МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Категорирование объектов критической информационной инфраструктуры

187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Редакция	v 2.2	19.08.2020
Размещение	https://step.ru/innovations/kriticheskaya-informatsionnaya-infrastruktura/	

Оглавление

Введение

Настоящий документ содержит методические рекомендации по проведению категорирования объектов критической информационной инфраструктуры (КИИ) в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Данная Методика разработана специалистами компании СТЭП ЛОДЖИК и основана на требованиях законодательства и опыте, полученном при взаимодействии с организациями, функционирующими в областях, на которые распространяются требования законодательства.

Наша компания обладает компетенцией для реализации проектов любой сложности, но, вместе с тем, мы осознаем, что некоторые решения не могут быть приняты исполнителем за Клиента. Так как, в соответствии с законодательством, вся ответственность за результаты категорирования объектов КИИ ложится на их владельцев, мы хотим помочь нашим Клиентам получить всю информацию по данному вопросу и принять лучшие решения. Мы уверены, что владельцы объектов КИИ должны лучше других знать особенности своих систем, а имеющийся опыт говорит о том, что любое обследование и сбор информации для категорирования в конечном счете сводится к сбору данных у владельцев систем.

В данной Методике мы постарались собрать информацию, необходимую для самостоятельного сбора данных, их анализа и принятия решений по категорированию объектов КИИ. Это позволит нашим Клиентам:

- выполнить часть требований законодательства собственными силами, сэкономив бюджет;
- осознанно принять ответственность за объекты КИИ, как того требует закон;
- более точно определить бюджет и сроки работ для следующих этапов, понимая перечень и категории объектов защиты;
- реализовать требования по категорированию в срок, благодаря отсутствию необходимости заключения дополнительных договоров, обследований сторонними компаниями и т. д.

Мы понимаем, что данный документ не может содержать ответы на все вопросы, так как разнообразие видов деятельности и специфичность разных систем слишком велика, чтобы сделать универсальный и однозначный алгоритм принятия решений. Поэтому мы постараемся ответить на все Ваши вопросы по

категорированию объектов КИИ или по использованию данного документа. Вы можете использовать данный контакты для связи:

Тел.: +7 (495) 775-3120
security@step.ru
Автор документа – Пащенко Денис

Методика является справочным руководством и может быть использована организациями для самостоятельного проведения работ по категорированию принадлежащих им объектов критической информационной инфраструктуры.

Данная методика была разработана при консультационной поддержке представителей ФСТЭК России.

! **Мы постоянно отслеживаем изменения в законодательстве и комментарии регуляторов. На основании этих данных мы планируем вносить изменения в данный документ и отправлять их нашим партнерам.**
Если Вы получили данный документ не от нашей компании, то рекомендуем обратиться по указанному адресу с запросом последней версии.

Используемые 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 информации — состояние защищённости информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

безопасность КИИ — состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

вредоносная программа — программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа к информации и или деструктивного воздействия на информацию или ресурсы информационной системы нарушение их целостности и/или доступности;

государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

государственная информационная система — федеральная информационная система или региональная информационная система, созданная на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях;

гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

доступ к информации — возможность получения информации и ее использования;

доступность информации — состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

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;

инцидент информационной безопасности — одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности;

компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

компьютерный инцидент — факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

критическая информационная инфраструктура — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

нарушитель безопасности информации — физическое лицо, случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах;

несанкционированный доступ к информации — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание — Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем;

обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

объект критической информационной инфраструктуры — информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры;

оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

субъекты критической информационной инфраструктуры — 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 здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

угроза безопасности информации — совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации;

целостность информации — состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и или непреднамеренного воздействия на нее.

Используемые сокращения

АСУ	Автоматизированная Система Управления
АСУ ТП	Автоматизированная Система Управления Технологическим Процессом
ИС	Информационная Система
ИТС	Информационно-Телекоммуникационная Сеть
КИИ	Критическая Информационная Инфраструктура
КСПД	Корпоративная Сеть Передачи Данных
ЛВС	Локальная Вычислительная Сеть
ОКВЭД	Общероссийский классификатор видов экономической деятельности
РФ	Российская Федерация
ФЗ	Федеральный Закон
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦОД	Центр Обработки Данных

1 Общая информация

01 января 2018 вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — 187-ФЗ), регулирующий отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В соответствии с требованиями Закона, субъекты КИИ должны присвоить одну из категорий значимости принадлежащим им объектам КИИ. Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

Критерии значимости, показатели их значений, а также порядок осуществления категорирования определены в Постановлении Правительства РФ 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» (далее — 127ПП).

В соответствии с требованиями 187-ФЗ, субъект КИИ должен направить сведения о результатах категорирования своих объектов КИИ во ФСТЭК России (Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ). Форма направления сведений определена приказом ФСТЭК России от 22 декабря 2017 г. № 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».

В соответствии с Постановлением Правительства РФ от 13 апреля 2019 г. N 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127»:

- государственные органы и государственные учреждения, являющиеся субъектами КИИ, **должны** утвердить до 1 сентября 2019 г. перечень объектов КИИ, подлежащих категорированию;
- юридическим лицам и индивидуальным предпринимателям, являющимся субъектами КИИ, **рекомендуется** утвердить до 1 сентября 2019 г. перечень объектов КИИ, подлежащих категорированию.

Крайним сроком завершения категорирования является 1 сентября 2020 г.

На текущий момент согласовываются изменения в КоАП РФ, определяющие ответственность за нарушение сроков категорирования и порядка категорирования. Нарушение порядка категорирования объектов КИИ РФ, влечет наложение административного штрафа:

- на должностных лиц - от десяти тысяч до пятидесяти тысяч рублей;
- на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

Непредставление или нарушение порядка либо сроков представления в ФСТЭК РФ, сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, влечет наложение административного штрафа:

- на должностных лиц - от десяти тысяч до пятидесяти тысяч рублей;
- на юридических лиц - от пятидесяти тысяч до ста тысяч рублей.

2 Общий порядок работ

Рисунок 1 – Общий порядок работ по категорированию объектов КИИ

3 Определение принадлежности к субъектам КИИ

Данный этап не относится непосредственно к категорированию объектов КИИ, но приведен в данном документе, так как это первый вопрос, с которым приходится столкнуться организациям и зачастую он вызывает самые большие затруднения.

В соответствии с определением в 187-ФЗ, субъект КИИ — это:

1) государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере:

- здравоохранения[1],
- науки,
- транспорта,
- связи[2],
- энергетики[3],
- банковской сфере и иных сферах финансового рынка,
- топливно-энергетического комплекса,
- атомной энергии,
- оборонной промышленности,
- ракетно-космической промышленности,
- горнодобывающей промышленности,
- металлургической промышленности,
- химической промышленности;

[1] Для субъектов, относящихся к сфере здравоохранения рекомендуется использовать документ «Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения», Приказ Министерства здравоохранения Московской области № 1123 от 20.08.2020 (об утверждении Методических рекомендаций) и Методические рекомендации по определению объектов КИИ и категорий значимости объектов КИИ в медицинских учреждениях Департамента здравоохранения города Москвы.

[2] Для субъектов, являющихся операторами связи рекомендуется использовать документ «Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи».

[3] Для субъектов, работающих в сфере ТЭК рекомендуется использовать документ «Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса». Настоящая методика может быть использована дополнительно в качестве справочного руководства.

2) российское юридическое лицо и (или) индивидуальный предприниматель, который обеспечивает взаимодействие указанных систем или сетей.

Рассмотрение варианта, когда субъект является владельцем систем, приводится в разделе 3.1.

Рассмотрение варианта, когда субъект обеспечивает взаимодействие систем, приводится в разделе 3.2.

3.1 Субъекты КИИ, которым принадлежат системы, работающие в сферах КИИ

В данном разделе в качестве субъекта КИИ рассматриваются организации (государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели), которым принадлежат объекты КИИ.

Входная информация:

1) учредительные документы, устав, иные положения организации, где прописаны виды деятельности (дополнительно, о видах деятельности организации можно узнать из выписки ЕГРЮЛ/ЕГРИП);
2) лицензии, сертификаты и иные разрешительные документы на виды деятельности;
3) предварительные сведения о наличии систем, работающих в областях деятельности, рассматриваемых Законом.

Участники процесса:

1) руководитель Организации;
2) руководители функциональных подразделений.

Результат:

1) решение о признании организации субъектом КИИ (или об отсутствии такой необходимости);
2) перечень областей деятельности, рассматриваемых 187-ФЗ, в которых организация функционирует, осуществляет деятельность или выполняет функции (полномочия) организация;
3) предварительный перечень объектов КИИ.

Схема процесса

Общий порядок принятия решения о признании организации субъектом КИИ, описывающийся в данном разделе, приведен на Рисунке 2.

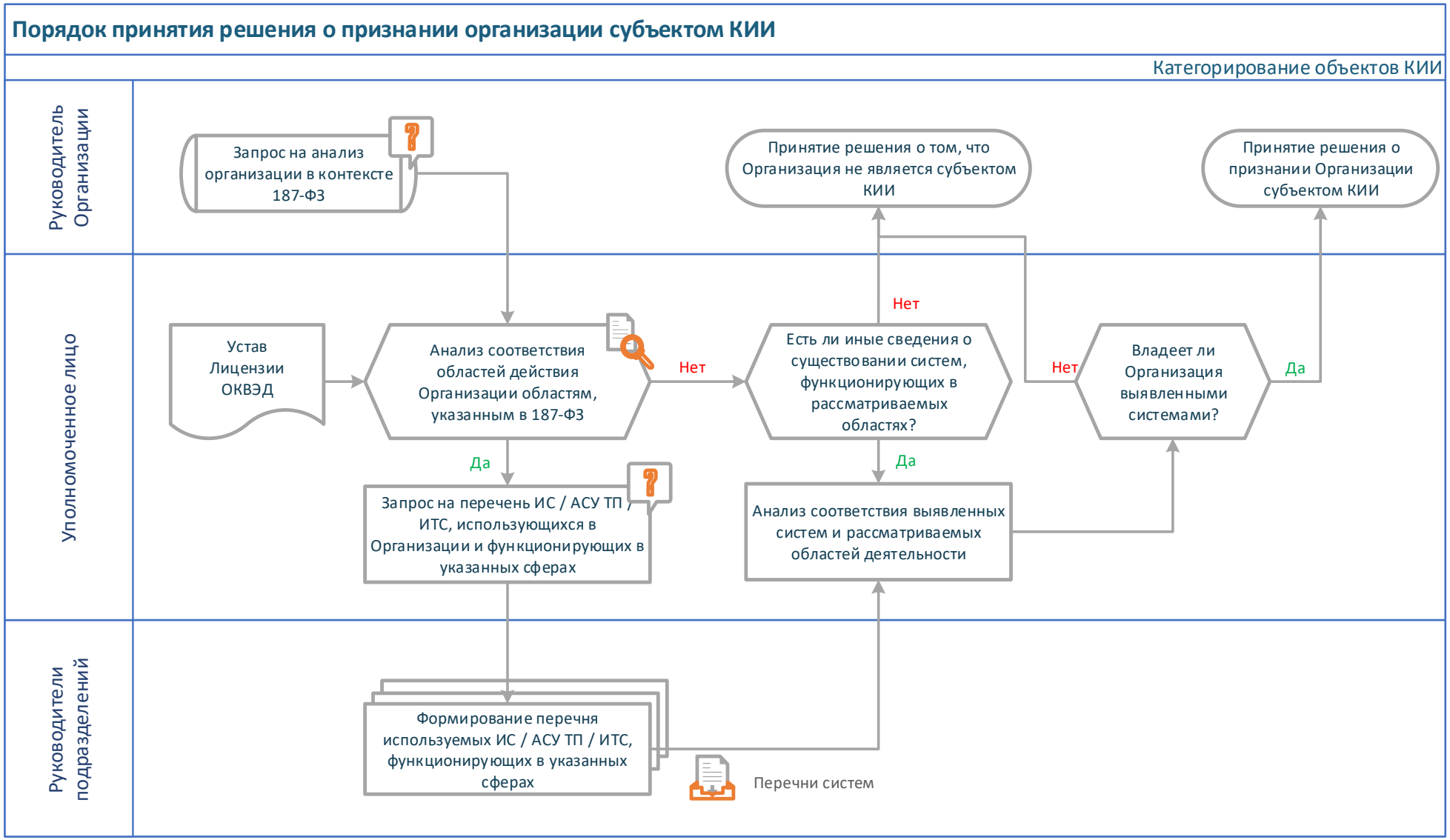

Рисунок 2 – Порядок принятия решения о признании организации субъектом КИИ

Описание процесса

В 187-ФЗ установлены 13 сфер (областей деятельности), которые подпадают под его область действия. При этом, по определению, к субъектам КИИ относятся те организации, которые владеют объектами, функционирующими в указанных сферах, а не организации, работающие в данных областях (ФЗ-187 Статья 2, п.8).

