СОГЛАСОВАНО
Первый заместитель
директора ФСТЭК России

В.С. Лютиков

«14» февраля 2025 г.

УТВЕРЖДАЮ
Заместитель Министра
науки и высшего образования
Российской Федерации

А.В. Омельчук

«21» февраля 2025 г.

Методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере науки

Термины и определения

В настоящих Методических рекомендациях используются следующие термины и определения:

Автоматизированная система управления	Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.
Безопасность критической информационной инфраструктуры	Состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении нее компьютерных атак.
Значимый объект критической информационной инфраструктуры	Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информационно-телекоммуникационная сеть	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.
Категорирование объектов критической информационной инфраструктуры	Установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости.
Комиссия по категорированию объектов критической информационной инфраструктуры	Постоянно действующая комиссия по формированию перечня и категорированию объектов критической информационной инфраструктуры органов государственной власти, государственных учреждений, российских юридических лиц и (или) индивидуальных предпринимателей.

Критическая информационная инфраструктура	Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.
Критический процесс	Управленческий, технологический, производственный, финансово-экономический и (или) иной процесс в рамках выполнения функций (полномочий) или осуществления видов деятельности органа государственной власти, государственного учреждения, российского юридического лица и (или) индивидуального предпринимателя, нарушение и (или) прекращение которого, может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.
Объект критической информационной инфраструктуры (Объект КИИ)	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.
Организация	Российское юридическое лицо и (или) индивидуальный предприниматель, осуществляющие свою деятельность в сфере науки, государственный орган, его подведомственная организация и иное российское юридическое лицо, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере науки.
Субъекты критической информационной инфраструктуры (Субъект КИИ)	Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере науки, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Перечень сокращений и обозначений

В настоящем документе используются следующие сокращения и соответствующие им обозначения:

АС	автоматизированная система
АСУ	автоматизированная система управления
ИС	информационная система
ИТ	информационные технологии
ИТКС	информационно-телекоммуникационная сеть
КИИ	критическая информационная инфраструктура
ОКВЭД	общероссийский классификатор видов экономической деятельности
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ФСБ России	Федеральная служба безопасности Российской Федерации

Нормативные правовые акты и документы

Настоящие Методические рекомендации разработаны с учетом требований следующих нормативных правовых актов и документов:

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Федеральный закон от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике»;

Постановление 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»;

Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

Рекомендации по структуре и содержанию методических указаний (рекомендаций), регламентирующих особенности категорирования объектов критической информационной инфраструктуры и присвоения им категорий значимости в установленной сфере, утвержденные ФСТЭК России от 28.06.2024;

Информационное сообщение ФСТЭК России от 17.04.2020 № 240/84/611 по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;

Информационное сообщение ФСТЭК России от 18.12.2021 № 240/81/2547 о порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий;

Информационное сообщение ФСТЭК России от 27.05.2024 № 240/82/1376 о порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

1. Общие положения

Настоящие Методические рекомендации разработаны на основании и в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ), 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» (далее – Постановление Правительства № 127, Правила категорирования), а также Рекомендациями по структуре и содержанию методических указаний (рекомендаций), регламентирующих особенности категорирования объектов критической информационной инфраструктуры и присвоения им категорий значимости в установленной сфере, утвержденными ФСТЭК России от 28.06.2024.

Методические рекомендации предназначены для оказания методической помощи российским юридическим лицам и (или) индивидуальным предпринимателям, осуществляющим свою деятельность в сфере науки, государственным органам, их подведомственным организациям и иным российским юридическим лицам, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере науки (далее – Организация).

Методические рекомендации применяются наряду с методическими документами, определяющими порядок категорирования объектов критической информационной инфраструктуры, разработанными органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры (ФСТЭК России), а также исполнительными органами государственной власти субъектов Российской Федерации в сфере науки и носят рекомендательный характер.

В случае, если в Организации имеются объекты КИИ которые функционируют не в сфере науки, а в иной сфере, установленной пунктом 8 статьи 2 Федерального закона № 187-ФЗ, то необходимо использовать методические указания (рекомендации), регламентирующих особенности категорирования объектов критической информационной инфраструктуры и присвоения им категорий значимости, той сферы, в которой функционирует объект КИИ.

Порядок проведения процедуры категорирования определен Правилами категорирования и включает следующие этапы:

определение принадлежности Организации к субъекту КИИ;

создание Организацией постоянно действующей комиссии по категорированию объектов КИИ;

присвоение одной из категорий значимости объекту КИИ либо принятие решения об отсутствии необходимости присвоения объекту КИИ одной из категорий значимости;

составление акта категорирования объекта КИИ и направление сведений в ФСТЭК России о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

2. Порядок определения принадлежности Организации к Субъекту КИИ в сфере науки

Организация является субъектом КИИ в сфере науки в случае (включая, но не ограничиваясь):

соответствия ч. 1 ст. 5 Федерального закона от 23.08.1996 № 127-ФЗ «О науке и государственной научно-технической политике»;

наличия в качестве основного вида деятельности в учредительных документах Организации (устав, учредительный договор) научной и (или) научно-технической деятельности и использования ОКВЭД приведенный в Приложении 1;

научная организация отнесена к одной из категорий в соответствии с п. 21 постановления Правительства Российской Федерации от 08.04.2009 № 312 «Об оценке и о мониторинге результативности деятельности научных организаций, выполняющих научно-исследовательские, опытно-конструкторские и технологические работы гражданского назначения»;

наличия в Организации на праве собственности, аренды или на ином законном основании ИС, ИТКС, АСУ, включенных в Перечень типовых отраслевых объектов КИИ, функционирующих в сфере науки.

Определение вышеуказанных критериев осуществляется на основании:

результатов инвентаризации ИС, ИТКС, АСУ, используемых Организацией;

финансово-хозяйственных документов Организации;

документов о вводе в эксплуатацию ИС, ИТКС, АСУ.

Решение постоянно действующей комиссии по категорированию объектов КИИ (далее – Комиссия) отражается в Протоколе Комиссии. Форма Протокола приведена в Приложении № 2.

В случае если в Организации отсутствуют ИС, ИТКС, АСУ в сфере науки Комиссия фиксирует эти результаты и организует хранение материалов, рассмотренных в ходе работы Комиссии.

Подведомственные Министерству науки и высшего образования Российской Федерации (далее – Минобрнауки России) Организации направляют уведомление об отсутствии объектов КИИ по форме, приведенной в Приложении № 3, непосредственно в Минобрнауки России.

Предоставление информации об отсутствии в Организации объектов КИИ или о том, что Организация не является Субъектом КИИ в ФСТЭК России в соответствии с законодательством о безопасности критической информационной инфраструктуры Российской Федерации не требуется.

