и отказы сетевой инфраструктуры	2	4	8
Не применимо	Внешние атаки к критичным активам	2	4	8
Не применимо	Снижение качества управления ИТ-инфраструктурой	4	2	8

результаты корректного категорирования субъектом своего множества объектов КИИ. Объектами КИИ в нормативной правовой базе Российской Федерации и некоторых международных (федеральных) стандартах называются разные сущности, соответственно, применяются различные подходы к обеспечению безопасности и защите информации объектов, рассматриваются различные критерии при оценке объектов категорирования. В качестве «сущностей» в ряде международных стандартов ISO (IEC) и, соответственно, ГОСТ Р ИСО (ГОСТ Р ИСО/МЭК) признаются активы с соответствующим методическим сопровождением — идентификацией, оцениванием имеющихся уязвимостей, выявлением актуальных УБИ, категорированием, и в качестве хорошего примера здесь можно отметить ГОСТ серии 13335-1[1]. В практике автора был пример (табл. 3), в котором для определенного объекта были сформированы риски без определения соответствующих активов (поле имело пометку «не применимо»).

При оценивании степени критичности объекта осуществим анализ игнорирования логики выполнения стандартных процедур (не определены активы, следовательно, не исследованы их свойства, соответственно, не определены присущие уязвимости, поэтому не могут быть корректно определены УБИ, и, в свою очередь, риски ИБ) может привести к серьезным ошибкам при проектировании СОИБ. В международном законодательстве осуществляется процесс категорирования, исходя из предопределенных целей безопасности (*security objectives*). Таким образом, предполагается, что ИС уже содержит определенную встроенную систему защиты (*by design*), и необходимо оперативно оценить ее достаточность, провести анализ влияния ИС и обрабатываемой информации на зависимые ИС в рамках конкретной (информационно-технологической) — экосистемы. Хорошим примером в данном контексте — учет атак по каналам поставщиков (*Supply chain attacks*), хотя и в «классическом» ISO/IEC серии 27001 (ГОСТ Р ИСО/МЭК 27001) и в ряде публикаций по прикладным аспектам обеспечения ИБ [20, 21] отражены эти базовые требования. К сожалению, примеры успешных атак говорят о том, что высший менеджмент «не видит» данных рисков и, скорее всего, причина кроется в недостаточно корректной и точной процедуре идентификации и категорирования объектов КИИ до начала построения СОИБ и обоснованного выбора множества конкретных мер защиты.

Соответственно, в международных и федеральных стандартах рассмотрено категорирование объектов КИИ как базовая процедура на этапе создания и модернизации самой ИС, а в нормативной правовой базе Российской Федерации предусматривается создание СОИБ также для уже существующего объекта (ИС, информационно-телекоммуникационная сеть или автоматизированная система управления технологическими процессами). При необходимости этот процесс может быть итерационным — последовательно оценивается существующая ИС (например, только собственная встроенная подсистема противоаварийной защиты, *Safety Instrumented System* в соответствии с ГОСТ Р МЭК серии 61508[2]), далее анализируются при необходимости дополнительные меры и средства защиты СОИБ. Критерии оптимальности для КБИС могут меняться на разных стадиях итерационного процесса в зависимости от изменения ландшафта УБИ, новых требований, оценки остаточных рисков и нормативных требований.

Заключение

Показана важность выполнения корректной и оперативной оценки требований к обеспечению безопасности объектов на стадии создания, как это предлагается в федеральных стандартах FIPS и BSI. Отмечена необходимость введения для субъектов Российской Федерации понятия «критическая информационная инфраструктура», и в настоящий момент процедуры категорирования являются технологическими и правовыми новациями. Итерационная процедура категорирования позволяет выявлять недостатки при обеспечении информационной безопасности и для созданных

[1] ГОСТ Р ИСО/МЭК 13335-1-2006 Национальный стандарт Российской Фдерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1 [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200048398?ysclid=lgxlr50yxq617100645, свободный. Яз. рус. (дата обращения: 20.10.2022).

[2] ГОСТ Р МЭК 61508-1-2012 Национальный стандарт Российской Фдерации. Функциональная безопасность систем электирических, электронных, программируемых электронных, связанных с безопасностью. Часть 1 [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200103191?ysclid=lgxlxhlbu274328778, свободный. Яз. рус. (дата обращения: 20.10.2022).

ранее компонентов в составе объектов критической информационной инфраструктуры в постоянно изменяющихся условиях функционирования и изменения технологических процессов. Именно по этой причине крайне важно реализовать полную процедуру оценки рисков и переоценки остаточных рисков. Это относится как к составу уже внедренных мер защиты (которые тоже требуется переоценивать с течением времени), так и постоянно изменяющего «ландшафта» угроз безопасности.