! В соответствии с разъяснениями ФСТЭК России, достаточным фактом для признания организации субъектом является сочетание следующих факторов:
- организация работает в одной из указанных сфер;
- организация владеет какими-либо ИС, АСУ, ИТС.
То есть предлагается отталкиваться от сферы работы организации, а не от области функционирования систем. Этот подход упраздняет все шаги, приводимые далее в этом подразделе и в случае выполнения данного условия организация признается субъектом КИИ.

Ситуация, когда организация работает в одной из указанных областей, но не имеет соответствующих систем, является скорее исключением из правил, поэтому со стороны ФСТЭК России был предложен подход, основанный на определение сферы деятельности организации в соответствии с:

- общероссийским классификатором видов экономической деятельности (ОКВЭД) и каталогом организаций России;
- учредительными документами, уставом или иными положения организации, где прописаны основные виды деятельности (дополнительно, о видах деятельности организации можно узнать из выписки ЕГРЮЛ/ЕГРИП).

Соответственно, если в любом из данных источников присутствует указание на рассматриваемые сферы деятельности, то, скорее всего, организация является субъектом КИИ. Таким образом, можно изучить сведения об областях деятельности, в которых работает организация и, если в их перечне есть область, входящая в область действия Закона, то уточнить наличие хотя бы одной ИС / АСУ / ИТС, принадлежащей организации и работающей в рассматриваемой сфере.

В качестве рекомендованного подхода предлагается следующая последовательность шагов:

1. В уставе организации / кодах ОКВЭД выявляется деятельность, соответствующая областям, подпадающим по 187-ФЗ.
2. От имени руководителя организации направляется запрос всем руководителям подразделений (и далее по уровням — от руководителей верхнего уровня к нижним)

об анализе используемых систем и предоставлении перечня систем, работающих в рассматриваемой области (областях).

Иначе говоря, нужно ответить на вопрос: **«Есть ли системы, используемые для реализации соответствующего вида деятельности, указанного в уставе или ОКВЭД?»**

3. Осуществляется дополнительный анализ полученных результатов на предмет принадлежности данных систем Организации (право собственности, аренда, договор пользования, хозяйственного ведения, право оперативного управления и т. д.).

! В соответствии с уточнениями ФСТЭК России принадлежность субъекту должна пониматься как явное право собственности, аренда, а также любое иное законное право на использование объекта КИИ.

4. Если выявлена система, удовлетворяющая указанным параметрам, то принимается решение о признании организации субъектом КИИ.

! На данном этапе нет цели составления полного перечня систем — достаточно будет даже одной, подходящей под указанные критерии.

Пример 1

1. *В уставе Организации определено, что Организация оказывает транспортные услуги и грузоперевозки.*
2. *Руководитель Организации рассылает соответствующие запросы руководителям департаментов с просьбой определить наличие систем, которые задействованы в автоматизации предоставляемых транспортных услуг.*
3. *В подразделениях организации осуществляется сбор информации / инвентаризация / обследование, в рамках которых выявлены системы, функционирующие в указанной сфере: система автоматизации движения, система учета и контроля трафика, система продажи и учета билетов, система планирования движения, система учета грузоперевозок и т. д.).*
4. *Осуществляется анализ принадлежности выявленных систем Организации, на основании которого определяется, что используемые системы автоматизации движения, учета и контроля трафика, а также планирования движения являются собственностью Организации.*

5. *На основании собранной информации принимается решение о признании Организации субъектом КИИ и выявленные данные о системах используются в качестве начальных данных для формирования перечня объектов КИИ.*

Пример 2

Проектно-конструкторская организация, работающая в сфере науки, в соответствии с 127-ФЗ «О науке и государственной научно-технической политике», и обладающая собственной ИС для автоматизации, учета проектов и работы сотрудников (относится к сфере науки).

Рассматриваемая организация ***является субъектом КИИ.***

Пример 3

Организация является владельцем электростанции и соответствующего оборудования. Также существует Региональное диспетчерское управление СО ЕЭС, которое владеет собственным оборудованием мониторинга и управления, взаимодействующим с оборудованием станции.

В данном случае обе организации являются ***субъектами КИИ, обладающими своими объектами КИИ.***

Какие могут быть исключения, на которые стоит обратить внимание?

1) **Организация не занимается рассматриваемой деятельностью**, в соответствии с приведенными классификаторами и документами, **но ей принадлежат системы, функционирующие в указанной сфере.**

Пример 1

Организация №1 не работает непосредственно в рассматриваемых областях, но владеет специализированной ИС и предоставляет ее по подписке в виде облачного сервиса - Организация №1 не будет признана субъектом КИИ.

Но, часто получается, что подобный сервис предоставляется некой другой организации - Организация №2, которая непосредственно работает в одной из рассматриваемых сфер и использует его в целях реализации своей деятельности. В данном варианте Организация №2 будет являться субъектом

КИИ, а поставщик облачного сервиса (Организация №1) должен будет выполнять требования безопасности, определяемые потребителем услуг по результатам категорирования.

Пример 2

Организация не работает непосредственно в сфере транспорта, но владеет системами, связанными с рассматриваемыми областями (продажа билетов на транспорт). ***Организация может быть признана субъектом КИИ*** *по формальным признакам. Для принятия окончательного решения рекомендуется направить соответствующий запрос в ФСТЭК России с детальным описанием ситуации.*

2) **Организация работает в рассматриваемых областях, но не имеет специализированных систем, работающих в указанных сферах**

Такие организации рассматривается как субъекты КИИ, не имеющие **значимых** объектов КИИ.

Пример

Организация, осуществляющая подготовку научных работников — центр дополнительного профессионального образования (относится к сфере науки в соответствии с 127-ФЗ «О науке и государственной научно-технической политике»).

В организации может не быть систем, функционирующих в сфере науки.

Q&A	**Мы провели анализ своей организации и пришли к выводу, что мы не являемся субъектом КИИ. Нужно ли готовить какое-то заключение и передавать его во ФСТЭК России?**

Нет, законодательством не предусмотрено подобное уведомление и регуляторы его не требуют. Для собственного спокойствия, на случай внезапных вопросов или проверок, можно подготовить формализованный акт в свободной форме, содержащий информацию, что комиссия или иное уполномоченное лицо рассмотрели вопрос актуальности требований 187-ФЗ, проверили Организацию на данный предмет, не выявили систем, функционирующих в указанных сферах, и приняли решение об отсутствии необходимости реализации требований 187-ФЗ.

3.2 Субъекты, обеспечивающие взаимодействие объектов КИИ

В данном разделе в качестве субъекта КИИ рассматриваются организации (российские юридические лица и (или) индивидуальные предприниматели), которые обеспечивают взаимодействие объектов КИИ.

Входная информация

1) Сведения о предоставляемых услугах сторонним организациям;
2) Договорная документация с организациями, которым предоставляются услуги.

Результат

1) Решение о признании организации субъектом КИИ (или об отсутствии такой необходимости);
2) Предварительный перечень объектов КИИ.

Участники процесса

1) Руководитель организации;
2) Руководители функциональных подразделений;
3) Представители организаций, которым оказываются услуги.

Описание процесса

В качестве обеспечения взаимодействия объектов КИИ может рассматриваться:

- предоставление и организация каналов информационного обмена (выделенные каналы доступа, а также локальные сети связи, например, в ЦОД);
- предоставление телекоммуникационных услуг, в рамках которых осуществляется взаимодействие объектов КИИ;
- предоставление иных информационных услуг для обеспечения взаимодействия с объектами КИИ.

Частными случаями таких субъектов являются операторы систем и сетей связи, обеспечивающие взаимодействие конкретных объектов, являющихся объектами КИИ. Для данных лиц ответственность за обеспечение взаимодействия объектов КИИ указывается в документации на системы/каналы связи, а также в их обязанностях.

В более неопределенных случаях, когда Организация предоставляет вычислительные мощности и каналы связи для широкого круга заказчиков, детальной информации о том, что инфраструктура может использоваться для организации

взаимодействия КИИ, может не быть. Однако, незнание данной информации не освобождает организацию от ответственности.

В качестве рекомендованного подхода предлагается следующий сценарий:

1. Провести анализ наличия объектов инфраструктуры, находящейся в собственности Организации, которая используется в интересах сторонних лиц и для организации информационного взаимодействия систем, не принадлежащих самой Организации.
2. В случае выявления соответствующих объектов инфраструктуры, сделать запрос владельцам сторонних систем о признании данных систем объектами КИИ. В случае положительного ответа, Организация признается субъектом КИИ.
3. В случае наличия инфраструктуры Организации, которая используется для информационного обмена сторонними системами, делается запрос владельцам данных систем об их принадлежности к субъектам КИИ. В случае положительного ответа, делается уточнение использования предоставляемой инфраструктуры для организации взаимодействия объектов КИИ. В случае положительного заключения Организация признается субъектом КИИ.
4. Организация далее рассматривает свою инфраструктуру (или ее часть, непосредственно задействованную в обеспечении взаимодействия объектов КИИ) в качестве объекта КИИ.

Пример 1

Организация владеет и обслуживает ЦОД, в котором размещаются ИС третьих сторон.

В рамках инвентаризации/запроса информации выявлено, что некоторые из размещаемых в ЦОД систем относятся к объектам КИИ. Программно-аппаратное обеспечение компонентов ИС является собственностью третьих сторон. При этом, для взаимодействия между данными объектами КИИ, а также с внешними системами и пользователями используются каналы передачи данных и коммутационное оборудование ЦОД, которые принадлежат Организации.

*В данном случае **Организация является субъектом КИИ**, как обеспечивающая взаимодействие объектов КИИ. Часть инфраструктуры Организации,*

непосредственно задействованная в обеспечении взаимодействия объектов КИИ, должна рассматриваться в качестве объекта КИИ.

Пример 2

Организация предоставляет услуги технической поддержки и сопровождения группе компаний, занимающихся нефтедобычей.

Работники Организации администрируют ИС, ИТС и АСУ компаний, являющихся объектами КИИ, управляют сетевыми компонентами, отвечают за работоспособность и взаимодействие систем.

В данном случае Организация ***не является субъектом КИИ****, так как ее работники обеспечивают «поддержку» работоспособности систем, но фактически взаимодействие объектов КИИ обеспечивается программно-аппаратными компонентами, находящимися в собственности самих компаний, а не Организации.*

4 Создание комиссии по категорированию

Входная информация:

1) Организационная структура Организации.

Участники процесса:

1) Руководитель организации;
2) Руководители функциональных подразделений.

Результат:

Постоянно действующая комиссия по категорированию объектов КИИ.

Описание процесса

Для проведения мероприятий по категорированию в соответствии с п. 11 127ПП решением руководителя субъекта КИИ создается постоянно действующая комиссия по категорированию. Проект Приказа по созданию комиссии по категорированию объектов КИИ приведен в Приложение 1.

В состав комиссии, в соответствии с 127ПП, должны включаться лица, приведенные в таблице 1.

Таблица 1 – Состав комиссии по категорированию

№	Участники, в соответствии с 127ПП	Уточнение и примеры
1.	Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо	• Руководитель • Заместитель • Директор по безопасности иное аналогичное лицо
2.	Работники субъекта критической информационной инфраструктуры, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и 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	В данном пункте подразумевается несколько категорий: 1) Руководители критичных направлений деятельности, процессы которых автоматизируются ИС / АСУ; 2) Руководители ИТ-подразделения; 3) Руководитель отдела автоматизации (АСУ ТП) — в случае наличия; 4) Ответственный за промышленную безопасность на предприятии — в случае наличия; 5) Ответственный за контроль за опасными веществами и материалами — в случае наличия.
3.	Работники субъекта критической информационной инфраструктуры, на которых возложены функции обеспечения безопасности (информационной безопасности)	Руководитель ИБ-подразделения (администратор ИБ в случае отсутствия выделенного подразделения). В соответствии с требованиями 235 Приказа ФСТЭК функциональная единица, отвечающая за ИБ, должна быть

	объектов критической информационной инфраструктуры	выделенной, то есть администраторы ИТ или Отдел АСУ ТП не может отвечать за обеспечение ИБ.
4.	Работники подразделения по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну)	Руководитель подразделения по защите государственной тайны — в случае наличия
5.	Работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций	Руководитель Отдела по ГОиЧС — в случае наличия
6.	Иные работники по решению Руководителя субъекта КИИ	Иные работники по решению Руководителя субъекта КИИ

Q&A	**Возможно ли включение в комиссию по категорированию представителей проектной/подрядной организации, которые реализуют проекты по защите КИИ?**
Привлечение сторонних лиц в законодательстве не регламентировано, явного запрета нет, однако, так как создается постоянно действующая комиссия, данный вариант будет проблематичным в будущем.	