3. Постоянно действующая комиссия по категорированию объектов КИИ

3.1. Формирование комиссии

Комиссия создается локальным нормативным актом (приказом или распоряжением) руководителя Организации. Локальный нормативный акт о создании Комиссии оформляется в соответствии с правилами документооборота, принятыми в Организации.

В целях регламентации и планирования деятельности Комиссии рекомендуется разработать Положение о Комиссии. Шаблон Положения о комиссии по категорированию объектов КИИ приведен в Приложении № 4.

Комиссию возглавляет руководитель Организации или уполномоченное им лицо. Уполномоченным лицом может являться заместитель руководителя Организации, в чьи полномочия входит обеспечение информационной безопасности.

3.2. Состав Комиссии

В состав Комиссии включаются:

руководитель Организации или уполномоченное им лицо;

работники Организации, являющиеся специалистами в области выполняемых функций (полномочий) или осуществляемых видов деятельности в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

работники Организации, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов КИИ;

работники подразделения по защите государственной тайны Организации (в случае, если объект КИИ обрабатывает информацию, составляющую государственную тайну);

работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники Организации, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

По решению руководителя Организации в состав Комиссии могут быть включены иные работники Организации, в том числе работники финансово-экономического подразделения Организации (обладающие знаниями и навыками, необходимыми для расчета показателей экономической значимости), а также специалисты юридического подразделения в целях проверки корректности соблюдения процедуры категорирования и оформления документов.

Включение в состав Комиссии представителей иных органов или организаций (к примеру работников организаций, имеющих лицензии ФСТЭК России или ФСБ России) законодательством не предусмотрено.

По решению руководителя Организации, имеющей филиалы, представительства, могут создаваться отдельные комиссии по категорированию объектов КИИ в этих филиалах, представительствах. Координацию и контроль деятельности таких комиссий осуществляет Комиссия Организации, имеющей филиалы, представительства.

Заседания Комиссии оформляются протоколами по форме, приведенной в Приложении № 2.

4. Определение объектов КИИ, подлежащих категорированию

Комиссия определяет объекты КИИ, подлежащие категорированию, путем выполнения следующих действий:

1. Инвентаризации ИС, ИТКС, АСУ, принадлежащих Организации на праве собственности, аренды или ином законном основании.

Комиссия определяет ИС, ИТКС, АСУ, подлежащие категорированию, в том числе с учетом Перечня типовых отраслевых объектов КИИ, функционирующих в сфере науки.

Рассматриваются ИС, ИТКС, АСУ, используемые Организацией в целях обеспечения выполнения функций (полномочий) или осуществления видов деятельности Организации.

К ИС, ИТКС, АСУ следуют относить также и сопутствующие подсистемы, работоспособность которых может напрямую или косвенно повлиять на обеспечение функционирования процессов в Организации.

В случае если объекты КИИ обеспечивают деятельность Организации, но функционируют не в сфере науки, то для их включения в список объектов КИИ, которые должны быть рассмотрены Комиссией необходимо руководствоваться перечнями типовых отраслевых объектов КИИ в иных сферах установленных пунктом 8 статьи 2 Федерального закона № 187-ФЗ.

В случае выявления ИС, ИТКС, АСУ, функционирующих в сфере науки, но не включенных в перечень типовых отраслевых объектов в сфере науки, рекомендуется провести категорирование выявленного объекта КИИ, а также направить в Минобрнауки России предложения по дополнению перечня типовых отраслевых объектов КИИ.

2. Формирования перечня всех управленческих, технологических, производственных, финансово-экономических и (или) иных процессов, протекающих при выполнении функций (полномочий) или осуществления видов деятельности Организации (далее – Перечень процессов).

3. Определение процессов нарушение или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка. Такие процессы признаются критическими процессами Организации и отражаются в отдельном документе. Рекомендованная форма Перечня критических процессов приведена в Приложении № 5.

4. На основании результатов инвентаризации, сформированных при выполнении рекомендаций пункта 1 раздела 4 настоящих методических рекомендаций, Комиссия определяет ИС, ИТКС, АСУ, используемые для обеспечения критических процессов, или осуществляющие управление, контроль или мониторинг этих критических процессов. По результатам этого этапа определяются ИС, ИТКС, АСУ, отнесенные к объектам КИИ, подлежащим категорированию.

К объектам КИИ Организации, подлежащим категорированию, имеющей филиалы, представительства, также относятся объекты КИИ филиалов, представительств, в случае если они не являются самостоятельными юридическими лицами.

5. Определение категории значимости объекта КИИ

5.1. Описание порядка присвоения категории значимости объекту КИИ либо принятия решения об отсутствии необходимости присвоения ему одной из категорий значимости

Комиссия по категорированию в ходе своей работы:

1. Рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации.

2. Анализирует угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ Организации. При рассмотрении угроз рекомендуется использовать в том числе, банк данных угроз безопасности ФСТЭК России. Комиссия по категорированию формирует перечень угроз безопасности информации с описанием возможных действий нарушителя, реализация которых может привести к возникновению компьютерных инцидентов на объекте КИИ. Перечень угроз безопасности информации может быть разработан как на основании уже имеющихся для объектов КИИ Моделей угроз безопасности информации, в том числе моделей

нарушителя, так и на основании актуализированных Моделей угроз безопасности информации.

3. Проводит оценку объектов КИИ в соответствии с показателями критериев значимости и присваивает каждому из объектов КИИ категорию, либо принимает решение об отсутствии необходимости ее присвоения.

Объекты КИИ оцениваются по показателям критериев значимости применимых к объектам КИИ в сфере науки. Перечень показателей критериев значимости, которые должны быть оценены Комиссией в обязательном порядке, приведен в Приложении № 6.

В целях обеспечения эффективного категорирования объектов КИИ, Комиссии рекомендуется руководствоваться расчетом показателей критериев значимости, применимых к объектам КИИ в сфере науки, приведенным в Приложении № 7. Показатели критериев значимости определяются исходя из параметров функционирования ИС, ИТКС, АСУ, являющихся объектами КИИ и включенных в Перечень типовых отраслевых объектов КИИ, функционирующих в сфере науки.

Оценка каждого объекта КИИ по показателям критериев значимости проводится с использованием экспертных мнений членов Комиссии по категорированию.

Перед проведением оценки рекомендуется провести оценку применимости Показателей критериев значимости к субъекту КИИ в целом, в целях исключения тех Показателей, которые явно не будут применимы ни к одному из принадлежащих Организации объектов КИИ.

При присвоении объекту КИИ категории значимости, принятые на объекте меры защиты не учитываются.

Объекту КИИ по результатам категорирования присваивается в соответствии с перечнем Показателей критериев значимости категория значимости с наивысшим значением.

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (например, территория, количество людей), оценка производится по каждому из значений Показателя критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.