Создание систем обеспечения информационной безопасности для существующих объектов критической информационной инфраструктуры позволяет быстро и достаточно эффективно пройти этап категорирования для тех субъектов, которые ввели свои объекты в эксплуатацию до вступления силу Федерального закона N 187. В положительном аспекте необходимо отметить, что в Постановлении Правительства РФ указаны требования сбора и анализа статистики инцидентов и иные процедуры, описанные ранее в различных международных стандартах, что позволяет в перспективе перейти к современным методикам управления рисками информационной безопасности. Представляется рациональным продолжить дальнейшую оптимизацию процедуры категорирования объектов критической информационной инфраструктуры, совершенствование показателей критериев для сокращения времени, повышения достоверности и объективности получения финального результата. Практическая значимость выполненного исследования заключается в предложении численных оценок для категорирования объектов критической информационной инфраструктуры, что позволит повысить точность, объективность и достоверность всего процесса создания современных систем обеспечения информационной безопасности. Полученные результаты могут быть применены для современных предприятий, в том числе для объектов топливно-энергетического комплекса.

Литература

1. Смирнов Е.В. Методика оценки политической значимости угроз объекту критической информационной инфраструктуры на примере объекта инфокоммуникаций // Экономика и качество систем связи. 2020. № 2. С. 49–56.
2. Новикова Е.Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. 2019. № 4. С. 127–135. https://doi.org/10.21672/2074-1707.2019.48.4.127-135
3. Щелкин К.Е., Звягинцева П.А., Селифанов В.В. Возможные подходы к категорированию объектов критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2019. Т. 6. № 1. С. 128–133. https://doi.or g/10.33764/2618- 981X-2019-6-1-128-133
4. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Принципы и задачи асимптотического управления безопасностью критических информационных инфраструктур // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 12. С. 29–35. https://doi.org/10.24411/2072-8735-2018-10330
5. Горелик В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // Научно-образовательный журнал для студентов и преподавателей «StudNet». 2020. Т. 3. № 9. С. 1438–1448.
6. Оюн Ч.О., Попантонопуло Е.В. Объекты критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2018. № 9. С. 45–49.
7. Лившиц И.И. Экономическое обеспечение информационной безопасности: учебно-методическое пособие. СПб.: Университет ИТМО, 2021. 69 с.
8. Лившиц И.И. Нормативно-методическое обеспечение информационной безопасности: учебно-методическое пособие. СПб.: Университет ИТМО, 2021. 68 с.
9. Konyukhov V.Y., Livshitz I.I., Oparina T.A. Improving the quality of electricity in electrical supply networks of industrial enterprises // Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2021. P. 156–160. https://doi.org/10.1109/itqmis53292.2021.9642875
10. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. Industrial Systems Security Assessments study // Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2021. P. 161–164. https://doi.org/10.1109/itqmis53292.2021.9642828
11. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. A study of modern risk management methods for industrial safety assurance in the fuel and energy industry // Proc. of

References

1. Smirnov E. Methodology for assessing the political significance of threats to a CII object on the example of an infocommunication object. *Jekonomika i kachestvo sistem svjazi*, 2020, no. 2, pp. 49–56. (in Russian)
2. Novikova E.F., Khalizev V.N. The development of a threat model for critical information infrastructure facilities considering social engineering methods. *Caspian Journal: Management and High Technologies*, 2019, no. 4, pp. 127–135. (in Russian). https://doi.org/10.21672/2074-1707.2019.48.4.127-135
3. Shchelkin K.E., Zvyagintseva P.A., Selifanov V.V. Possible approaches to categorization of critical information infrastructure objects. *Interexpo GEO-Siberia*, 2019, vol. 6, no. 1, pp. 128–133. (in Russian). https://doi.org/10.33764/2618-981X-2019-6-1-128-133
4. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Principles and tasks of asymptotic security management of critical information infrastructures. *T-Comm: Telecommunications in Transport Industry*, 2019, vol. 13, no. 12, pp. 29–35. (in Russian). https://doi.org/10.24411/2072-8735-2018-10330
5. Gorelik V.Yu., Bezus M.Iu. About security of critical information infrastructure of the russian federation. *StudNet*, 2020, vol. 3, no. 9, pp. 1438–1448. (in Russian)
6. Oyun Ch.O., Popantonopulo E.V. Objects of critical information infrastructure. *Interexpo GEO-Siberia*, 2018, no. 9, pp. 45–49. (in Russian)
7. Livshitc I.I. *Economic Support of Information Security*. St. Petersburg, ITMO University, 2021, 69 p. (in Russian)
8. Livshitc I.I. *Regulatory and Procedural Support of Information Security*. St. Petersburg, ITMO University, 2021, 68 p. (in Russian)
9. Konyukhov V.Y., Livshitz I.I., Oparina T.A. Improving the quality of electricity in electrical supply networks of industrial enterprises. *Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 156–160. https://doi.org/10.1109/itqmis53292.2021.9642875
10. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. Industrial Systems Security Assessments study. *Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 161–164. https://doi.org/10.1109/itqmis53292.2021.9642828
11. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. A study of modern risk management methods for industrial safety assurance in the fuel and energy industry. *Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 165–167. https://doi.org/10.1109/itqmis53292.2021.9642791