В случае, если в состав организации входит филиальная сеть, то рассматривается 2 основных варианта:

1. *Филиалы являются самостоятельными юридическими лицами.*

В соответствии с законодательством, обязанности и ответственность ложится непосредственно на субъекты КИИ, в данном случае отдельных юридических лиц. Но очевидно, что головная компания так или иначе должна участвовать в процессе категорирования и дальнейшей реализации требований 187-ФЗ, накладываемых на свои филиалы / «дочки» и формировать единую политику по защите активов.

Оптимальным решением будет включение в состав всех частных комиссий, создаваемых в каждом субъекте КИИ, ответственного (ответственных) со стороны головной организации или согласование принимаемых решений комиссией головной организации в иной форме. Данное решение позволит обеспечить согласованный подход и принятие решений, а также контроль реализации всех необходимых процедур.

2. *Филиалы являются подразделениями организации в рамках единого юридического лица.*

В соответствии с п. 11.2 127ПП, по решению руководителя субъекта КИИ, имеющего филиалы, представительства, могут создаваться отдельные комиссии по категорированию объектов КИИ в этих филиалах, представительствах. При этом общую координацию и контроль деятельности комиссий по категорированию в филиалах должна осуществлять комиссия по категорированию субъекта КИИ (юридического лица в целом).

Q&A	**Есть филиальная сеть и часть компаний использует общую систему, являющуюся объектом КИИ. Кто должен категорировать данную систему?**
Категорирование осуществляет субъект КИИ, которому принадлежит система на каком-либо основании. Данная информация устанавливается по договорным условиям между организациями (аренда, право пользования, и т.д.). *В случае, если компоненты системы формально принадлежат (стоят на балансе) у одного из филиалов, а пользуется ей головная организация (загружает и обрабатывает информацию), то субъектом КИИ будет являться скорее головная компания.* *В любом случае, такие пограничные моменты рекомендуется уточнять с учетом всех деталей посредством личного обращения во ФСТЭК России.*	

В соответствии с п. 12 127ПП, в состав комиссии по категорированию могут также включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с государственными органами и российскими юридическими лицами. Данный пункт имеет смысл использовать для подведомственных учреждений, которые должны согласовывать перечень объектов, подлежащих категорированию, и результаты категорирования с указанными органами. Если Организация не является подведомственным учреждением, то включать представителей данных органов в комиссию по категорированию необходимости нет. Для каждой подведомственной Организации должны выбираться соответствующие региональные органы, в ведомстве которых находится Организация и высылаться на их имя запрос с просьбой включения ответственного лица с их стороны в комиссию по категорированию. Так как данное включение является возможностью, а не требованием, то его можно не делать (также может быть отказано со стороны самих органов). Основной смысл включения данного ответственного — упрощение дальнейшего этапа согласования результатов с этими региональными органами.

Q&A	**Наша организация относится к субъектам, обеспечивающим взаимодействие объектов КИИ. Кого нам включать в комиссию?**
Нормативные документы не предусматривают каких-то дополнений в данном случае, поэтому основной состав комиссии остается таким же. Члены комиссии могут запрашивать необходимую информацию у сторонних организаций.	

! Дальнейшие этапы категорирования объектов КИИ проводит сформированная комиссия по категорированию. В случае необходимости, члены комиссии могут привлекать других работников Организации для сбора необходимой информации.

5 Формирование перечня критических процессов

Входная информация:

1) Перечень видов деятельности Организации;
2) Организационная структура Организации.

Участники процесса:

1) Комиссия по категорированию;
2) Руководители функциональных подразделений.

Результат:

Перечень критических процессов Организации.

Схема процесса

Общий порядок формирования перечня критических процессов, описывающийся в данном разделе, приведен на рисунке 3.

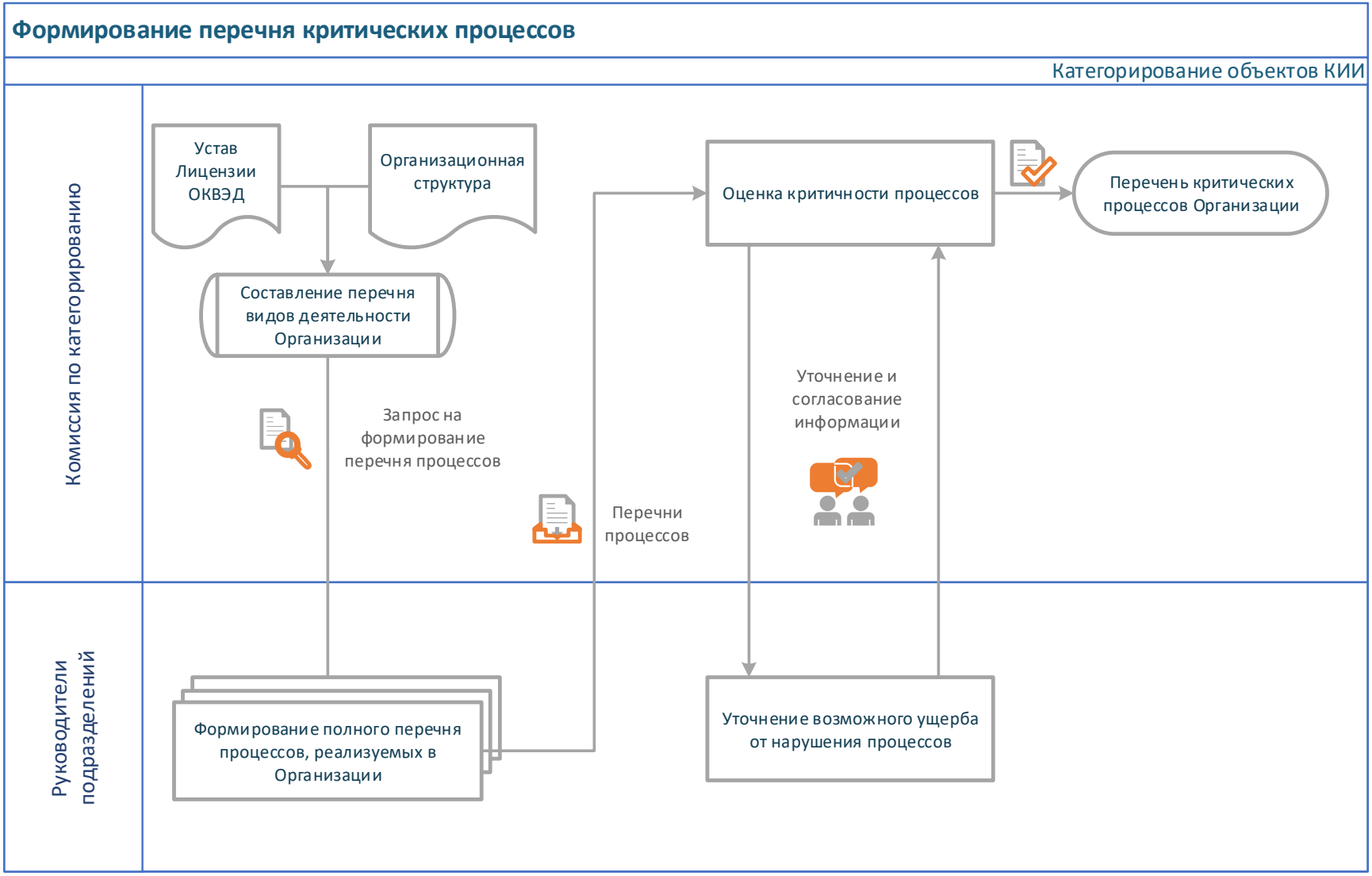

Рисунок 3 – Порядок формирования перечня критических процессов

Описание процесса

В соответствии с 127ПП, категорированию подлежат объекты КИИ, которые обеспечивают критические процессы субъектов КИИ. Критическими процессами считаются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Соответственно, задачами данного этапа является определение критических процессов в Организации.

5.1 Формирование перечня процессов

Анализируются учредительные документы, устав, иные положения организации, где прописаны основные виды деятельности (дополнительно, о видах деятельности организации можно узнать из выписки ЕГРЮЛ/ЕГРИП).

Анализируется организационная структура Организации, анализируются положения об отделах и/или запрашивается информация об обязанности и функциях подразделений Организации. Данная информация используется для детализации или расширения перечня, полученного на первом шаге.

Для каждой выявленной функции / осуществляемого вида деятельности (соответствующих областям (сферам), установленным пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации») формируется перечень процессов, реализуемых в рамках этой функции / вида деятельности.

Согласованный перечень процессов рекомендуется (не требуется нормативной документацией, но предлагается для удобства учета и контроля собираемой информации) фиксировать в виде Отчете об обследовании объектов КИИ (шаблон Отчета представлен в Приложение 2).

Q&A	**Какая детализация в перечне процессов необходима? Можно ли указывать «нефтепереработка» / «оказание медицинской помощи» или нужна большая степень детализации?**
Степень обобщенности или декомпозиции процессов не регламентирована и остается на усмотрение Организации. На основании имеющегося опыта мы рекомендуем делать более детальное подразделение процессов, относящихся к основным видам деятельности Организации. Как некоторую отправную точку можно взять организационную структуру Организации и отталкиваться от принципа «одно подразделение нижнего уровня — один процесс», а дальше уже корректировать по необходимости.	

Q&A	**Процесс бухгалтерского делопроизводства или иной финансовой деятельности непосредственно связан с одним из критериев. Нужно ли его включать в рассматриваемый перечень?**
В перечень включаются процессы, реализующие виды деятельности, соответствующие областям (сферам), установленным пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». *В общем случае бухгалтерские расчеты, выплата налогов и т.д. не является одним из указанных видов деятельности, поэтому не должны включаться в перечень.* *Можно специально выделить процесс «Закупка сырья», связанный с процессом производственной деятельности, но это скорее искусственное усложнение, так как конечная цель – выделение объектов, а любые закупки или переводы не завязаны строго на системах 1С и к ним не предъявляются жесткие требования безотказного функционирования – оплату можно сделать с помощью печатной формы через банк.* *С другой стороны, могут существовать специализированные процессы, например, отчетности по гособоронзаказу, которые завязаны на строгие условия и системы. Их включать имеет смысл.* *Если сомневаетесь, то включайте все процессы, включая оплату сырья/оборудования – на более поздних стадиях анализа вы должны будете отсеять соответствующие объекты или признать их незначимыми.*	

Q&A	**Что включать в процесс производства, входят ли туда такие связанные процессы, как противоаварийная защита, процесс контроля доступа, процесс пожаротушения, извещение о чрезвычайных ситуациях и т. д.?**
Мы рекомендуем отделять такие процессы, как пожаротушение или видеонаблюдение, от процесса производства, связанного с технологическими процессами обработки, транспортировки и учета сырья и продукции. Видеонаблюдение, контроль доступа, сигнализация и т. д. могут быть связаны и взаимодействовать с производственными процессами, но, как правило, само производство технически может функционировать без них. *Сам факт нарушения контроля доступа или видеофиксации не влечет автоматически какого-то ущерба. Поэтому данные процессы должны выделяться отдельно и в большинстве случаев они не будут являться критическими.* *При этом необходимо учитывать потенциальное влияние на другие процессы.*	

Например, отсутствие пожаротушения не обязательно приведет к тому, что цех сгорит (потому что пожар – это уже инцидент сам по себе, а не обычное состояние), но несанкционированная активация системы пожаротушения в некоторых случаях может стать причиной нарушения функционирования других процессов КИИ.
Противоаварийная автоматика может рассматриваться как часть производственного процесса, если она технически интегрирована в промышленные системы, а может рассматриваться в качестве самостоятельного объекта и процесса.