5.2. Оценка масштаба возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ

При категорировании объекта КИИ необходимо определить масштаб возможных последствий в результате возникновения компьютерных инцидентов, основываясь на выявленных возможных угрозах безопасности информации, типах компьютерных атак, назначении объекта КИИ и автоматизируемого процесса. Для рассматриваемого объекта КИИ должны выбираться те типы последствий, которые могут стать следствием реализации вероятных угроз безопасности информации для данного объекта КИИ.

Полученная оценка масштаба возможных последствий должна соотноситься со значениями показателей критериев значимости и для каждого показателя должна быть определена соответствующая категория значимости.

При оценке масштаба возможных последствий в случае возникновения компьютерных инцидентов при проведении компьютерных атак на объект КИИ необходимо:

рассматривать наихудшие сценарии, учитывающие проведение

целенаправленных компьютерных атак на объекты КИИ, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба;

учитывать зависимость процессов от осуществления иных процессов, выполняемых субъектом КИИ;

учитывать зависимость функционирования одного объекта КИИ от функционирования другого объекта КИИ;

оценить возможность реализации угроз безопасности информации в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа.

В Приложении № 8 приведены предложения по проведению оценки возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ.

5.3. Описание расчета показателей критериев значимости объектов КИИ

До начала расчета показателей критериев значимости объекта КИИ Организации определяется применимость критериев значимости для оценки значимости ИС, ИТКС, АСУ Организации.

Для показателей критериев значимости объекта КИИ Организации, по которым обоснована их неприменимость, расчет показателей критериев значимости не проводится.

Расчет показателей критериев значимости объектов КИИ, установленных Постановлением Правительства № 127, проводится для каждого возможного события (инцидента), которое может возникнуть в результате реализации наихудшего сценария одной целенаправленной компьютерной атаки.

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей), оценка производится по каждому из значений показателя критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.

В случае, если ИС, ИТКС, АСУ Организации по одному из показателей критериев значимости отнесена к первой категории, расчет по остальным показателям критериев значимости не проводится.

В случае, если ИС, ИТКС, АСУ Организации не соответствует ни одному значению показателя критериев значимости, категория значимости объекту КИИ не присваивается.

В случае, если функционирование одного объекта КИИ зависит от функционирования другого объекта КИИ, оценка масштаба возможных последствий проводится исходя из предположения о прекращении или нарушении функционирования вследствие компьютерной атаки объекта КИИ, от которого зависит оцениваемый объект.

В случае, если ИС, ИТКС, АСУ Организации обрабатывают информацию, необходимую для обеспечения нескольких критических процессов Организации, и (или) осуществляют управление, контроль или мониторинг нескольких критических процессов Организации, оценка показателей критериев значимости производится для каждого критического процесса Организации, а категория значимости присваивается по наивысшему значению показателя.

6. Документация по результатам категорирования

По итогам работы Комиссии оформляются Акт о категорировании объектов КИИ и Сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

6.1. Акт о категорировании объектов КИИ

Форма Акта о категорировании объектов КИИ приведена в Приложении № 9 настоящих методических рекомендаций.

Акт о категорировании подписывается председателем и членами Комиссии по категорированию и утверждается руководителем Организации.

В случае если председатель Комиссии по категорированию и руководитель Субъекта КИИ одно и то же лицо, Акт должен содержать две его подписи: на месте подписи председателя комиссии и в поле утверждения документа.

Организация обеспечивает хранение Акта до вывода из эксплуатации объекта КИИ или до изменения категории значимости.

Направление Акта о категорировании в ФСТЭК России не требуется.

6.2. Сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий

Комиссия формирует Сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий (далее – Сведения о категорировании) по форме, приведенной в приложении № 1 к Акту категорирования (Приложение № 9).

Сведения о категорировании в течение 10 дней со дня утверждения Акта о категорировании направляются в ФСТЭК России.

Допускается оформление единого Акта о категорировании по результатам категорирования нескольких объектов КИИ, принадлежащих одному Субъекту КИИ, при этом Сведения о категорировании готовятся в отношении каждого из объектов КИИ отдельно и направляются в бумажном и электронном виде в ФСТЭК России либо ее территориальный орган.

В части Субъектов КИИ, осуществляющих деятельность в сфере науки, являющихся федеральными органами исполнительной власти, государственными корпорациями, головными организациями интегрированных структур, а также включенных в Перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 04.08.2004 № 1009, рассмотрение сведений осуществляется центральным аппаратом ФСТЭК России.

В части Субъектов КИИ, осуществляющих деятельность в сфере науки, являющихся самостоятельными юридическими лицами, дочерними, зависимыми обществами, входящими в интегрированные структуры, а также организациями, подведомственными органам власти субъектов Российской Федерации или органам местного самоуправления, рассмотрение сведений осуществляется управлением ФСТЭК России по федеральному округу, на территории которого расположены указанные Субъекты КИИ.

7. Сроки категорирования

Решение о включении сведений о значимом объекте КИИ в Реестр значимых объектов КИИ принимается в течение 30 дней со дня получения ФСТЭК России сведений от Организации (Субъекта КИИ).

Категория значимости, к которой отнесен значимый объект КИИ может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

по мотивированному решению ФСТЭК России, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ;

в случае изменения значимого объекта КИИ, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;

в связи с ликвидацией, реорганизацией Организации (Субъекта КИИ) и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки Субъекта КИИ.

Организация (Субъект КИИ) не реже чем один раз в 5 лет, а также в случае изменения Показателей критериев значимости объектов КИИ или их значений, осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий в соответствии с Правилами категорирования. В случае изменения категории значимости объекта КИИ, сведения о результатах пересмотра категории значимости направляются в ФСТЭК России. Обо всех изменениях, повлекших за собой не соответствие Сведениям о категорировании, направленных ранее в ФСТЭК России, Субъект КИИ информирует об этом ФСТЭК России и направляет актуализированные Сведения о категорировании в ФСТЭК России в течение 20 рабочих дней с момента фиксации факта изменений.

