УДК 004.056

К ВОПРОСУ О КАТЕГОРИРОВАНИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

К.А. Моисеева, Р.М. Яппаров
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: критическая информационная инфраструктура, категорирование, типовые объекты, отраслевой подход.

Обеспечение безопасности критической информационной инфраструктуры (КИИ) Российской Федерации является важной задачей государственной политики в области информационной безопасности [5]. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» установил правовые основы защиты объектов критической информационной инфраструктуры. К таким объектам относятся информационные системы (ИС), информационно-телекоммуникационные сети (ИТС) и автоматизированные системы управления (АСУ) субъектов КИИ. [1]

Основным этапом обеспечения безопасности критической информационной инфраструктуры является процедура категорирования, в ходе которой определяется значимость объектов критической информационной инфраструктуры и устанавливается необходимость применения мер защиты [1]. До недавнего времени процесс категорирования регулировался Постановлением Правительства РФ от 08.02.2018 № 127, которое определяло общие правила оценки последствий компьютерных инцидентов и присвоения категорий значимости [2]. Однако существенные изменения произошли после принятия Постановления Правительства от 07.11.2025 № 1762 и Распоряжения Правительства Российской Федерации от 26 февраля 2026 №360-р [3].

Категорирование проводят субъекты КИИ в отношении принадлежащих им объектов. Категорированию подлежат объекты, соответствующие типам из перечней типовых отраслевых объектов. Этапы категорирования следующие [2]:

1. Выявление ИС, ИТС, АСУ, соответствующих типовым объектам.
2. Оценка масштаба возможных последствий компьютерных инцидентов по показателям критериев значимости.
3. Присвоение категории значимости или принятие решения об отсутствии необходимости присвоения категории [2].

Постановление Правительства РФ от 07.11.2025 № 1762 исключило понятие «критических процессов» и усилило отраслевой подход. Теперь установление соответствия объекта критериям значимости, расчет показателей и присвоение категории осуществляется в соответствии с

отраслевыми особенностями категорирования. Для объектов, которые не входят в типовые перечни, но масштаб возможных последствий компьютерного инцидента соответствует показателям значимости, субъект КИИ обязан самостоятельно присвоить категорию и направить в уполномоченный орган предложение о дополнении перечней [2].

26 февраля 2026 года было опубликовано Распоряжение Правительства РФ №360-р, утвердившее перечень типовых отраслевых объектов критической информационной инфраструктуры. Данный документ призван устранить неопределенность в вопросе определения состава объектов, подлежащих категорированию, и сформировать единую методологическую основу для субъектов КИИ различных отраслей [3]. Перечень изображен в виде таблицы и включает 397 типовых объектов, сгруппированных по отраслевому принципу: здравоохранение, наука, транспорт, энергетика и другие сферы деятельности. Для каждого типового объекта указаны типовые процессы, которые он выполняет, а так же виды деятельности субъекта КИИ с привязкой к кодам ОКВЭД [4].

Таким образом, введение Перечня типовых объектов и новые правила Постановления Правительства №1762 перевели категорирование из категории субъективных оценок в строгую отраслевую процедуру. Перечень типовых объектов будет актуализироваться в дальнейшем в соответствии с совершенствованием законодательства РФ. Дальнейшее утверждение отраслевых особенностей и конкретизация требований по защите информации позволит повысить эффективность системы, направленной на обеспечение безопасности критической информационной инфраструктуры Российской Федерации.

Список использованных источников

1. Федеральный закон от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в ред. от 07.04.2025 №58-ФЗ) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 11.03.2026).

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «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» (в ред. от 07.11.2025 № 1762) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_290595/1b445ea2ca2e30b9350044e3133a1aced3b23a6c/ (дата обращения 11.03.2026).

3. Распоряжение Правительства Российской Федерации от 26.02.2026 № 360-р «Об утверждении перечня типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL:

https://www.consultant.ru/document/cons_doc_LAW_527541/ (дата обращения 11.03.2026).

4. Правительство РФ утвердило перечень типовых объектов КИИ [Электронный ресурс] // РБК Компании. – 27 февраля 2026. – URL: https://companies.rbc.ru/news/3W11TNmuF9/pravitelstvo-rf-utverdilo-perechen-tipovyih-obektov-kii/ (дата обращения 11.03.2026).

5. Исмагилова, А. С. Теоретико-графовая интерпретация системы защиты информации / А. С. Исмагилова, И. А. Шагапов, И. В. Салов // Инженерный вестник Дона. – 2024. – № 9(117). – С. 171-179. – EDN LWCKXX.

Моисеева Карина Артемовна, студ. 4 курса ИИГУ, moiseeva_012@mail.ru
Яппаров Рауф Мидхатович, к.ю.н., доцент, доцент каф. управления информационной безопасностью, bist2002@yandex.ru

УДК 004.056.53

РАЗРАБОТКА МЕТОДИКИ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ ПРАВИЛ ДЛЯ МЕЖСЕТЕВОГО ЭКРАНА

Н. Ф. Махмутова, И. А. Ушаков, М. М. Ковцур, С. Алькаттан
Санкт-Петербургский государственный университет телекоммуникаций им проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

Ключевые слова: межсетевой экран, корпоративная сеть, автоматизация проверки правил, информационная безопасность

Обеспечение информационной безопасности в корпоративных сетях является одной из приоритетных задач для организаций любого масштаба. Ключевую роль в выполнении этих функций играют межсетевые экраны (МСЭ), которые фильтруют входящие и исходящие соединения на основе заданных правил. С ростом компании поддержание актуальности правил МСЭ становится трудоемкой задачей, а поскольку большинство обращений пользователей вызвано именно отсутствием разрешающих правил, автоматизация их проверки необходима для оперативного восстановления доступа к сервисам и обеспечения непрерывности бизнеса [1].

Логика функционирования схемы корпоративной сети строится вокруг фильтрации трафика на МСЭ: все запросы от пользователей к внешним или внутренним ресурсам проходят через него, и доступ предоставляется только при наличии соответствующего разрешающего правила. Для решения проблемы оперативного реагирования на пользовательские запросы о недоступности сервисов разработана методика автоматизированного обнаружения отсутствующих правил на межсетевых экранах. Ниже описаны ключевые этапы предлагаемой методики [2].

1. Получение и первичная обработка входных параметров от пользователя. Исходными данными для работы методики служат обращения пользователей, поступающие в службу технической поддержки.