Пример

Организация владеет гидроэлектростанцией и, соответственно, ИС и АСУ ТП, функционирующими в области энергетики. При этом, в перечень процессов в рамках осуществляющей деятельности могут быть включены:

- *управление выработкой электроэнергии;*
  - *управление гидроагрегатами;*
  - *управление активной и реактивной мощностью;*
  - *управление трансформаторным оборудованием;*
  - *мониторинг переходных режимов;*
  - *управление электрооборудованием (ОРУ/КРУЭ);*
- *управление распределением и передачей электроэнергии;*
- *учет и планирование выработки электроэнергии;*
- *коммерческий и технический учет электроэнергии;*
- *обеспечение информационного обмена с регуляторами энергорынка;*
- *контроль вибрации оборудования и сооружений;*
- *контроль противоаварийной автоматики и релейных защит;*
- *управление очистными сооружениями;*
- *управление насосным и дренажным оборудованием;*
- *передача и контроль данных телемеханики;*
- *управление ремонтными работами и контроль состояния оборудования;*
- *обеспечение эксплуатации гидротехнических сооружений, энергетического и гидромеханического оборудования;*
- *управление состояниями активов;*
- *управление персоналом;*
- *бухгалтерский учет;*
- *организация контрольно-пропускного режима и антитеррористического режима;*

- *управление системой пожаротушения;*
- *оповещение об аварийных ситуациях;*
- *автоматизированная регистрация аварийных событий;*
- *ведение делопроизводства;*
- *и т. д.*

Как пример, процессы «контроль вибрации оборудования и сооружений» и «контроль противоаварийной автоматики и релейных защит» не связаны непосредственно с деятельностью в сфере энергетики, но нарушение их работы может повлечь остановку по аварийному сигналу других систем, связанных с производством электроэнергии, поэтому указанные процессы должны быть включены в область анализа, так как они попадают в перечень критических процессов и далее должны рассматриваться системы, участвующие в автоматизации данных процессов.

Q&A	**Наша организация относится к субъектам, обеспечивающим взаимодействие объектов КИИ. Нам так и назвать этот процесс – «обеспечение взаимодействия объектов ХХХ»?**
Наверное, это не лучшее решение. Мы рекомендуем давать более реалистичные наименования, например: «предоставление услуг информационного взаимодействия и управление сетью передачи данных для обеспечения взаимодействия ИС1 и ИС2», «оказание услуг по предоставлению технических средств и управлению информационной инфраструктурой ЦОД» и т. д.	

5.2 Определение критичности процессов

Для каждого выявленного процесса должна быть проведена оценка критичности его нарушения с точки зрения возможных негативных социальных, политических, экономических, экологических последствий, последствий для обеспечения обороны страны, безопасности государства и правопорядка.

Критериев оценки критичности нарушения процессов в 127ПП явно не определено, поэтому мы предлагаем использовать перечень показателей критериев значимости объектов и их значения из 127ПП. Соответственно, нужно определить для каждого рассматриваемого процесса - способно ли его нарушение повлечь последствия, соответствующие критериям значимости из 127ПП.

! В соответствии с разъяснениями ФСТЭК России, критическим процесс становится, если есть соответствующие последствия от нарушений в любом масштабе, даже если они по своему масштабу не превышают нижний порог показателей для 3-й категории значимости, поэтому оцениваются не масштабы возможных последствий, а сам факт их возможности.

Q&A	**Почему бы не рассмотреть сразу все ИС / АСУ ТП / ИТС? Ведь получается двойная работа: сначала нужно классифицировать процессы, а потом еще категорировать системы. Можно ведь сразу категорировать все системы.**
По логике регуляторов и по предложенной методике процессный подход позволит упростить работу, потому что процессов обычно меньше, чем систем (один процесс автоматизируется несколькими системами. Соответственно, проще провести, например, категорирование 10 процессов, выявить 5 критических и далее категорировать 10 связанных с ними систем, чем сразу категорировать 20 систем, участвующих во всех 10 процессах (цифры примерные, для наглядности принято, что одному процессу соответствует 2 системы). Более того, после первого этапа Организация должна получить перечень объектов КИИ, подлежащих категорированию и передать его в ФСТЭК России. Если пойди по пути без учета процессов, то нужно будет категорировать и документировать эти работы для всех систем (иначе как обосновать, что они не являются значимыми?). При этом промежуточного списка «подлежащих категорированию» систем не будет — будет или полный перечень систем или уже итоговый, со значимыми объектами КИИ.	

Рекомендуется (требования в нормативной документации отсутствуют) при оценке критичности процессов результаты анализа отражать в Отчете об обследовании объектов критической информационной инфраструктуры. Форма отчета и шаблоны для оценки критичности процессов приведены в Приложение 2 (раздел 2 Выявление критических процессов).

! **Критический процесс** — процесс, для которого хотя бы по одному из оцениваемых критериев было сделано заключение о возможности соответствующего ущерба.
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.

Q&A	**При оценке на промышленных предприятиях в критические попадают только процессы управления?**
Не только. В частности, представители ФСТЭК России считают (и мы с ними согласны), что получение и обработка телеметрии также может являться критическим процессом, так как на основании этих данных возможно принятие	

решений об управляющих воздействий. Поэтому каждый процесс нужно рассматривать со всех сторон и возможных последствий.

Q&A	**Наша организация относится к субъектам, обеспечивающим взаимодействие объектов КИИ. Как нам делать данную оценку критичности?**
Если вы осуществляете обеспечение функционирования/взаимодействия объектов КИИ, подлежащих категорированию, то данный процесс является критическим (даже, если данные объекты по результатам категорирования не являются значимыми). Соответственно, необходимо запрашивать данные сведения (результаты категорирования) у владельцев этих объектов.	

6 Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию

Входная информация:

Перечень критических процессов Организации.

Участники процесса:

1) Руководитель Организации;
2) Комиссия по категорированию;
3) Руководители функциональных подразделений;
4) Государственный орган или юридическое лицо, выполняющее функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере работы Организации.

Результат:

Перечень объектов КИИ, подлежащих категорированию.

Схема процесса

Общий порядок формирования перечня объектов КИИ, подлежащих категорированию, описывающийся в данном разделе, приведен на рисунке 4.

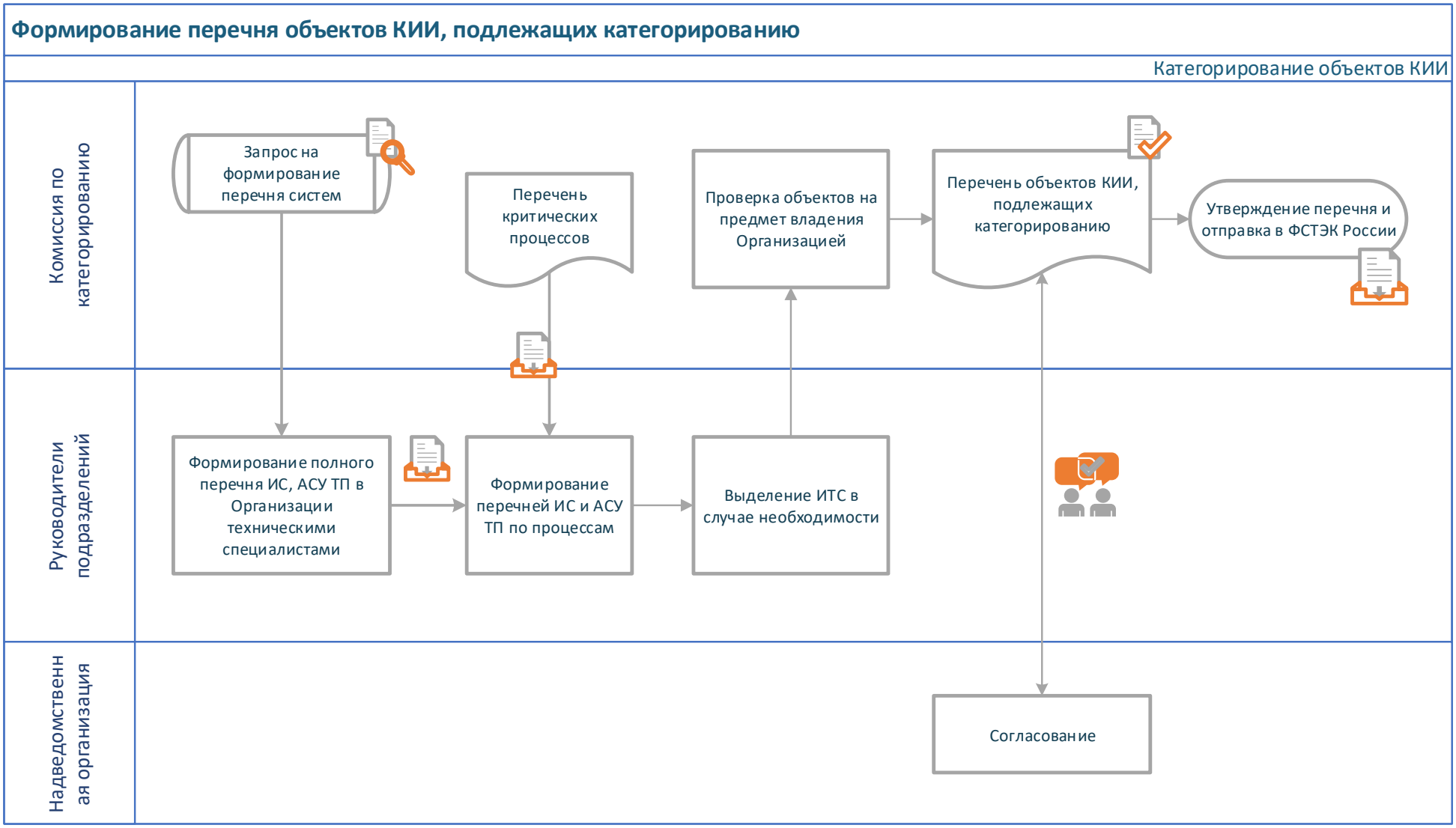

Рисунок 4 – Порядок формирования перечня объектов КИИ, подлежащих категорированию

Описание процесса

6.1 Формирование перечня объектов

Для каждого критического процесса определяется перечень ИС / АСУ / ИТС, которые осуществляют что-либо из следующего:

- обработку информацию, необходимую для критических процессов;
- управление критическим процессом;
- контроль или мониторинг критических процессов.

Иначе говоря, для каждого критического процесса необходимо сформировать перечень ИС / АСУ / ИТС, которые реализуют (полностью или частично) данный процесс, участвуют в его автоматизации.

При формировании перечня данных систем рекомендуется:

- провести инвентаризацию систем (сделать запрос ответственным за управление информационной инфраструктурой, прикладным ПО, автоматизацией предприятия с просьбой составить перечень ИС / АСУ Организации);
- сделать запрос владельцам выявленных критических процессов с просьбой указать ИС / АСУ из сформированного перечня, участвующих в рассматриваемых процессах;
- уточнить итоговый перечень систем с ответственным за управление информационной инфраструктурой, прикладным ПО, автоматизацией предприятия, в случае необходимости добавить ИТС, используемые для реализации информационных потоков рассматриваемых процессов.

Q&A	**Мы рассматриваем все системы, включая 1С, кадровые и т. д., или только явно важные, типа АСУ ТП и ERP?**
Изначально должны рассматриваться ВСЕ системы, которые так или иначе связаны с реализацией критических процессов. Если ИС 1С участвует в автоматизации какого-либо процесса, признанного критическим на предыдущем шаге, то она должна включаться в перечень. Далее при категорировании часть подобных систем не получит категорию и на них не будут накладываться требования по защите. *Почти наверняка такие системы как 1С, банк-клиент и иные системы общего характера в рассматриваемый перечень не войдут, потому что не участвуют непосредственно в критических процессах.*	

Q&A	**Какова степень детализации объектов? Можно ли их объединять или наоборот сегментировать?**

Рекомендуемая степень детализации (очерчивание границ объектов) – на основании существующей проектной и эксплуатационной документации на системы. Также можно ориентироваться на цели и задачи систем.
Объединять несколько систем в единый объект допускается в том случае, если несколько объектов КИИ решают однотипные задачи или участвуют в автоматизации общего критического процесса.
Сегментирование объектов также допускается, но не всегда оправданно, так как в конечном счете масштаб последствий должен определяться от нарушения функционирования системы в целом и может оказаться, что у вас появится 5 значимых объектов КИИ вместо одного (например, атаки на АРМ оператора или инженера АСУ ТП в конечном итоге могут привести к нарушению функционирования АСУ ТП в целом, поэтому не получится обосновать их меньшую значимость)

Q&A	**У нас есть системы, которые участвуют в нескольких процессах — как быть с ними?**

На данном этапе лучше их связать со всеми процессами и записать и там, и там. Важным является сам факт того, что данная система попадает в перечень объектов, подлежащих категорированию и будет рассматриваться на следующих этапах. Далее при категорировании связь с несколькими процессами может использоваться при оценке ущерба - он должен суммироваться в случае нарушения нескольких процессов.

