



Чек-лист готовности к категорированию объектов КИИ

Что проверить до начала работ

ФГУП «НПП „Гамма“» · Екатеринбургский научно-технический центр

Отметьте пункты, которые уже закрыты: незакрытые — это и есть объём подготовки. Правовая основа — Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в редакции Федерального закона от 07.04.2025 № 58-ФЗ; далее — Закон № 187-ФЗ) и Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утверждённые постановлением Правительства Российской Федерации от 08.02.2018 № 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 редакции постановления Правительства Российской Федерации от 07.11.2025 № 1762; далее — Правила).

Если вы готовились по материалам прошлых лет. Перечень объектов, подлежащих категорированию, в ФСТЭК России больше не направляется, годичного срока на категорирование нет (постановление Правительства Российской Федерации от 19.09.2024 № 1281). В редакции постановления № 1762 отправная точка — не перечень процессов организации, а перечни типовых отраслевых объектов КИИ. Сроки работ, актуальность и достоверность сведений теперь отслеживают и отраслевые регуляторы — вплоть до ознакомления с объектами на месте (п. 19(2) Правил).

Порядок и сроки

1. Создание комиссии по категорированию.
2. Выявление систем, соответствующих типовым отраслевым объектам.
3. Оценка показателей значимости.
4. Оформление акта комиссии.
5. Направление сведений в ФСТЭК России — 10 дней со дня решения (по Правилам — 10 рабочих дней со дня утверждения акта).
6. Проверка ФСТЭК России — 30 дней; при возврате сведений — 10 дней на исправление.
7. Внесение в реестр значимых объектов.
8. Далее: при изменении сведений — новые сведения в течение 20 рабочих дней; пересмотр — не реже одного раза в 5 лет.

1. Организация — субъект КИИ

☐ Организация — государственный орган, государственное учреждение или российское юридическое лицо (индивидуальные предприниматели в перечне субъектов КИИ не названы), и ей на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети или автоматизированные системы управления (п. 8 ст. 2 Закона № 187-ФЗ).

☐ Системы функционируют в одной из сфер, названных в Законе № 187-ФЗ (здравоохранение, наука, транспорт, связь, энергетика, государственная регистрация прав на недвижимое имущество и сделок с ним, банковская сфера и иные сферы финансового рынка, топливно-энерге-

тический комплекс, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность), либо организация обеспечивает взаимодействие таких систем. Субъектом КИИ организацию делает сфера, в которой работают её системы, а не код вида деятельности; коды в ЕГРЮЛ — лишь признак, по которому организацию найдут и запросят у неё сведения.

☐ Найдены перечни типовых отраслевых объектов КИИ и отраслевые особенности категорирования для своей отрасли, их реквизиты зафиксированы. Категорированию подлежат системы, соответствующие типовым объектам из этих перечней; ФСТЭК России проверяет результат с учётом перечней и особенностей (п. 4 ч. 2 ст. 6, ч. 4 и 6 ст. 7 Закона № 187-ФЗ; п. 3, 5 и 6(1) Правил). Если создаваемого объекта в перечнях нет, но последствия инцидента на нём достигают показателей значимости, он тоже категоризируется, а в ФСТЭК России направляются предложения дополнить перечни (п. 22 Правил).

☐ Определён периметр: категоризирует юридическое лицо — с филиалами и обособленными подразделениями; дочерние общества — самостоятельно. С головной организацией согласовано, кто и что подаёт.

2. Комиссия по категорированию

☐ Решением руководителя создана постоянно действующая комиссия по категорированию; её возглавляет руководитель организации или уполномоченное им лицо (п. 11 и 13 Правил). В филиалах по решению руководителя могут работать отдельные комиссии — их деятельность координирует комиссия организации (п. 11(2) Правил).

☐ В состав комиссии включены специалисты по основной деятельности организации, по информационным технологиям и связи, по эксплуатации основного технологического оборудования, по промышленной безопасности, по контролю и учёту опасных веществ и материалов; работники, отвечающие за информационную безопасность, за гражданскую оборону и защиту от чрезвычайных ситуаций; если объект обрабатывает сведения, составляющие государственную тайну, — работники подразделения по её защите (п. 11 Правил).

☐ У комиссии есть регламент и сроки; за каждой системой закреплён владелец, который готовит исходные данные к назначенной дате.

3. Исходные данные

☐ Выявлены все системы, соответствующие типовым отраслевым объектам, а не только офисная ИТ-инфраструктура: автоматизированные системы управления технологическими процессами, телемеханика, диспетчеризация, учёт ресурсов, системы в аренде, у подрядчиков и в облаке. Границы каждого объекта определены: объекты не объединены искусственно и не раздроблены.

☐ По каждому объекту собраны исходные данные (п. 10 Правил): назначение, архитектура, программные и программно-аппаратные средства, связи с другими объектами и зависимость от них, доступ к сетям связи; состав обрабатываемой информации и сервисы управления, контроля и мониторинга; угрозы и данные о прошлых компьютерных инцидентах на объектах такого типа; декларация промышленной безопасности, декларация безопасности гидротехнического сооружения или паспорт безопасности объекта топливно-энергетического комплекса, если они требуются по закону; иные данные, определённые отраслевыми особенностями.

☐ От других субъектов КИИ получены данные для категорирования: если система управляет оборудованием другого субъекта — его исходные данные; если в ней используются сторонние программные и программно-аппаратные средства — данные их владельца о последствиях (п. 9 Правил). Передача данных закреплена в договоре. Категорирует тот, кому система принадлежит на законном основании, включая аренду; на подрядчика эта обязанность не переходит.