the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2021. P. 165–167. https://doi.org/10.1109/itqmis53292.2021.9642791
12. Lontsikh P.A., Gulov A.E., Livshitz I.I., Koksharov A.V., Golovina E.Y. System-oriented analysis and classification of process control methods for software development // Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2021. P. 174–177. https://doi.org/10.1109/itqmis53292.2021.9642850
13. Breaux T.D., Gordon D.G., Papanikolaou N., Pearson S. Mapping legal requirements to IT controls // Proc. of the 6th International Workshop on Requirements Engineering and Law (RELAW). 2013. P. 11–20. https://doi.org/10.1109/RELAW.2013.6671341
14. Hale G., Lenzner R. Introducing the National Security Cyber Assistance Program (NSCAP) // Journal of Information Warfare. 2014. V. 13. N 2. P. 39–45.
15. Lam D.D., Carayannis E.G. Standard insecurity: How, why and when standards can be a part of the problem // Journal of the Knowledge Economy. 2011. V. 2. N 2. P. 234–248. https://doi.org/10.1007/s13132-010-0029-0
16. Gandhi R.A., Crosby K., Siy H., Mandal S. Gauging the impact of FISMA on software security // Computer. 2014. V. 47. N 9. P. 103–107. https://doi.org/10.1109/MC.2014.248
17. Murray A.T., Grubesic T.H. Overview of reliability and vulnerability in critical infrastructure // Critical Infrastructure: Reliability and Vulnerability. Berlin: Springer, 2007. P. 1–8. https://doi.org/10.1007/978-3-540-68056-7_1
18. Taylor L.P. Categorizing data sensitivity // FISMA Compliance Handbook (Second Edition). 2013. P. 63–78. https://doi.org/10.1016/B978-0-12-405871-2.00008-7
19. Calder A. NIST Cybersecurity Framework: A Pocket Guide. IT Governance Publishing, 2018. 78 p. https://doi.org/10.2307/j.ctv4cbhfx
20. Лившиц И.И., Соколов Е.О. Проектирование международного значимого электронного документооборота для компаний холдингового типа // Вопросы кибербезопасности. 2020. № 5(39). С. 61–68. https://doi.org/10.21681/2311-3456-2020-05-61-68
21. Басырова А.А., Лившиц И.И. Анализ методики аудита информационной безопасности предприятия с помощью аутсорсинговых компаний // Автоматизация в промышленности. 2020. № 7. С. 6–9. https://doi.org/10.25728/avtprom.2020.07.02

12. Lontsikh P.A., Gulov A.E., Livshitz I.I., Koksharov A.V., Golovina E.Y. System-oriented analysis and classification of process control methods for software development. *Proc. of the 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 174–177. https://doi.org/10.1109/itqmis53292.2021.9642850
13. Breaux T.D., Gordon D.G., Papanikolaou N., Pearson S. Mapping legal requirements to IT controls. *Proc. of the 6th International Workshop on Requirements Engineering and Law (RELAW)*, 2013,pp. 11–20. https://doi.org/10.1109/RELAW.2013.6671341
14. Hale G., Lenzner R. Introducing the National Security Cyber Assistance Program (NSCAP). *Journal of Information Warfare*, 2014, vol. 13, no. 2, pp. 39–45.
15. Lam D.D., Carayannis E.G. Standard insecurity: How, why and when standards can be a part of the problem. *Journal of the Knowledge Economy*, 2011, vol. 2, no. 2, pp. 234–248. https://doi.org/10.1007/s13132-010-0029-0
16. Gandhi R.A., Crosby K., Siy H., Mandal S. gauging the impact of FISMA on software security. *Computer*, 2014, vol. 47, no. 9, pp. 103–107. https://doi.org/10.1109/MC.2014.248
17. Murray A.T., Grubesic T.H. Overview of reliability and vulnerability in critical infrastructure. *Critical Infrastructure: Reliability and Vulnerability.* Berlin, Springer, 2007, pp. 1–8. https://doi.org/10.1007/978-3-540-68056-7_1
18. Taylor L.P. Categorizing data sensitivity. *FISMA Compliance Handbook (Second Edition)*, 2013, pp. 63–78. https://doi.org/10.1016/B978-0-12-405871-2.00008-7
19. Calder A. *NIST Cybersecurity Framework: A Pocket Guide*. IT Governance Publishing, 2018, 78 p. https://doi.org/10.2307/j.ctv4cbhfx
20. Livshitz I., Sokolov E. Designing an internationally significant electronic document flow for holding companies. *Voprosy kiberbezopasnosti*, 2020, no. 5(39), pp. 61–68. (in Russian). https://doi.org/10.21681/2311-3456-2020-05-61-68
21. Basyrova A.A., Livshits I.I. Analyzing the methodology of enterprise cybersecurity audit with the help of outsourcing companies. *Journal Automation in Industry*, 2020, no. 7, pp. 6–9. (in Rusian). https://doi.org/10.25728/avtprom.2020.07.02

Автор

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

Author

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

Статья поступила в редакцию 15.10.2022
Одобрена после рецензирования 14.02.2023
Принята к печати 23.05.2023

Received 15.10.2022
Approved after reviewing 14.02.2023
Accepted 23.05.2023