Q&A	**Что делать со специфичными системами: СКУД, видеонаблюдение, системой охранной сигнализации, пожаротушения, извещения о чрезвычайных ситуациях и т. д.?**

Если система каким-то образом участвует в реализации (управление, контроль, обеспечение и т.д.) критического процесса, то она включается. Общая рекомендация с уровня выделения процессов: обеспечение режима на производстве, наблюдение за контролируемой зоной, пожаротушение, сигнализация о чрезвычайных ситуациях и т.д. — самостоятельные процессы, системы, реализующие их, следует отделять от производственных систем производства и оцениваться отдельно.
В большинстве случаев данные процессы не будут признаны критическими, поэтому соответствующие системы не попадут в перечень объектов, подлежащих категорированию.
Но, например, при рассмотрении системы пожарной сигнализации и пожаротушения в ЦОД или на промышленном объекте необходимо учесть, что несанкционированная активация пожарной тревоги и включение данных систем могут повлечь нарушение работоспособности других объектов КИИ, размещенных на данной площадке.

Q&A	**Что делать с корпоративной сетью? Указывать ее по сегментам, указывать целиком, разделять по филиалам? Выделять ли ее в качестве ИТС?**

Данные требования не определены в нормативных документах.
Если есть возможность выделить ИС / АСУ в цельный сегмент, в котором локализованы информационные потоки единого процесса, то данную сеть / подсеть указывать дополнительно нет смысла — она будет являться неотъемлемой частью ИС / АСУ.
Если есть несколько различных систем (ИС / АСУ), которые совместно используют единый сетевой сегмент (например, сегмент технологической сети для взаимодействия с MES или АСУ верхнего уровня), то такую сеть / сегмент стоит выделить отдельно — далее она будет категорироваться по максимальному или суммарному потенциальному ущербу объектов, использующих данную ИТС.
В случае, если выделить сегменты затруднительно и рассматривается информационный обмен внутри общей корпоративной сети, то можно указывать такую сеть в целом. Один из вариантов – указать ее как общую ИС, если можно завязать все ИС по единому признаку. Второй вариант – выделить КСПД в качестве самостоятельной ИТС (не самый простой вариант, так как частные ИС нужно будет дополнительно дробить, что увеличивает объем и сложность общих работ). При этом допускается дополнительное разграничение: «серверный сегмент», «сегмент ЦОД», «рабочий сегмент офиса 1», «рабочий сегмент офиса 2» и т. д. Данное разграничение может быть полезным в дальнейшем при снижении категорий объектов КИИ и упрощении требований по защите.
Не стоит углубляться в максимальное дробление ИС до уровня частных серверов и АРМ в целях снизить требования по их защите. На уровне реализации могут возникнуть сложности с разграничением доступа на таком детальном уровне, к тому же сложно будет обосновать отсутствие взаимосвязанности компонентов.
Оптимальный принцип – выделение ИС по функциональному назначению.
При указании ИТС необходимо также придерживаться правила, что указываются сети, которые принадлежат Организации.

Пример

Процесс производства электроэнергии на ГЭС:

- *САУ ГА;*
- *ГРАМ;*
- *ГРНРМ;*
- *ЭГР-МП;*
- *СУР;*
- *Управление маслонапорной установкой;*
- *Система управления трансформаторами;*
- *ОРУ-220 кВ;*
- *КРУЭ 500 кВ;*
- *Автоматизированная система управления верхнего уровня;*
- *MES-системы верхнего уровня;*
- *Технологическая сеть производства.*

Процесс контроля состояния оборудования и гидросооружений:

- *Система вибродиагностики;*
- *Система термоконтроля;*
- *Автоматизированная система контроля гидротехнических сооружений;*
- *Комплекс телемеханики;*
- *Автоматизированная система управления верхнего уровня;*
- *Технологическая сеть производства.*

Рекомендуется при формировании перечня объектов, подлежащих категорированию отражать в Отчете об обследовании объектов критической информационной инфраструктуры. Форма отчета и шаблоны приведены в Приложение 2 (раздел 3 Определение объектов критической информационной инфраструктуры). Также на этапе обследования рекомендуем собирать основные сведения об объектах КИИ, подлежащих категорированию, которые используются в ходе работ (шаблоны приведены в разделе 4 Информация об объектах КИИ).

В случае, если по итогам анализа Комиссия пришла к заключению, что в Организации нет ИС / АСУ / ИТС, участвующих в автоматизации критичных процессов (или используемые ИС / АСУ / ИТС принадлежат иным организациям), то перечень объектов КИИ, подлежащих категорированию, не оформляется. Рекомендуется оформлять Заключение Комиссии об отсутствии объектов КИИ, подлежащих категорированию (пример протокола и заключения приведен в Приложение 3)

6.2 Передача перечня объектов, подлежащих категорированию в ФСТЭК России

Итоговый перечень ИС / АСУ / ИТС оформляется в виде перечня объектов КИИ, подлежащих категорированию и передается в ФСТЭК России.

Рекомендованная форма перечня объектов КИИ, подлежащих категорированию, приведена в Приложение 4.

В соответствии с информационным сообщением ФСТЭК России от 24 августа 2018 г. N 240/25/3752, а также требованиями 127ПП, **необходимо**:

- согласовать перечень объектов КИИ, подлежащих категорированию, с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию

в сфере работы Организации (в случае необходимости, если Организация является подведомственным учреждением).

– направить перечень объектов КИИ, подлежащих категорированию, в ФСТЭК России в течение 10 рабочих дней после утверждения руководителем субъекта КИИ (или уполномоченным лицом) в бумажном виде с приложением электронных копий в формате файлов .ods и (или) .odt.

Согласование перечня объектов КИИ, подлежащих категорированию, с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере работы Организации, осуществляется в произвольной форме. Возможна передача запроса согласования с приложением предварительно заполненной формы перечня объектов КИИ, подлежащих категорированию, без утверждающей подписи руководителя Организации. В случае получения замечаний или корректировок, они должны быть рассмотрены комиссией по категорированию и перечень может быть пересмотрен, после чего отправлен на повторное согласование. Отметка о согласовании на итоговом перечне, отправляемом во ФСТЭК России, не требуется.

! В перечень объектов включаются объекты КИИ филиалов, представительств субъекта КИИ (в случае общей принадлежности к одному юридическому лицу).

Сроки категорирования, которые указываются в перечне, не формализованы, единственное ограничение — категорирование должно быть завершено в течение 12 месяцев после утверждения перечня объектов КИИ, подлежащих категорированию.

Утвержденный перечень объектов КИИ, подлежащих категорированию, дополняется сопроводительным письмом в произвольной форме и отправляется по следующим реквизитам:

Экспедиция ФСТЭК России,

105066, г. Москва, ул. Старая Басманная, д. 17.

2 управление ФСТЭК России

Отправляется:

– общее сопроводительное письмо;

- утвержденный перечень объектов КИИ, подлежащих категорированию (в печатном виде);
- утвержденный перечень объектов КИИ, подлежащих категорированию (копия в электронном виде).

ФСТЭК России не утверждает и не согласует направляемые перечни, поэтому ответа ждать не стоит.

7 Категорирования объектов критической информационной инфраструктуры

Входная информация:

Перечень объектов КИИ, подлежащих категорированию.

Участники процесса:

1) Руководитель Организации;
2) Комиссия по категорированию;
3) Руководители функциональных подразделений.

Результат:

1) Акт категорирования объектов КИИ;
2) Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости.

Схема процесса

Общий порядок категорирования объектов КИИ, описывающийся в данном разделе, приведен на рисунке 5.

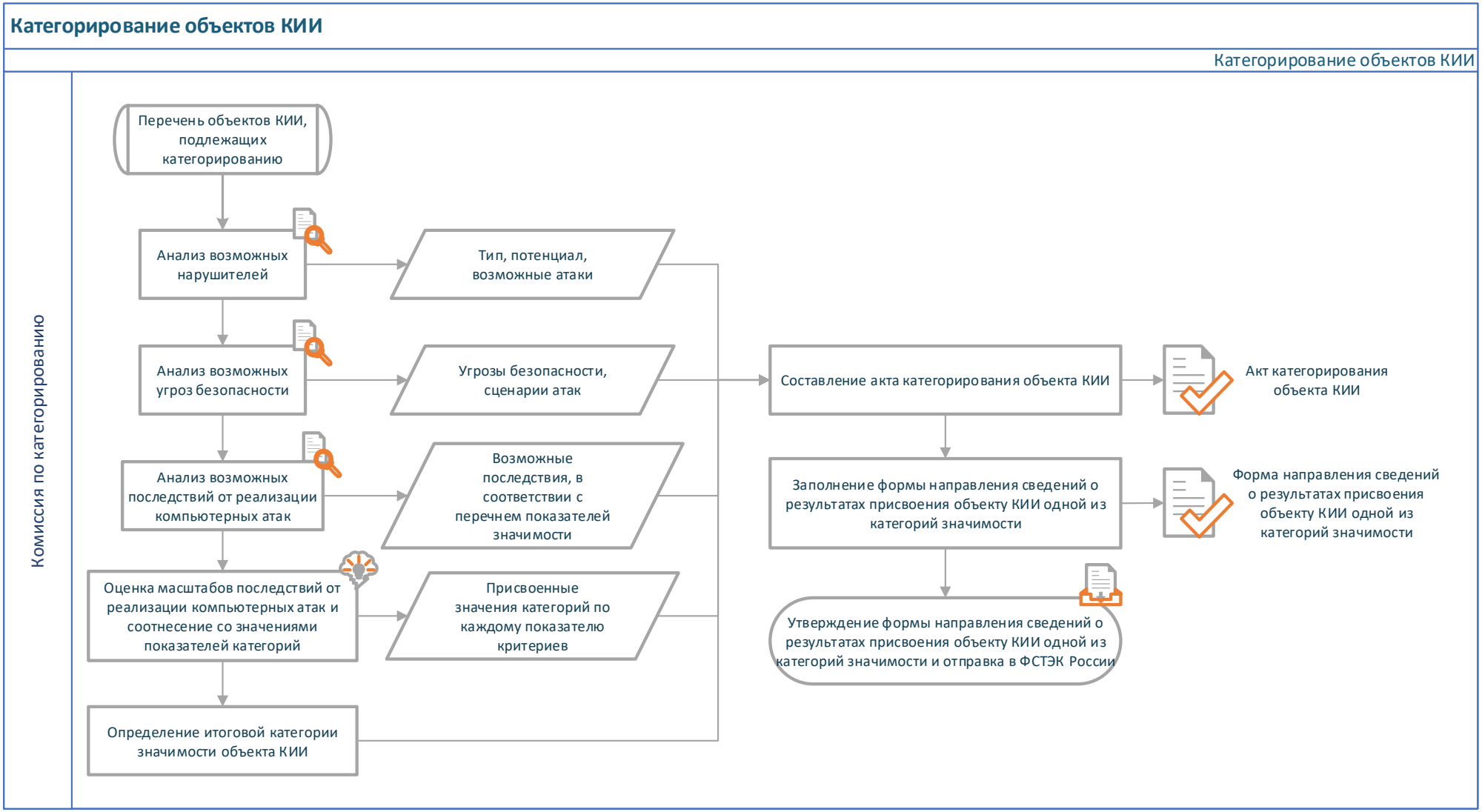

Рисунок 5 – Порядок категорирования объектов КИИ

Описание процесса

Определение категорий значимости объектов КИИ осуществляется на основании показателей критериев значимости и их значений, утвержденных 127ПП. При категорировании осуществляется:

- анализ возможных источников угроз и действий предполагаемых нарушителей;
- анализ возможных угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;
- оценка масштаба последствий угроз и соотнесение со значениями показателей категорий;
- определение категории значимости объекта КИИ.

7.1 Анализ возможных источников угроз и действий предполагаемых нарушителей

Комиссия по категорированию с помощью работников, ответственных за обеспечение ИБ в Организации, должна определить возможные источники угроз и их характеристики. Данная информация получается экспертным путем. В случае, если для рассматриваемого объекта ранее разрабатывалась модель угроз и нарушителей, то эти данные можно взять напрямую из нее. Также могут использоваться существующие данные из моделей угроз и моделей нарушителей для схожих систем, функционирующих в Организации.

Анализ возможных нарушителей рекомендуется отражать в Отчете об обследовании объектов критической информационной инфраструктуры. Форма отчета и шаблоны приведены в Приложение 2 (раздел 5 Анализ возможных действий нарушителей в отношении объектов КИИ). Шаблоны приведены в виде справочного материала и должны адаптироваться под нужды и характеристики Организации, применительно к конкретному объекту. Классификация приведена с учетом БДУ ФСТЭК России, сформированный итоговый набор может использоваться в дальнейшем для формирования модели нарушителей и модели угроз для значимых объектов КИИ. Рекомендуется сразу выбирать наборы потенциальных нарушителей для групп объектов КИИ, для которых они характерны, так как данная информация в

любом случае понадобится при передаче сведений о результатах категорирования объектов КИИ во ФСТЭК России.