Приложение № 1
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Перечень (включая, но не ограничиваясь) ОКВЭД, используемых в сфере науки

72: Научные исследования и разработки

72.1 - Научные исследования и разработки в области естественных и технических наук

72.11 - Научные исследования и разработки в области биотехнологии

72.19 - Научные исследования и разработки в области естественных и технических наук прочие

72.19.1 - Научные исследования и разработки в области естественных наук

72.19.2 - Научные исследования и разработки в области технических наук

72.19.3 - Научные исследования и разработки в области нанотехнологий

72.19.4 - Научные исследования и разработки в области защиты информации

72.19.9 - Научные исследования и разработки в области естественных и технических наук прочие, не включенные в другие группировки

72.2 - Научные исследования и разработки в области общественных и гуманитарных наук

72.20 - Научные исследования и разработки в области общественных и гуманитарных наук

72.20.1 - Научные исследования и разработки в области общественных наук

72.20.2 - Научные исследования и разработки в области гуманитарных наук

Приложение № 2
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Протокол заседания комиссии по категорированию объектов критической информационной инфраструктуры

Форма

Протокол
заседания комиссии по категорированию объектов критической информационной инфраструктуры

_____
наименование субъекта КИИ

от «__»_____20__г.
по_____
тема заседания комиссии

Постоянно действующая комиссия по категорированию объектов критической информационной
инфраструктуры_____
наименование субъекта КИИ

в составе:

Председатель комиссии:

_____ _____
должность Фамилия Имя Отчество

Члены комиссии:

_____ _____
должность Фамилия Имя Отчество

_____ _____
должность Фамилия Имя Отчество

_____ _____
должность Фамилия Имя Отчество

рассмотрев исходные данные с целью_____
тема заседания комиссии

ОПРЕДЕЛИЛА:
1. <указываются решения комиссии по теме заседания>
2.....
3.....

Приложения: <Указываются приложения, содержащие согласованные комиссией исходные данные, результаты анализа, отчетные документы по теме заседания>.

Председатель комиссии:

_____

должность Фамилия Имя Отчество подпись

«___»_____20___г.

Члены комиссии:

_____

должность Фамилия Имя Отчество подпись

«___»_____20___г.

_____

должность Фамилия Имя Отчество подпись

«___»_____20___г.

_____

должность Фамилия Имя Отчество подпись

«___»_____20___г.

Секретарь комиссии

_____

должность Фамилия Имя Отчество подпись

«___»_____20___г.

Приложение № 3
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Уведомление об отсутствии в <название организации> объектов критической информационной инфраструктуры

Форма

Наименование органа в адрес
которого направляется Уведомление

Адрес

УВЕДОМЛЕНИЕ

_____
наименование организации

не имеет объектов критической информационной инфраструктуры в соответствии с решением комиссии по категорированию.

Приложение: Протокол заседания комиссии по категорированию объектов критической информационной инфраструктуры от «___»_____20__г. №____

_____ _____ _____
(Наименование должности руководителя (подпись) (инициалы, фамилия)
организации или уполномоченного им лица)

Приложение № 4
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Приказ о создании постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры

Форма

ПРИКАЗ № _____

«____»_____20__г. г.
Москва

О создании постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры

Во исполнение требований законодательства Российской Федерации о безопасности критической информационной инфраструктуры и на основании результатов определения основных видов деятельности _____с целью организации
Наименование организации

и проведения работ по категорированию объектов критической информационной инфраструктуры

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры, принадлежащих Организации на праве собственности, аренды или ином законном основании (далее - комиссия).

2. Председателем комиссии назначить (должность, ФИО), заместителем председателя комиссии назначить (должность, ФИО).

3. Утвердить Положение о комиссии (Приложение к Приказу).

4. В состав комиссии включить:

(должность, ФИО);

(должность, ФИО).

5. Комиссии в срок до «____»_____20__г.:

определить процессы в рамках осуществления видов деятельности Организации;

выявить критические процессы в деятельности Организации;

выявить объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

рассмотреть возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;

проанализировать угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;

оценить в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;

установить каждому из объектов КИИ категорию значимости либо принять решение об отсутствии необходимости присвоения им категорий значимости;

представить на утверждение акты по результатам категорирования;

представить на утверждение сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему категории значимости.

6. Комиссии в своей деятельности руководствоваться положениями действующих нормативных правовых актов и методических рекомендаций в сфере обеспечения безопасности КИИ.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель И.О. Фамилия

Приложение к Приказу №_____

УТВЕРЖДАЮ

_____

должность руководителя организации или уполномоченного им лица

_____

подпись руководителя организации или уполномоченного им лица	фамилия, имя, отчество руководителя организации или уполномоченного им лица

«_____»_____20___г.

дата утверждения Положения

Положение о комиссии по категорированию объектов критической информационной инфраструктуры

наименование организации

1. Общие положения

1.1. Настоящее положение о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры (далее – Положение) определяет порядок формирования и деятельности постоянно действующей комиссии по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры (далее – Комиссия).

1.2. Комиссия в своей деятельности руководствуется Конституцией Российской Федерации, федеральными законами, актами Президента Российской Федерации, Правительства Российской Федерации, в том числе Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных 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» (далее – Правила категорирования), а также настоящим Положением.

1.3. Комиссия создается в целях принятия решений об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании (наименование организации) к объектам критической информационной инфраструктуры (далее – КИИ), , с последующим установлением одной из категорий значимости объектов КИИ, либо решений об отсутствии оснований для их отнесения к объектам КИИ.

1.4. Состав комиссии утверждается приказом или распоряжением руководителя Организации.

1.5. В состав Комиссии входят:

председатель Комиссии;

члены Комиссии;

секретарь Комиссии.

1.6. Комиссия принимает решение об отнесении объектов информационной инфраструктуры Организации к объектам КИИ с последующим установлением одной из категорий значимости объектов КИИ, либо решение об отсутствии оснований для отнесения объектов информационной инфраструктуры Организации к объектам КИИ.

1.7. Заседания Комиссии по категорированию оформляются протоколами по форме, приведенной в Приложении 2 к Методическим рекомендациям по категорированию объектов КИИ, функционирующих в сфере науки.

2. Задачи Комиссии

Комиссия в ходе своей работы:

2.1. Определяет объекты КИИ, подлежащие категорированию, в том числе с учетом Перечня типовых отраслевых объектов КИИ, функционирующих в сфере науки. 2.2. Определяет процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы), в рамках выполнения функций (полномочий) или осуществления видов деятельности Организации.

2.3. Выявляет управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения Организацией функций (полномочий) в установленной сфере деятельности, а также в рамках выполнения Организацией требований законодательства о КИИ, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее – критические процессы).

2.4. Определяет объекты КИИ, обрабатывающие информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляющие управление, контроль или мониторинг критических процессов, готовит предложения для включения в перечень объектов, а также оценивает необходимость категорирования вновь создаваемых информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей.

2.5. Проводит оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры.

2.6. Рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации.

2.7. Присваивает каждому из объектов КИИ Организации одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости.

2.8. Проводит анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ.

2.9. Рассматривает ежегодные планы мероприятий по защите информации и отчеты по результатам выполненных мероприятий.

3. Организация деятельности Комиссии

3.1. Председатель Комиссии:

осуществляет руководство работой Комиссии;

ведет заседания комиссии;

утверждает повестку заседаний комиссии;

утверждает акты.

3.2. Члены Комиссии:

принимают участие в работе комиссии;

присутствуют на заседаниях комиссии;

подписывают акты и протоколы по результатам проведения заседаний комиссии.