☐ Значение каждого показателя из перечня, утверждённого постановлением № 127, определено числом в единицах, заданных перечнем (число людей, территория, объекты жизнеобеспечения, государственные услуги, размер ущерба), либо обоснована его неприменимость; к значениям приложены документы-источники. Категория присваивается по наивысшему значению; если объект по одному показателю отнесён к первой категории, остальные показатели не рассчитываются (п. 6 и 14 Правил).

☐ Угрозы и возможные действия нарушителей рассмотрены по наихудшему сценарию целенаправленной компьютерной атаки; если объект зависит от другого объекта, последствия оценены и на случай его отказа (п. 14, 14(1) и 14(2) Правил).

☐ Для создаваемых объектов, в том числе при строительстве, категория определена уже при формировании требований к объекту и при необходимости уточнена при проектировании (п. 8 Правил); подача сведений по ним запланирована в два этапа: первая часть — в течение 10 рабочих дней после утверждения требований, вторая — в течение 10 рабочих дней после ввода объекта в эксплуатацию (п. 18 Правил).

4. Акт, сведения, сроки

☐ Решение комиссии оформлено актом; акт подписан членами комиссии и утверждён руководителем. Допускается единый акт на несколько объектов. Акт хранится до вывода объекта из эксплуатации или до изменения категории (п. 16 Правил).

☐ Сведения о результате категорирования направлены в ФСТЭК России в печатном и электронном виде по форме, утверждённой приказом ФСТЭК России от 22.12.2017 № 236 (в редакции приказа ФСТЭК России от 11.07.2025 № 247). Направлять их обязательно в обоих случаях — и при присвоении категории значимости, и при решении, что присваивать её не нужно. Срок по Закону № 187-ФЗ — 10 дней со дня решения (ч. 5 ст. 7 Закона № 187-ФЗ), по Правилам — 10 рабочих дней со дня утверждения акта (п. 17 и 18 Правил); ориентируйтесь на более ранний срок. В сведения входят данные об объекте, о субъекте и эксплуатирующей организации, о взаимодействии с сетями электросвязи, о программных и программно-аппаратных средствах и сертификатах средств защиты, об угрозах и нарушителях, о последствиях, о значениях показателей с обоснованием, о мерах защиты, а также доменные имена и сетевые адреса объекта, взаимодействующего с сетями связи общего пользования, в том числе с сетью «Интернет» (п. 17 Правил).

☐ Назначен ответственный, который не более чем за 10 дней устранил недостатки, если ФСТЭК России вернёт сведения с мотивированным обоснованием (ч. 8 и 9 ст. 7 Закона № 187-ФЗ), и в течение 20 рабочих дней направит новые сведения, если прежние изменились (п. 19(1) Правил).

☐ Руководитель ознакомлен с ответственностью: за непредставление сведений о категорировании, нарушение сроков или недостоверные сведения — штраф для должностных лиц от 10 до 50 тыс. руб., для организации — от 50 до 100 тыс. руб.; при повторном нарушении — от 50 до 100 тыс. руб. и от 100 до 200 тыс. руб. соответственно (ч. 1 и 3 ст. 19.7.15 КоАП РФ).

☐ Предусмотрен пересмотр — и категорий, и решений об отсутствии необходимости их присваивать: не реже одного раза в 5 лет, если отраслевыми особенностями не установлен иной срок, а также при изменении показателей значимости, их значений или отраслевых особенностей. Если категория изменилась, новые сведения направляются в ФСТЭК России (п. 21 Правил). Категория значимого объекта может быть изменена также: по мотивированному решению ФСТЭК России по итогам проверки; если объект изменился и перестал соответствовать критериям значимости; при ликвидации, реорганизации или смене организационно-правовой формы, если из-за них изменились либо утрачены признаки субъекта КИИ (ч. 12 ст. 7 Закона № 187-ФЗ).

5. Что действует уже сейчас и что начнётся после категорирования

☐ Ответственный за информирование назначен уже сейчас, до итогов категорирования: о компьютерных атаках и инцидентах все субъекты КИИ незамедлительно информируют ФСБ России (НКЦКИ — Национальный координационный центр по компьютерным инцидентам), в финансовой сфере — также Банк России (п. 1 ч. 2 ст. 9 Закона № 187-ФЗ). За непредставление информации в ГосСОПКА (государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак) или нарушение порядка и сроков — штраф для должностных лиц от 10 до 50 тыс. руб., для организации — от 100 до 500 тыс. руб. (ч. 2 ст. 19.7.15 КоАП РФ).

☐ Для значимых объектов запланированы бюджет и сроки на выполнение обязанностей субъекта КИИ: создание системы безопасности по требованиям ФСТЭК России (приказы от 21.12.2017 № 235 и от 25.12.2017 № 239), непрерывное взаимодействие с ГосСОПКА, использование программного обеспечения из реестра российского ПО и соблюдение требований к программно-аппаратным средствам (п. 1 и 5–7 ч. 3 ст. 9 Закона № 187-ФЗ). Непрерывное взаимодействие с ГосСОПКА обязательно также для государственных организаций и компаний под контролем государства (ч. 4 ст. 9 Закона № 187-ФЗ).

Дата проверки _____

Ответственный (должность, подпись, Ф. И. О.) _____

Екатеринбургский научно-технический центр — филиал ФГУП «НПП „Гамма“» помогает пройти категорирование: обследование систем, методическое сопровождение комиссии, подготовка актов и сведений для ФСТЭК России. Чек-лист носит справочный характер; нормы — по состоянию на 04.10.2026, перед началом работ сверьте действующие редакции актов.

Контакты: +7 (343) 374-84-82 · info@gammaural.ru · ekb.nppgamma.ru · ул. Студенческая, д. 51, г. Екатеринбург, Свердловская обл., 620078