7.2 Анализ возможных угроз ИБ

Для рассматриваемого объекта КИИ проводится анализ возможных угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объекте КИИ. В соответствии с комментариями ФСТЭК России, на данном этапе не требуется разработка полноценных моделей угроз (они требуются только для значимых объектов КИИ на последующих этапах). Поэтому предлагается экспертным путем определить общие классы угроз безопасности информации.

Анализ возможных угроз рекомендуется отражать в Отчете об обследовании объектов критической информационной инфраструктуры. В качестве ориентира можно использовать классификацию основных типов угроз, приведенную в Приложение 2 (раздел 6 Анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ). Данная классификация приведена в виде справочного материала и должна адаптироваться под нужды и характеристики Организации, применительно к конкретному объекту.

! При выборе возможных угроз должны рассматриваться наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты КИИ, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба.

Пример 1

Рассматриваемый объект — АСУ на производстве, физически изолированная от иных сетей.

***Актуальные типы угроз**:*

- *Нарушение целостности обрабатываемых данных;*
- *Нарушение доступности обрабатываемых данных;*
- *Нарушение целостности конфигурации и настроек технологического процесса;*
- *Нарушение доступности конфигурации и настроек технологического процесса;*
- *Нарушение целостности компонентов АСУ ТП;*
- *Нарушение доступности компонентов АСУ ТП.*

***Возможные сценарии атак**:*

- *Эксплуатация уязвимостей системного, прикладного или сетевого ПО;*
- *Атаки с использованием вредоносного ПО;*
- *Направленные атаки на пользователей (фишинг и иные методы социальной инженерии);*
- *Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи.*

Пример 2

Рассматриваемый объект — медицинский комплекс обследования пациентов (рентгеновская установка).

***Актуальные типы угроз**:*

- *Нарушение конфиденциальности обрабатываемых данных;*
- *Нарушение целостности обрабатываемых данных;*
- *Нарушение доступности обрабатываемых данных;*
- *Нарушение целостности конфигурации и настроек технологического процесса;*
- *Нарушение доступности конфигурации и настроек технологического процесса;*
- *Нарушение целостности компонентов АСУ ТП;*
- *Нарушение доступности компонентов АСУ ТП.*

Возможные сценарии атак:

- *Доступ к информации, хранящейся в незащищенном, открытом виде;*
- *Эксплуатация уязвимостей системного, прикладного или сетевого ПО;*
- *Компрометация данных идентификации и аутентификации;*
- *Перехват информации в каналах передачи данных;*
- *Атаки с использованием вредоносного ПО;*
- *Сетевые атаки (нарушение связи с помощью специальных сетевых пакетов, подмена и изменение адресов, таблиц маршрутизации, обход правил сетевого разграничения доступа и т. д.);*
- *Направленные атаки на пользователей (фишинг и иные методы социальной инженерии);*
- *Модификация данных при их передаче по каналам связи;*
- *Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи;*
- *Передача подложных команд, перехват управления.*

7.3 Оценка масштаба последствий и соотнесение со значениями показателей категорий

Для рассматриваемого объекта КИИ необходимо определить возможные последствия нарушений, основываясь на выявленных возможных угрозах ИБ, сценариях компьютерных атак, назначении объекта КИИ и автоматизируемого

процесса. Для рассматриваемого объекта КИИ должны выбираться те типы последствий, которые могут стать следствием возможных угроз для данного объекта. В качестве возможных предлагается рассматривать последствия, соответствующие показателям значимости из 127ПП, в соответствии с которыми будет проводиться категорирование:

1) причинение ущерба жизни и здоровью людей;

2) прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений;

3) прекращение или нарушение функционирования объектов транспортной инфраструктуры;

4) прекращение или нарушение функционирования сети связи;

5) отсутствие доступа к государственной услуге;

6) прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции;

7) нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ;

8) возникновение ущерба субъекту КИИ, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей);

9) возникновение ущерба бюджетам Российской Федерации;

10) прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом КИИ, 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;

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);

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 КИИ;

14) прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка.

! В качестве предварительного фильтра можно сразу рассматривать только те типы последствий, которые свойственны для выявленных ранее критических процессов, автоматизируемых рассматриваемым объектом КИИ.

Пример 1

Рассматриваемый объект — АСУ на производстве, физически изолированная от иных сетей.

***Актуальные типы угроз**:*

- *Нарушение целостности обрабатываемых данных;*
- *Нарушение доступности обрабатываемых данных;*
- *Нарушение целостности конфигурации и настроек технологического процесса;*
- *Нарушение доступности конфигурации и настроек технологического процесса;*
- *Нарушение целостности компонентов АСУ ТП;*
- *Нарушение доступности компонентов АСУ ТП.*

Возможные сценарии атак:

- *Эксплуатация уязвимостей системного, прикладного или сетевого ПО;*
- *Атаки с использованием вредоносного ПО;*
- *Направленные атаки на пользователей (фишинг и иные методы социальной инженерии);*
- *Несанкционированная модификация конфигурации и настроек технологического процесса.*

Возможные последствия (следствия реализации соответствующих типов угроз):

- *Причинение ущерба жизни и здоровью людей:*
- *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).

Пример 2

Рассматриваемый объект — медицинский комплекс обследования пациентов (рентгеновская установка).

***Актуальные типы угроз**:*

- *Нарушение конфиденциальности обрабатываемых данных;*
- *Нарушение целостности обрабатываемых данных;*
- *Нарушение доступности обрабатываемых данных;*
- *Нарушение целостности конфигурации и настроек технологического процесса;*
- *Нарушение доступности конфигурации и настроек технологического процесса;*
- *Нарушение целостности компонентов АСУ ТП;*
- *Нарушение доступности компонентов АСУ ТП.*

Возможные сценарии атак:

- *Несанкционированный доступ к защищаемой информации;*
- *Эксплуатация уязвимостей системного, прикладного или сетевого ПО;*
- *Компрометация данных идентификации и аутентификации;*
- *Перехват информации в каналах передачи данных;*
- *Атаки с использованием вредоносного ПО;*
- *Сетевые атаки (нарушение связи с помощью специальных сетевых пакетов, подмена и изменение адресов, таблиц маршрутизации, обход правил сетевого разграничения доступа и т. д.);*
- *Направленные атаки на пользователей (фишинг и иные методы социальной инженерии);*
- *Модификация данных при их передаче по каналам связи;*
- *Несанкционированная модификация конфигурации и настроек технологического процесса;*
- *Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи;*
- *Передача подложных команд, перехват управления.*

Возможные последствия (следствия реализации соответствующих типов угроз):

- *Причинение ущерба жизни и здоровью людей.*

При оценке масштабов последствий и соотнесении со значениями показателей категорий следует использовать (для соответствующих объектов):

- договоры на оказание соответствующих услуг (учет количества потребителей и подключаемых территориальных объектов);
- ТЗ на объекты;
- результаты категорирования объектов транспортной инфраструктуры;
- декларация промышленной безопасности опасного производственного объекта;
- декларация безопасности гидротехнического сооружения;
- паспорт безопасности объекта топливно-энергетического комплекса;
- паспорта безопасности опасного производственного объекта;
- результаты категорирования объектов, оказывающих негативное воздействие на окружающую среду;
- результаты классификации сетей электросвязи.

В соответствии с п. 14.2 127ПП, 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.

Пример

Рассмотрим взаимосвязанные объекты КИИ А и зависящий от него Б, допустим, А предоставляет информацию в Б или А является сетью связи, обеспечивающей доступ к Б.

В данном случае при оценке масштаба возможных последствий для объекта Б необходимо учитывать не только свойственные для него угрозы, но и угрозы от нарушения безопасности А, то есть абстрактный перечень угроз будет выглядеть как:

- *нарушение целостности обрабатываемых данных;*
- *нарушение целостности конфигурации и настроек технологического процесса;*
- *нарушение доступности компонентов;*
- *нарушение доступности входных данных из-за нарушения работоспособности объекта А;*
- *нарушение доступности каналов передачи данных, реализуемых объектом А.*

И в рассматриваемом варианте необходимо будет рассчитывать ущерб в том числе от дополнительных угроз.

Во многих случаях такое изменение не повлияет на оценку ущерба, но есть варианты, когда это может быть существенно, например, рассматривается АСУ ТП, в которой входные управляющие сигналы являются аналоговыми и не подвержены компьютерным атакам, рассматриваемым в рамках 187-ФЗ. Но один из вариантов управления – централизованная SCADA, Которая подвержена атакам, в том числе получению несанкционированного доступа и, таким образом, при расчете масштаба возможных последствий для АСУ ТП необходимо учитывать угрозу передачи ложных команд от компрометированной SCADA.

Другой пример – случай, когда выделяются общие или централизованные компоненты в отдельные объекты КИИ, например, сегмент ЛВС или общая СХД. Для каждого объекта, использующего данные компоненты, необходимо будет учитывать их влияние и последствия от атак на них. Нельзя сказать, что мы рассматриваем систему отдельно от ЛВС и угрозы сетевых атак поэтому не учитываем при оценке ущерба (такой вариант некорректен по очевидным причинам, однако искусственно использовался субъектами для снижения категорий значимости).

В соответствии с п. 14.3 127ПП, в случае если осуществление критического процесса зависит от осуществления иных критических процессов, оценка проводится исходя из совокупного масштаба возможных последствий от нарушения или прекращения функционирования всех выполняемых критических процессов. Данная ремарка также была добавлена в целях предотвращения искусственного ухода от категорирования части объектов, однако не оказывает принципиального влияния на сам процесс категорирования, если выполнять его в соответствии с методикой:

- в соответствии с 127ПП, определение критических процессов не включает в себя оценку масштаба возможных последствий от нарушения или прекращения их функционирования;
- оценка масштаба возможных последствий проводится для объектов КИИ и данную оценку рекомендуется проводить уже без привязки к частным процессам, а рассматривать в целом.

В соответствии с п. 9 127ПП, категорирование объектов КИИ, в составе которых используются программные и (или) программно-аппаратные средства, принадлежащие и эксплуатируемые иными лицами, осуществляется субъектом КИИ с учетом данных о последствиях нарушения или прекращения функционирования указанных программных и (или) программно-аппаратных средств, представляемых этими лицами.

Пример

Данное уточнение используется, например, в таких случаях как:

- *аренда ЦОД с ЛВС или системой виртуализации, обеспечивающей взаимодействие ИС;*
- *аренда линий связи для организации взаимодействия ИС;*
- *использование централизованной ИС в холдинге, принадлежащей головной организации;*
- *и т.д.*

Q&A	**Как оценивать финансовый ущерб или иные последствия? Сбои могут быть разные – где-то предприятие встанет на месяц, где-то за час восстановится.**

Данный вопрос не регламентирован. В целом предлагается экспертная оценка. Необходимо рассматривать максимальный негативный сценарий, без учета существующих средств защиты и компенсирующих мер, которые могут существенно снизить масштаб возможных последствий. То есть:

1. *нужно 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 РАС и ПАЗ не рассматриваются как фактор, снижающий риск. Физические блокировки и ограничители можно принимать в расчет;*
2. *оценка длительности воздействия сбоя делается по наихудшему сценарию, но с учетом прогнозируемого времени восстановления для него. Данное время может быть взято из SLA, планов восстановления и иных существующих требований и процедур. Если ничего из этого нет, то оценка остается на усмотрение комиссии, с учетом, что она должна быть обоснована. На этапе выявления процессов стоит рассматривать длительные нарушения, не пытаясь сократить их влияния и «уйти из-под требований».*

Оценку масштаба последствий в результате возникновения компьютерных инцидентов предлагается отражать в Отчете об обследовании объектов критической информационной инфраструктуры. Шаблон раздела приведен в Приложение 2

(раздел 7 Оценка возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ).

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей и т. д.), оценка производится по **каждому** из значений показателя критериев значимости.

В случае если показатель критерия значимости неприменим для объекта КИИ или объект КИИ не соответствует ни одному показателю и их значениям (оцененный масштаб ниже минимальной оценки критерия), категория значимости не присваивается (в рассматриваемом шаблоне ставится значение БК).