3.3. Секретарь Комиссии:

извещает Председателя и членов Комиссии, представителей государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, присутствие которых необходимо для принятия решения Комиссией, о повестке заседания Комиссии, дате, времени и месте проведения заседания Комиссии в порядке, установленном настоящим Положением;

обеспечивает Председателя и членов Комиссии необходимыми материалами и документами;

составляет акты и протоколы работы Комиссии;

осуществляет организационно-техническое обеспечение деятельности Комиссии;

выполняет поручения Председателя Комиссии по другим вопросам, связанным с деятельностью Комиссии;

обеспечивает хранение протоколов и актов Комиссии до вывода из эксплуатации объектов КИИ, или до изменения категории значимости объекта КИИ.

3.4. Заседания Комиссии проводятся по мере необходимости, но не менее двух раз в год.

3.5. Решение о проведении заседания Комиссии принимается Председателем Комиссии по предложению, внесенному секретарем Комиссии, в том числе на основании предложений членов Комиссии.

3.6. Секретарь Комиссии в срок не позднее трех рабочих дней до даты проведения заседания направляет членам Комиссии уведомление о созыве Комиссии, содержащее повестку заседания Комиссии, сведения о дате, времени и месте проведения заседания, материалы и документы к заседанию.

В случаях, требующих оперативного созыва Комиссии, срок направления уведомлений о созыве Комиссии по решению Председателя Комиссии может быть сокращен до одного дня.

3.7. Заседания Комиссии правомочны, если на них присутствует председатель Комиссии и не менее 50% численного состава членов Комиссии.

При отсутствии кворума заседание Комиссии переносится на другую дату, определяемую Председателем Комиссии.

1.8.Заседания Комиссии проводятся Председателем Комиссии.

По результатам заседания комиссии оформляется протокол, который подписывает Председатель Комиссии и секретарь.

3.9. Все решения по рассматриваемым Комиссией вопросам принимаются открытым голосованием простым большинством голосов присутствующих на заседании членов Комиссии. При голосовании каждый член Комиссии имеет один голос. При равенстве голосов решающим является голос Председателя Комиссии.

3.10. Решения Комиссии о присвоении объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий оформляются с учетом пункта 16 Правил категорирования объектов КИИ Российской Федерации, Актом Комиссии, подписываемым всеми присутствующими на заседании Комиссии членами Комиссии и утверждаемым Председателем Комиссии.

3.11. Проект Акта Комиссии не позднее 5 календарных дней со дня проведения заседания Комиссии направляется Секретарем Комиссии всем членам Комиссии на подписание, за исключением Председателя Комиссии.

3.12. Срок подписания проекта Акта членом Комиссии не может превышать 3 рабочих дней с даты его получения от Секретаря Комиссии.

3.13. Подписанный членами Комиссии Акт, не позднее 1 календарного дня направляется Секретарем Комиссии на утверждение Председателю Комиссии.

Приложение № 5
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Перечень критических процессов, для обеспечения которых используются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления Организации

Форма

УТВЕРЖДАЮ

_____

должность руководителя организации
или уполномоченного им лица

_____

подпись руководителя организации или уполномоченного им лица	фамилия, имя, отчество руководителя организации или уполномоченного им лица

«_____»_____20___г.
дата утверждения

Перечень
критических процессов, для обеспечения которых используются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления_____

наименование Организации

№ п/п	Критический процесс	Система, с помощью которой осуществляется процесс	Тип процесса	Вид негативных последствий нарушения или прекращения процесса	Документ, в котором определен процесс
1.					
2.					
...					

Приложение № 6
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Перечень показателей критериев значимости, применимых к объектам КИИ в сфере науки

№ п/п	Показатель[1]	Обоснование применимости
Социальная значимость		
1	Причинение ущерба жизни и здоровью людей (человек)	Применим, в случае если при проведении научно-исследовательской работы (НИР), опытно-конструкторской работы (ОКР) или научно-исследовательской опытно-конструкторской работы (НИОКР) предусматривается использование потенциально опасных веществ (опасных веществ)[2], в т.ч. вредных веществ[3], опасных химических веществ[4], взрывчатых веществ[5]
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Не применим

---

[1] В соответствии с постановлением 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» (с изменениями и дополнениями) (ред. 27.09.2024).

[2] Потенциально опасное вещество; опасное вещество – вещество, которое вследствие своих физических, химических, биологических или токсикологических свойств предопределяет собой опасность для жизни и здоровья людей, для сельскохозяйственных животных и растений (ГОСТ 22.0.05-97).

[3] Вредное вещество – вещество, которое при контакте с организмом человека в случае нарушения требований безопасности может вызывать производственные травмы, профессиональные заболевания или отклонения в состоянии здоровья, обнаруживаемые современными методами как в процессе работы, так и в отдаленные сроки жизни настоящего и последующих поколений (ГОСТ 12.1.007-76).

[4] Опасное химическое вещество – химическое вещество, прямое или опосредованное воздействие, которого на человека может вызвать острые и хронические заболевания людей или их гибель (ГОСТ Р 22.2.13-2023).

[5] Взрывчатое вещество – химическое соединение или смесь веществ, способные в определенных условиях к крайне быстрому самораспространяющемуся химическому превращению с выделением тепла и образованием большого количества газообразных продуктов (ГОСТ Р 22.0.08-96).

№ п/п	Показатель[1]	Обоснование применимости
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств	Не применим
4	Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи	Не применим
5	Отсутствие доступа к государственной услуге	Не применим
Политическая значимость		
6	Прекращение или нарушение функционирования государственн ого органа в части невыполнения возложенной на него функции (полномочия)	Не применим
7	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	Применим в случае, если Организация выполняет НИР, ОКР или НИОКР в рамках международного договора
Экономическая значимость		
8	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от	Применим в случае, если Организация является: государственной корпорацией; государственным унитарным предприятием; государственной компанией; организацией оборонно-промышленного комплекса; стратегическим акционерным обществом, включенным в перечень стратегических предприятий и стратегическим акционерным обществом, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009; стратегическим предприятием, включенным

№ п/п	Показатель[1]	Обоснование применимости
	годового объема доходов, усредненного за прошедший 5-летний период)	в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009
9	Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)	Применим в случае, если Организация является: государственным органом; государственным учреждением; российским юридическим лицом; индивидуальным предпринимателем
10	Прекращение или нарушение проведения клиентами операций по осуществлению перевода денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, кредитной организацией, выполняющей функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитной организацией, значимой на рынке платежных услуг, оператором услуг платежной инфраструктуры, оказывающим услуги платежной инфраструктуры в рамках системно значимых платежных систем, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	Не применим