Q&A	**Для АСУ ТП реализованы противоаварийные системы, для других ИС цифровое резервирование, меры защиты — как быть с ними и как их учитывать при оценке последствий?**

ФСТЭК России требует оценивать масштаб возможных последствий нарушений ИБ без учета существующих средств защиты и компенсирующих мер, которые могут существенно снизить масштаб возможных последствий — учитывать можно только меры, которые не подвержены угрозам ИБ (обычно это меры восстановления деятельности).

Не стоит учитывать: ПАЗ, резервное хранилище данных, резервные каналы передачи данных, межсетевые экраны, антивирусы. Все данные меры не дают 100% защиты, резервные хранилища могут быть также подвержены вирусным и другим атакам, а цифровая ПАЗ, подключенная в сеть АСУ ТП также может стать объектом атаки.

Допускается учитывать: механические блокировки и иные промышленные защиты, реализованные на физических принципах, физически изолированные от сети передачи данных, отчуждаемые носители с резервными копиями, тестируемые планы восстановления системы и соответствующие SLA, комплекты ЗИП и т. д. Данные меры не подвержены соответствующим компьютерным атакам и могут быть использованы при обосновании оценки последствий.

Полученные оценки масштаба последствий соотносятся со значениями показателей категорий, установленными 127ПП – по каждому показателю критичности выбирается значение показателя, соответствующее полученной оценке масштаба последствий. Выбранное значение рекомендуется, также, вносить в отчетную форму, приведенную в Приложение 2 (раздел 7 Оценка возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ).

7.4 Определение категории значимости объекта КИИ

Объекту КИИ присваивается категория значимости, соответствующая наивысшему значению из присвоенных категорий при соотнесении возможного ущерба с значениями категорий значимости (самая высокая категория — первая, самая низкая — третья).

! В соответствии с п.6 127ПП, в случае если объект КИИ по одному из показателей критериев значимости отнесен к первой категории, расчет по остальным показателям критериев значимости не проводится.
Таким образом, можно заполнить данные по определению категории значимости только для одного показателя критерии значимости, если по нему получен ущерб, соответствующий первой категории – в данном случае расчет по остальным категориям для объекта КИИ можно не заполнять.

Q&A	**Как поступать с объектами, чьи категории не выше третьей, но если атака будет одновременной сразу на несколько из них, то суммарный ущерб может наступить как у 2-й или даже у 1-й категории?**
Текущие требования данный момент не учитывают, поэтому формально необходимо также категорировать их по 3 категории, если последствия атаки являются невзаимосвязанными. *В случае, если один объект зависит от другого, то суммарный ущерб должен суммироваться: ущерб от атаки на объект А равен ущербу от нарушения функционирования объекта А + ущерб от нарушения функционирования объекта Б, зависящего от объекта А (в случае, если данная атака влечет нарушение работы объекта Б).*	

Q&A	**Нашей Организации принадлежит объект КИИ, но он используется для управления/мониторинга объектов другой Организации. Как нам проводить оценку ущерба и категорирование данного объекта?**
В соответствии с п. 9 127ПП, для объектов, принадлежащих одному субъекту КИИ, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащим другому субъекту КИИ, категорирование осуществляется на основе исходных данных, представляемых субъектом КИИ, которому принадлежит технологическое и (или) производственное оборудование. *Соответственно, рекомендуется сделать запрос сторонней организации для уточнения возможных последствий от нарушения ИБ рассматриваемого объекта КИИ.*	

Пример

В группе компаний, работающей в сфере горнодобывающей промышленности, в головной/управляющей организации функционирует централизованная SCADA верхнего уровня, которая используется для агрегации данных и частичного управления распределенными объектами (рудниками/цехами), которые принадлежат и управляются другими организациями (дочерними предприятиями).

В данном случае категорирование рассматриваемой централизованной SCADA осуществляет ее владелец (управляющая организация), а для категорирования она должна запрашивать необходимые данные для оценки ущерба от нарушения функционирования SCADA у дочерних предприятий.

Q&A	**Наша организация относится к субъектам, обеспечивающим взаимодействие объектов КИИ. Как нам провести категорирование?**
Весь общий процесс остается универсальным. При определении возможного ущерба необходимо запрашивать результаты соответствующего определения ущерба от нарушения функционирования объектов, взаимодействие которых нарушается.	

В соответствии с п. 16 127ПП, решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Допускается оформление единого акта по результатам категорирования нескольких объектов КИИ, принадлежащих одному субъекту КИИ.

Шаблон данного акта с рекомендациями по заполнению приведен в Приложение .

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта КИИ.

Субъект критической информационной инфраструктуры обеспечивает хранение акта до вывода из эксплуатации объекта КИИ или до изменения категории значимости.

7.5 Оформление и передача в ФСТЭК России результатов категорирования

В соответствии с п. 17 127ПП, субъект КИИ должен направить в ФСТЭК России сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий в течение 10 рабочих дней со дня утверждения акта категорирования объекта КИИ. Данные сведения направляются в форме, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 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».

Форма с рекомендациями по заполнению представлена в Приложение .

! Основным критерием проверки правильности категорирования объектов КИИ для ФСТЭК России является полнота и достоверность предоставляемых данных и обоснование решения по оценке степени вероятного ущерба и выбору соответствующих категорий. Таким образом, рекомендуется наиболее детально раскрывать информацию в разделе 8 формы передачи сведений.

Q&A	**У нас несколько объектов (возможно даже типовых), можно ли как-то объединять их по группам или делать одну форму на всех?**
Нет, такой вариант не предусмотрен в нормативных документах и необходимо оформлять отдельные формы с полным описанием для каждого объекта КИИ. Проверочное правило — для каждого объекта из высланного раннее перечня объектов КИИ, подлежащих категорированию, должна быть отчетная форма.	

Q&A	**После отправки перечня объектов, подлежащих категорированию, или результатов категорирования в организации произошли изменения и у нас поменялся состав, категория объектов КИИ. Что нам делать в данном случае?**
Необходимо провести категорирование новых объектов КИИ или объектов КИИ, в которых произошли изменения. Обновленные результаты категорирования отправляются во ФСТЭК России с сопроводительным письмом (поясняющим изменения). Отправляются только данные по измененным объектам, полный перечень отправлять заново не требуется.	

Q&A	**У нас пока не создана (не введена в эксплуатацию) система, которая является потенциальным объектом КИИ? Как нам быть в этом случае?**

В соответствии с п.8 127ПП, в отношении объекта КИИ, создаваемого в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных о критических процессах субъекта критической информационной инфраструктуры.
Соответственно, на указанном этапе должны формироваться необходимые сведения и требования и проводиться предварительное категорирование. В случае необходимости категорирование может быть пересмотрено позже, в ходе проектирования.

По вновь создаваемым объектам КИИ сведения, указанные в подпунктах "а" - "в" и "з" пункта 17 127ПП, направляются во ФСТЭК России в течение 10 рабочих дней после утверждения требований к создаваемому объекту КИИ, а сведения, указанные в подпунктах "г" - "ж" и "и" пункта 17 127ПП, - в течение 10 рабочих дней после ввода объекта КИИ в эксплуатацию (принятия на снабжение).

Утвержденную форму со сведениями о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, необходимо дополнить носителем с электронными копиями высылаемых форм сопроводительным письмом в произвольной форме и отправить по следующим реквизитам:

Экспедиция ФСТЭК России,

105066, г. Москва, ул. Старая Басманная, д. 17.

2 управление ФСТЭК России

Отправляется:

- общее сопроводительное письмо;
- утвержденные формы (в печатном виде);
- утвержденные формы (копия в электронном виде в формате .ods).

! В случае, если отправляемые данные содержат сведения, относящиеся к государственной тайне, необходимо учесть соответствующие требования ФЗ «О государственной тайне» при их передаче во ФСТЭК России.

7.6 Внесение изменений в результаты категорирования

В данном разделе дополнительно рассматриваются ситуации, которые могут возникнуть в ходе функционирования субъектов КИИ.

Q&A	**Мы ранее провели категорирование своих объектов и отправили соответствующую информацию во ФСТЭК России. Сейчас вышли изменения в 127ПП и 236 Приказ. Нужно ли нам что-то делать по этому поводу?**
В соответствии с 21 пунктом 127ПП, в случае изменения показателей критериев значимости объектов КИИ или их значений необходимо провести пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий. Изменения 127ПП ввели корректировку как некоторых показателей критериев значимости, так и их значений по части показателей, соответственно, единственным способом убедиться, что для существующих объектов КИИ не произошли изменения выявленных ранее категорий, является проведение категорирования по новым критериям и показателям. Субъекты КИИ должны провести переоценку своих объектов КИИ, подлежащих категорированию, в части измененных критериев и показателей и, в случае изменения категории значимости, должны отправить обновленные данные во ФСТЭК России.	

Q&A	**Мы составили перечень объектов КИИ, подлежащих категорированию, и отправили соответствующую информацию во ФСТЭК России. Сейчас часть объектов была выведена из эксплуатации / была объединена. Как поступить?**
В данном случае рекомендуется отправить обновленный перечень объектов КИИ, подлежащих категорированию. К перечню добавить сопроводительное письмо, в котором указать перечень объектов КИИ, который нужно удалить из списка ранее переданных, а также причины изменений. Рекомендуется приложить подтверждающие документы.	

Q&A	**Мы ранее провели категорирование своих объектов и отправили соответствующую информацию во ФСТЭК России. Сейчас часть объектов была выведена из эксплуатации / была объединена. Как поступить?**
В данном случае рекомендуется отправить во ФСТЭК России информационное письмо, в котором указать перечень объектов КИИ, который нужно удалить из списка ранее переданных, а также причины изменений. В случае, если объекты КИИ были объединены, то также, в соответствии с основной процедурой, высылаются результаты категорирования новых объектов. Рекомендуется приложить подтверждающие документы.	

Q&A	**Мы ранее провели категорирование своих объектов и отправили соответствующую информацию во ФСТЭК России. Сейчас часть объектов была изменена. Как поступить?**

В данном случае рекомендуется оценить изменения, которые были проведены в объектах:

- *изменены ли адреса размещения компонентов объекта?*
- *изменена ли архитектура объекта?*
- *изменились ли сети электросвязи, с которым взаимодействует объект или их характеристики?*
- *изменился ли функциональный состав компонентов объекта или перечень используемого системного и прикладного ПО (имеется в виду не добавление еще одного типового АРМ или сервера, а появление принципиально новых компонентов или изменение используемых технологий, например, использование виртуализации или Wi-Fi)?*
- *изменились ли подключения к сетям взаимодействия или новым ИС?*

В том случае, если на какой-либо из данных вопросов был дан положительный ответ, то необходимо обновить сведения о результатах категорирования и направить обновленную форму во ФСТЭК России с соответствующим сопроводительным письмом. В случае изменения функционально-технических характеристик объекта КИИ, очень вероятно, что изменятся перечни возможных нарушителей и/или угроз безопасности для объекта. В данном случае нужно будет провести новый анализ нарушителей и угроз, а в случае изменения перечня возможных угроз также провести новую оценку масштаба возможных последствий от нарушений безопасности объекта КИИ.

Q&A	**Мы ранее провели категорирование своих объектов и отправили соответствующую информацию во ФСТЭК России. Сейчас изменились автоматизируемые процессы. Как поступить?**

В данном случае рекомендуется провести новую оценку масштаба возможных последствий от нарушений безопасности объекта КИИ и в случае изменений в категории значимости объекта КИИ необходимо обновить сведения о результатах категорирования и направить обновленную форму во ФСТЭК России с соответствующим сопроводительным письмом.

Q&A	**Мы проектируем систему, потенциально являющуюся объектом КИИ. Предварительно провели ее категорирование и отправили соответствующую информацию во ФСТЭК России. В ходе проектирования в систему были внесены корректировки, в том числе в автоматизируемые процессы. Как поступить?**

В данном случае процедура изменения сведений о результатах категорирования аналогична описанным ранее: необходимо обновить сведения о результатах категорирования с указанием всех актуальных сведений о самом объекте, а также о результатах оценки возможного ущерба и присвоенной категории, и направить обновленную форму во ФСТЭК России с соответствующим сопроводительным письмом, поясняющим изменения.