№ п/п	Показатель[1]	Обоснование применимости
Экологическая значимость		
11	Вредные воздействия на окружающую среду	Применим, в случае если при проведении НИР, ОКР или НИОКР предусматривается использование потенциально опасных веществ (опасных веществ), в т.ч. вредных веществ, опасных химических веществ, взрывчатых веществ
Значимость для обеспечения обороны страны, безопасности государства и правопорядка		
12	Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра	Не применим
13	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры	Применим в случае выполнения Организацией НИР, ОКР или НИОКР в рамках государственного оборонного заказа[6]
14	Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемые в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	Не применим

[6] Расчет показателя производится согласно отраслевым требованиям, регламентирующие особенности категорирования объектов критической информационной инфраструктуры, функционирующих в области оборонной промышленности, утвержденным Министерством промышленности и торговли Российской Федерации

Приложение № 7
к Методическим рекомендациям по
категорированию объектов
критической информационной
инфраструктуры, функционирующих
в сфере науки

**Расчет показателей критериев значимости,
применимых к объектам КИИ, в сфере науки**

№[7]	Показатель критериев значимости	Типовые отраслевые объекты критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Расчет показателя
1	Причинение ущерба жизни и здоровью людей (человек)	Системы, обеспечивающие автоматизацию и (или) выполнение процессов в лаборатории[8]	Значение показателя рассчитывается исходя из количества лиц, задействованных при научных исследованиях, исследованиях объектов (процессов) и обеспечении безопасности производственных процессов
		Автоматизированные системы, предназначенные для управления оборудованием с числовым программным управлением, задействованного в научных исследованиях и (или) разработках	Значение показателя рассчитывается исходя из количества лиц, задействованных в процессе изготовления изделия

[7] Нумерация показателей критериев значимости указана в соответствии с Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденным постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127

[8] Лаборатория – это Орган, который осуществляет один или несколько из следующих видов деятельности: испытания; калибровка; отбор образцов, связанный с последующими испытаниями или калибровкой (ГОСТ ISO/IEC 17025-2019)

№[7]	Показатель критериев значимости	Типовые отраслевые объекты критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Расчет показателя
		Автоматизированные системы, предназначенные для управления жизненным циклом изделия (продукции)	Значение показателя рассчитывается исходя из штатного количества, участвующих в испытаниях, производстве и (или) утилизации изделия
		Автоматизированные системы, обеспечивающие работоспособность испытательных и (или) измерительных стендов	Значение показателя рассчитывается исходя из количества лиц, задействованных при испытаниях и (или) измерениях
		Автоматизированные системы, предназначенные для управления производством	Значение показателя рассчитывается исходя из количества лиц, задействованных при научных исследованиях, исследованиях объектов (процессов) и обеспечении безопасности производственных процессов
7	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	Все типовые отраслевые объекты критической информационной инфраструктуры, функционирующие в сфере науки	Показатель ущерба определяется с учетом нарушения условий международного договора за счет снижения количества завершенных испытаний (опытов, экспериментов, измерений) за определенный промежуток времени, снижения точности (правильности, прецизионности) результатов изменений при проведении испытаний (опытов, экспериментов, измерений) или целостности, доступности информации, полученной в ходе НИР, ОКР, НИОКР, наступающих в результате совершения компьютерной атаки на категорируемый объект КИИ

№[7]	Показатель критериев значимости	Типовые отраслевые объекты критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Расчет показателя
8	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)	Все типовые отраслевые объекты критической информационной инфраструктуры, функционирующие в сфере науки	Показатель ущерба субъекту КИИ определяется снижением уровня дохода субъекта КИИ, наступающим в результате совершения компьютерной атаки на категорируемый объект КИИ
9	Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета,	Все типовые отраслевые объекты критической информационной инфраструктуры, функционирующие в сфере науки	Показатель ущерба бюджетам оценивается снижением субъектом КИИ налоговых выплат (отчислений) в бюджеты Российской Федерации, наступающим в результате совершения компьютерной атаки на категорируемый объект КИИ

№[7]	Показатель критериев значимости	Типовые отраслевые объекты критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Расчет показателя
	усредненного за планируемый 3-летний период)		
11	Вредные воздействия на окружающую среду	Системы, обеспечивающие автоматизацию и (или) выполнение процессов в лаборатории	Значение показателя рассчитывается исходя из штатного расписания лаборатории (человек)
		Автоматизированные системы, предназначенные для управления оборудованием с числовым программным управлением, задействованного в научных исследованиях и (или) разработках	Значение показателя рассчитывается исходя из количества лиц, задействованных в процессе изготовления изделия (человек)
		Автоматизированные системы, предназначенные для управления жизненным циклом изделия (продукции)	Значение показателя рассчитывается исходя из штатного количества, участвующих в испытаниях, производстве и (или) утилизации изделия (человек)
		Автоматизированные системы, обеспечивающие работоспособность испытательных и (или) измерительных стендов	Значение показателя рассчитывается исходя из количества лиц, задействованных при испытаниях и (или) измерениях (человек)
		Автоматизированные системы, предназначенные для управления производством	Значение показателя рассчитывается исходя из количества лиц, задействованных при научных исследованиях, исследованиях объектов (процессов) и обеспечении безопасности производственных процессов (человек)

№[7]	Показатель критериев значимости	Типовые отраслевые объекты критической информационной инфраструктуры (ИС, ИТКС, АСУ)	Расчет показателя
13	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры	Все типовые отраслевые объекты критической информационной инфраструктуры, функционирующие в сфере науки	Расчет показателя производится согласно отраслевым требованиям, регламентирующие особенности категорирования объектов критической информационной инфраструктуры, функционирующих в области оборонной промышленности, утвержденным Министерством промышленности и торговли Российской Федерации

Приложение № 8
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Предложения по проведению оценки возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ

1. Причинение ущерба жизни и здоровью людей (человек)

Должна оцениваться возможность причинения ущерба жизни и здоровью при проведении НИР, ОКР, НИОКР, наступающим в результате совершения компьютерной атаки на категорируемый объект КИИ. При этом должны рассматриваться следующие сценарии развития компьютерных инцидентов:

инциденты, из-за которых возможно возникновение техногенных катастроф на производстве (взрывы, утечки и разливы опасных веществ), связанных с нарушением работы объекта (нарушение параметров техпроцесса, нарушение работы или состояния исполнительных механизмов и т.д.);

инциденты, из-за которых возможно возникновение техногенных катастроф и аварий, связанных с нарушением управления, нарушением работы объекта (нарушение параметров техпроцесса, нарушение работы или состояния исполнительных механизмов и т.д.);

инциденты, из-за которых возможен ущерб потребителям продукции или услуг (производство медицинских препаратов, использование медицинского оборудования, пищевая продукция, бытовая химическая продукция, транспортные средства, топливо и т.д.), связанный с нарушением технологического процесса.

Масштаб возможного ущерба может рассчитываться как:

число человек, которые могут потенциально находиться в зоне поражения при возникновении аварии или техногенной катастрофы;

число человек, находящихся в зоне, потенциально подверженной воздействию последствий техногенной катастрофы;

число потенциальных потребителей продукции, которая может нанести вред здоровью до выявления нарушений.

При оценке возможных последствий необходимо рассматривать максимальный негативный сценарий, без учета компенсирующих защитных мер (систем противоаварийной автоматики, систем защит и т.д.), необходимо делать прогноз возможного развития аварии или сбоя без учета аварийных систем (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака не считается возможной).

2. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации

Данный критерий касается объектов КИИ, от работоспособности которых зависит реализация соответствующих договорных обязательств или выполнение

предварительных условий, требуемых для выполнения (заключения) соответствующих международных договоров.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных систем, а также нарушение доступности или целостности информации, полученной в ходе НИР, ОКР, НИОКР, наступающих в результате совершения компьютерной атаки на категорируемый объект КИИ, влекущие нарушение требований международных договоров.

Масштаб возможного ущерба оценивается на основании сведений о типе международного договора, выполнение которого зависит от рассматриваемого объекта КИИ:

договор межведомственного характера;

межправительственный договор;

межгосударственный договор.

При оценке возможных последствий необходимо рассматривать максимальный негативный сценарий, без учета компенсирующих защитных мер (межсетевое экранирование, резервирование и т.д.), необходимо делать прогноз возможного развития аварии или сбоя без учета аварийных систем (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака не считается возможной).

3. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом 4, стратегическим предприятием 4, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)

Должна рассматриваться возможность снижения уровня дохода соответствующего субъекта (государственной корпорации; государственного унитарного предприятия; государственной компании; организации оборонно-промышленного комплекса; стратегического акционерного общества, включенным в перечень стратегических предприятий и стратегического акционерного общества, утвержденного Указом Президента Российской Федерации от 4 августа 2004 г. № 1009; стратегического предприятия, включенного в перечень стратегических предприятий и стратегических акционерных обществ, утвержденный Указом Президента Российской Федерации от 4 августа 2004 г. № 1009) в случае прекращения или нарушения функционирования рассматриваемого объекта КИИ.

Данный критерий касается объектов КИИ, которые реализуют процессы, связанные с производством продукции или предоставлением услуг, являющимися источниками дохода субъекта.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных объектов, влекущие нарушение производственных процессов или процессов предоставления услуг. При оценке должны рассматриваться такие последствия как:

1) нарушение производства / предоставления услуг субъекта;

2) изменение качества, скорости, объема выпускаемой продукции, которые способны повлечь нарушение договорных обязательств, штрафные санкции

и разрыв договорных отношений.

Ущерб оценивается как прогнозируемые потери за ожидаемый период нарушения объекта в процентах от среднегодового дохода за прошедший 5-летний период:

1) выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта КИИ с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления.

2) оценивается какие процессы будут нарушены из-за нарушения работоспособности объекта КИИ и связанные с ними усредненные дневные потери дохода субъекта: суммарный доход, связанный с рассматриваемым процессом за прошедший 5-летний период / 5 / 365.

3) для оценки влияния объекта на доход субъекта рекомендуется строить дерево процессов, отражающее взаимосвязь процессов с указанием зависимости (полная, частичная и т.д.). В случае, если автоматизируемый процесс не является непосредственным источником дохода, то необходимо рассмотреть процессы, на которые он оказывает влияние и выполнение которых будет невозможно или усложнится в случае нарушения данного процесса. В случае, если объект оказывает влияние на несколько процессов, являющихся самостоятельными источниками дохода, расчет потерь должен выполняться для каждого подобного процесса.

4) рассчитывается итоговый ущерб посредством умножения максимальной оценочной длительности нарушения работоспособности объекта КИИ на суммарные дневные потери от нарушения работоспособности данного объекта КИИ.

При оценке возможных последствий необходимо рассматривать максимальный негативный сценарий, без учета компенсирующих защитных мер (межсетевое экранирование, резервирование и т.д.), необходимо делать прогноз возможного развития аварии или сбоя без учета аварийных систем или мер защиты (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака не считается возможной).

4. Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)

Должна оцениваться возможность снижения соответствующих выплат государственным органом, государственным учреждением, российским юридическим лицом, индивидуальным предпринимателем в бюджет в случае нарушения функционирования рассматриваемого объекта КИИ.

Данный критерий касается объектов КИИ, которые реализуют процессы, связанные с производством продукции или предоставлением услуг, являющимися источниками дохода субъекта, облагаемыми налогами, пошлинами, акцизами и т.д.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных объектов, влекущие нарушение производственных процессов или процессов предоставления услуг. При оценке должны рассматриваться такие последствия как:

нарушение производства / предоставления услуг субъекта;

изменение качества, скорости, объема выпускаемой продукции.

Ущерб оценивается как прогнозируемое снижение выплат в бюджет за ожидаемый период нарушения объекта КИИ в процентах от среднегодового дохода федерального бюджета за 3-летний период:

1) выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта КИИ с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления.

2) Рассчитываются средние выплаты субъекта КИИ. Необходимо запросить данные о среднегодовых выплатах субъекта в бюджет (запрашивается в бухгалтерии в соответствии с перечнем кодов видов доходов бюджетов и соответствующих им кодов аналитической группы подвидов доходов бюджетов). Необходимо рассматривать исключительно выплаты, связанные с деятельностью субъекта (производство, оказание услуг), выплаты, связанные со страховыми взносами, НДФЛ и т.д. рассматриваться не должны, так как не зависят напрямую от работоспособности объектов (если не планируется сокращение персонала из-за остановки производства). Чаще всего рассматриваются налоги на прибыль, на добавленную стоимость, акцизы, на доходы от оказания платных услуг и т.д.

3) Оценивается влияние объекта КИИ на выплаты в бюджет – для этого необходимо определить какие процессы будут нарушены из-за нарушения работоспособности объекта КИИ и их влияние на выплаты в бюджет. Для оценки влияния объекта на процессы рекомендуется строить дерево процессов, отражающее взаимосвязь процессов с указанием зависимости (полная, частичная и т.д.). В случае, если автоматизируемый процесс не является непосредственным источником отчислений в бюджет, то необходимо рассмотреть процессы, на которые он оказывает влияние и выполнение которых будет невозможно или усложнится в случае нарушения данного процесса. В случае, если объект оказывает влияние на несколько процессов, являющихся самостоятельными источниками отчислений в бюджет, расчет потерь должен выполняться для каждого подобного процесса. В случае затруднений с оценкой влияния объекта и/или процессов на выплаты в бюджет, для объектов, связанных с процессами, являющимися источниками дохода, можно рассматривать 100%-ую зависимость (остановка объекта КИИ влечет к полной остановке производства / оказания услуг и в соответствующим масштабе будет недополучена прибыль и, соответственно, не произведены выплаты в бюджет).

На данном этапе необходимо рассчитать усредненное дневное уменьшение выплат в бюджеты Российской Федерации: среднегодовые выплаты в бюджет, связанные с рассматриваемыми процессами / 365.

4) Рассчитывается итоговый ущерб посредством умножения максимальной оценочной длительности нарушения работоспособности объекта КИИ на усредненное дневное уменьшение выплат в бюджеты Российской Федерации, связанное с нарушением работоспособности объекта КИИ.

5) Итоговый ущерб оценивается в процентном соотношении к прогнозируемому годовому доходу федерального бюджета, усредненному за планируемый 3-летний период.

При оценке возможных последствий необходимо рассматривать максимальный негативный сценарий, без учета компенсирующих защитных мер (межсетевое экранирование, резервирование и т.д.), необходимо делать прогноз возможного развития аварии или сбоя без учета аварийных систем или мер защиты (за исключением вариантов, когда данные системы являются неотъемлемой

технологической частью системы, на которую атака не считается возможной).

5. Вредные воздействия на окружающую среду

Должна оцениваться возможность возникновения выбросов/сбросов/разливов вредных и загрязняющих веществ в атмосферу/водоемы/почву из-за нарушения функционирования объекта КИИ, при проведении НИР, ОКР или НИОКР.

Данный критерий касается систем управления соответствующими промышленными объектами, которые осуществляют управление процессами, связанными с производством, использованием, переработкой, утилизацией, транспортом вредных и загрязняющих веществ, а также мониторинг данных процессов (если на основании данных мониторинга могут приниматься управляющие решения).

Так как в критерии не указана рассматриваемая длительность нарушения функционирования, то рассмотрению подлежит в том числе кратковременные / разовые факты выбросов / сбросов / разливов, достигающих соответствующего масштаба.

При этом должны рассматриваться следующие сценарии развития компьютерных инцидентов:

инциденты, из-за которых возможно возникновение техногенных катастроф на производстве (взрывы, утечки и разливы опасных веществ);

инциденты, связанные с нарушением работы объекта (нарушение параметров техпроцесса, нарушение работы или состояния исполнительных механизмов и т.д.).

В соответствии с разъяснениями ФСТЭК России, необходимо рассматривать максимальный негативный сценарий, без учета компенсирующих мер (систем противоаварийной автоматики, систем защит и т.д.). То есть, стоит делать прогноз возможного развития аварии или сбоя без учета аварийных систем (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака в целом не рассматривается). Пример: системы противоаварийной защиты не рассматриваются как фактор, снижающий риск. Физические блокировки и ограничители можно принимать в расчет.

Масштаб возможного ущерба оценивается относительно:

территории, на которой окружающая среда может подвергнуться вредным воздействиям;

количества людей, которые могут быть подвержены вредным воздействиям (тыс. человек).

6. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры

Должна оцениваться вероятность снижения объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции), а также увеличение времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовление единицы продукции) при прекращении и (или) нарушении функционирования объекта КИИ, в случае выполнения НИР, ОКР или НИОКР в рамках государственного оборонного заказа.

Приложение № 9
к Методическим
рекомендациям по
категорированию объектов
критической информационной
инфраструктуры,
функционирующих в сфере
науки

Акт о категорировании объекта КИИ

Форма

УТВЕРЖДАЮ

_____
должность руководителя организации
или уполномоченного им лица

_____
подпись руководителя организации или уполномоченного им лица | фамилия, имя, отчество руководителя организации или уполномоченного им лица

«_____»_____20___г.
дата утверждения

АКТ
о категорировании объекта (-ов) критической информационной инфраструктуры
наименование объекта КИИ

На основании приказа от «___» _____20____ г. №_____комиссия в составе:

председатель комиссии: _____
(роль, должность, фамилия, инициалы)

члены комиссии: _____
(роль, должность, фамилия, инициалы)
_____

в соответствии с требованиями пункта 4 статьи 7 Федерального закона от 26.07.2017 № 187-ФЗ, пункта 2 постановления Правительства Российской Федерации от 08.02.2018 № 127 провела категорирование объекта критической информационной инфраструктуры *(наименование объекта).*

В ходе работы комиссия по категорированию использовала имеющиеся данные об объекте критической информационной инфраструктуры *(наименование объекта)*:

1. Сведения об объекте критической информационной инфраструктуры.
2. Сведения о субъекте критической информационной инфраструктуры.
3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи.
4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры.
5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры.
6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры.
7. Возможные последствия в случае возникновения компьютерных инцидентов.

На основании результата анализа значений показателей критериев значимости объекта критической информационной инфраструктуры в соответствии с постановлением Правительства Российской Федерации от 08.02.2018 № 127 объекту критической информационной инфраструктуры *(наименование объекта)* присвоена категория_____.

Сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, сведения о возможных последствиях в случае возникновения компьютерных инцидентов, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры приведены в приложении 1 к настоящему акту.

Председатель комиссии: (ФИО, подпись)

Члены комиссии: (ФИО, подпись)

(ФИО, подпись)

(ФИО, подпись)

(ФИО, подпись)

Приложение 1 к акту категорирования

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1. Сведения об объекте критической информационной инфраструктуры

Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	
Назначение объекта	
Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктуры

Наименование субъекта	
Адрес местонахождения субъекта	
Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	
Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта	

Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
Наименование оператора связи и (или) провайдера хостинга	
Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

Наименование лица, эксплуатирующего объект	
Адрес местонахождения лица, эксплуатирующего объект	
Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	

ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	
Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются)	
Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	

6. Сведения об угрозах безопасности информации и категориях 5 нарушителей в отношении объекта критической информационной инфраструктуры

Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	
Основные угрозы безопасности информации или обоснование их неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости

Категория значимости, которая присвоена объекту либо информация о не присвоении объекту ни одной из таких категорий	
Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	
Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	

Перечень показателей критериев значимости и их значения

№	Показатель	Критерий значимости	Обоснование
	Социальная значимость		
1.	Причинение ущерба жизни и здоровью людей (человек)		
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:		
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;		
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)		

№	Показатель	Критерий значимости	Обоснование
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:		
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;		
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)		
4.	Прекращение или нарушение функционирования сети связи, оцениваемые:		
	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;		
	б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)		
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)		
Политическая значимость			
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)		
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации		
Экономическая значимость			
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства		

№	Показатель	Критерий значимости	Обоснование
	и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)		
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого:		
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);		
	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);		
	в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)		
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)		

№	Показатель	Критерий значимости	Обоснование
Экологическая значимость			
11.	Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:		
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;		
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)		
12.	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра		
13.	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:		
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);		
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)		
14.	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)		

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	

(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)	(подпись)	(инициалы, фамилия)