Лист регистрации изменений

Версия	Дата	Описание изменений	№ стр.
1.0	22.10.2018	Создание	
1.1	12.12.2018	Уточнено определения статуса субъекта на основании комментариев ФСТЭК России	15
		Добавлен альтернативный упрощенный вариант определения критичности процессов на основании комментариев ФСТЭК России	30
		Добавлен комментарий ФСТЭК России по поводу ответственности за объекты КИИ, к которым организации предоставляется доступ, а также наши уточнения по данному комментарию	38
		Уточнение контактных данных ФСТЭК России, по которым отправляются результаты категорирования	40, 53
1.2	14.02.2019	Добавлена информация о готовящихся изменениях в ПП127	10
1.2	14.02.2019	Частично скорректированы примеры в Приложении 7	88-94
2	05.07.2019	Общие изменения, касающиеся выхода изменений 127ПП и приказа №236	-
2	05.07.2019	Обновлена информация о сроках категорирования и ответственности за нарушение сроков и порядка категорирования	9-10
2	05.07.2019	Корректировка сроков действия и условий расформирования Комиссии по категорированию	П. 1
2	05.07.2019	Корректировка состава Комиссии по категорированию и описание Комиссии по категорированию для филиальной структуры	23-25
2	05.07.2019	Уточнена область обследования процессов	29-30
2	05.07.2019	Уточнены правила информирования о создаваемых объектах КИИ	55
2	05.07.2019	Добавлена информация о необходимости повторного категорирования объектов КИИ после выхода изменений в 127ПП	56
2	05.07.2019	Добавлена форма отчета об обследовании объектов КИИ	66
2	05.07.2019	Добавлены рекомендации по оценке масштаба последствий	97
2.1	10.10.2019	Промежуточный вариант, используемый для обсуждения со специалистами ФСТЭК России	-
2.2	20.02.2020	Внесены доработки документа по результатам обсуждения со специалистами ФСТЭК России	-

Приложение 1

ПРИКАЗ № _____

г. _____ «___» _____ 201__ г.

о создании комиссии по категорированию объектов критической информационной инфраструктуры

В целях исполнения Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», утвержденные постановлением Правительства РФ от 08.02.2018 г. №127.

Приказываю:

1. Создать комиссию по категорированию объектов критической информационной инфраструктуры (далее — Комиссия).
2. Утвердить состав Комиссии согласно Приложению № 1 к настоящему приказу.
3. В своей работе комиссии по категорированию объектов КИИ руководствоваться Постановлением Правительства РФ 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» и Положением о комиссии по категорированию объектов критической информационной инфраструктуры (Приложение 2 к настоящему приказу).
4. Комиссии:
   - определить процессы в рамках осуществления видов деятельности ООО «Металлургический завод им. Джона Голта»;
   - выявить критические процессы, реализуемые ООО «Металлургический завод им. Джона Голта»;

- выявить объекты КИИ, которые обрабатывают информацию, необходимую для выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
- в срок до 01.09.2019 г. оформить и подготовить к утверждению перечень объектов КИИ, подлежащих категорированию;
- согласовать[4] перечень объектов КИИ, подлежащих категорированию, с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере;
- направить перечень объектов КИИ, подлежащих категорированию в ФСТЭК России для согласования в течение 5 рабочих дней после его утверждения;
- рассмотреть возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;
- провести анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
- оценить масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
- в срок до 01.09.2020 г. провести категорирование объектов КИИ, подлежащих категорированию, и оформить решение в виде актов категорирования;
- направить сведения о результатах категорирования в ФСТЭК России по присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения таких категорий (в течение 10 дней со дня утверждения актов категорирования);
- проводить корректировки данных и отвечать на соответствующие запросы в ходе процедуры категорирования объектов КИИ;
- обеспечить хранение актов категорирования до вывода из эксплуатации соответствующих объектов КИИ или до изменения категории значимости.

5. Контроль над исполнением настоящего приказа оставляю за собой.

Директор _____ *Джон Голт*

[4] Пункт актуален в случае применимости

Приложение № 1

к приказу от _____ 201_г. №__

С О С Т А В

комиссии по и категорированию объектов критической информационной инфраструктуры

Председатель комиссии: *Директор Джон Голт*

Ф.И.О,. должность

Члены комиссии: *Заместитель директора по безопасности, Дагни Таггарт*

Ф.И.О,. должность

Главный инженер, Хэнк Риарден

Ф.И.О,. должность

Начальник ГО и ЧС, Джеймс Таггарт

Ф.И.О,. должность

_____

Ф.И.О,. должность

_____

Ф.И.О,. должность

_____

Ф.И.О,. должность

Приложение № 2

к приказу от _____201_г. №__

Положение

О комиссии по категорированию объектов критической информационной инфраструктуры

1. Положение о комиссии по категорированию объектов критической информационной инфраструктуры (далее – Комиссия) определяет задачи Комиссии, ее права и порядок организации ее деятельности.
2. Состав Комиссии устанавливается приказом по Организации.
3. Задачи Комиссии

3.1 определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления деятельности Организации.

3.2 выявление критических процессов в рамках выполнения функций (полномочий) или осуществления деятельности Организации.

3.3 определение перечня объектов критической информационной инфраструктуры, принадлежащих Организации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов).

3.4 формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию в Организации.

3.5 рассмотрение возможных действий нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации.

3.6 анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры.

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

3.8 присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

4. Организация деятельности Комиссии.

4.1 Комиссия является постоянно действующим органом, проводящим заседания по мере необходимости.

4.2 Решение о проведении заседаний Комиссии принимается председателем Комиссии на основании предложений членов Комиссии.

4.3 Заседания Комиссии проводятся в случае присутствия не менее 50% численного состава постоянных членов Комиссии.

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

4.5 Комиссия вправе привлекать для решения частных задач работников организаций, экспертов сторонних организаций, представителей надведомственных организаций (без права голоса).

4.6 Решение Комиссии о включении объектов критической информационной инфраструктуры, принадлежащих Организации, в перечень объектов критической информационной инфраструктуры, подлежащих категорированию, оформляется актом Комиссии, подписывается всеми участниками Комиссии и утверждается Председателем Комиссии.

4.7 Решение Комиссии о присвоении объектам критической информационной инфраструктуры, принадлежащих Организации, одной из категорий значимости, а также решения об отсутствии необходимости присвоения категорий значимости оформляется актом категорирования, подписывается всеми участниками Комиссии и утверждается Председателем Комиссии.

4.8 По результатам заседания Комиссии, помимо решений, указанных в пунктах 4.6, 4.7 настоящего Положения, могут приниматься иные решения Комиссии, которые должны быть отражены в протоколе заседания Комиссии.

4.9 Проекты заключений и актов Комиссии, не позднее 5 календарных дней со дня проведения заседания, направляются Секретарем Комиссии всем членам Комиссии на подписание, за исключением Председателя Комиссии.

4.10 Срок подписания заключений и актов Комиссии членом Комиссии не может превышать 2 рабочих дней со дня получения от секретаря Комиссии.

4.11 Подписанные заключения и акты Комиссии направляются Секретарем Комиссии Председателю Комиссии на утверждение.

5. Протоколы заседаний Комиссии, заключения и акты должны храниться в Организации до вывода из эксплуатации соответствующих объектов критической информационной инфраструктуры или до изменения решений, принятых в указанных документах из-за изменений в работе Организации или самих объектов критической информационной инфраструктуры.

6. Комиссия по категорированию подлежит расформированию в следующих случаях:

6.1 прекращение Организацией выполнения функций (полномочий) или осуществления видов деятельности в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

6.2 ликвидация, реорганизация Организации и (или) изменение ее организационно-правовой формы, в результате которых были утрачены признаки субъекта критической информационной инфраструктуры.

Приложение 2

Шаблон Отчета об обследовании объектов критической информационной инфраструктуры

Отчет содержит информацию об ИС, ИТС и АСУ Организации, а также автоматизируемых ими процессах используемую в рамках процесса категорирования объектов КИИ в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127.

1. Определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры

В таблице ниже приводится перечень процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры.

Примечание к заполнению:

Наименования *желательно делать краткими и отражающими суть процесса, например: кадровое делопроизводство, оказание скорой медицинской помощи, учет медицинских препаратов, производство электроэнергии, учет и распределение электроэнергии, управление железнодорожными путями, предоставление государственной услуги по регистрации в очереди на прем к врачу, видеонаблюдение за территорией предприятия и т.д.*

Степень обобщенности или декомпозиции процессов произвольная, но для процессов, относящихся к основным видам деятельности Организации рекомендуется делать более детальное разделение.

Краткое описание *служит для определения границ деятельности, включаемой в процесс, подразделений, задействованных в нем и, возможно, используемых систем.*

Ответственный *- руководитель подразделения или работник, отвечающий за функционирование процесса (владелец процесса). Это лицо, которое может сделать оценку критичности последствий нарушения процесса и составить перечень систем, участвующих в автоматизации процесса.*

Принадлежность процесса к областям функционирования из 187-ФЗ *- отмечается участие процесса в соответствующей деятельность организации в рассматриваемых сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.*

№	Наименование процесса	Краткое описание	Ответственный	Принадлежность процесса к областям функционирования из 187-ФЗ
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

2. Выявление критических процессов

Критическими процессами считаются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Примечание:

В качестве критериев оценки может использоваться информация, представленная в таблице ниже. В случае, если для рассматриваемого процесса актуален какой-либо из указанных показателей, то процесс считается критическим.

№	Показатель	Критерий оценки актуальности показателей
I. Социальная значимость		
1	Причинение ущерба жизни и здоровью людей (человек)	Возможность причинения ущерба жизни и здоровью из-за нарушения рассматриваемого процесса (остановка процесса или сбой в нем / изменение параметров, в том числе выход за предел допустимых). Рассматриваются: 1. Непосредственные последствия от нарушения технологических процессов, связанные с угрозой для работников и людей, находящихся в близости от оборудования (выработка электроэнергии, химическое производство, управление металлургическим производством и т.д.); 2. Последствия, связанные с нарушением процесса как оказываемой услуги, и представляющие угрозу для потребителей услуги (управление движением железно-дорожных составов, оказание срочной медицинской помощи, фармацевтическая деятельность, производство транспортных средств и т.д.).
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Актуален для процессов, участвующих в обеспечении жизнедеятельности населения (водо-, тепло-, газо- и электроснабжение), нарушение которых может привести к прекращению оказания данных услуг (прекращение подачи воды, тепла, газа, электричества) или к отклонению значений параметров указанных услуг от проектных (штатных) режимов функционирования (падение напряжения электросети, снижение температуры или напора горячей воды/теплоносителя и т.д.).

№	Показатель	Критерий оценки актуальности показателей
		В рассматриваемых масштабах нарушение объектов обеспечения жизнедеятельности самого субъекта КИИ не попадает в критичные значения, то есть аварии на котельной предприятия, на локальных распределительных щитах, канализации и т.д. не являются достаточным фактором, если они не повлекли последствия в более обширном масштабе, в рамках оказания соответствующих услуг населению
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Актуален для процессов, связанных с управлением объектами транспортной инфраструктуры[5], нарушение которых может привести к прекращению функционирования данных объектов (нарушение работы транспорта) или к отклонению значений параметров функционирования данных объектов от проектных (штатных) режимов функционирования (сбои в движении электропоездов, задержки в регистрации пассажиров, багажа, сбои в работе трубопровода, связанные с изменением давления и т.д.)
4	Прекращение или нарушение функционирования сети связи	Актуален для процессов, связанных с управлением сетью связи[6], нарушение которых может привести к прекращению функционирования сети связи или к отклонению значений параметров функционирования сетей связи от проектных (штатных) режимов функционирования (сбои в передачи данных, падение скорости передачи данных, потеря пакетов и т.д.). Данный критерий актуален для организаций, предоставляющих услуги связи. Должны рассматриваться процессы управления каналообразующим оборудованием, обеспечения доступности услуг связи и т.д. Нарушение ЛВС самого субъекта КИИ не попадает в рассматриваемые критерии, то есть отказ ЛВС субъекта не являются достаточным фактором, если они не повлекли последствия в рамках оказания услуг связи.
5	Отсутствие доступа к государственной услуге	Актуален для процессов, связанных с предоставлением государственных услуг[7], нарушение которых может привести к прекращению доступа к предоставляемым государственным услугам (автоматизация государственных услуг с помощью ГИС и связанных систем). Данный критерий должен рассматриваться организациями, на которых возложены соответствующие обязанности по оказанию государственных услуг. Участники предоставления государственных услуг, чьи процессы должны анализироваться, определяются в частных регламентах предоставления государственных услуг.

[5] В соответствии с 16-ФЗ от 09.02.2007 "О транспортной безопасности"
[6] в соответствии с 126-ФЗ от 07.07.2003 "О связи"
[7] в соответствии с 210-ФЗ от 27.07.2010 "Об организации предоставления государственных и муниципальных услуг"

№	Показатель	Критерий оценки актуальности показателей
II. Политическая значимость		
6	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Актуален для процессов, связанных с реализацией функций (полномочий), возложенных на органы власти, нарушение которых может привести к прекращению реализации указанных функций (полномочий) (невозможность оказания государственных услуг, регистрации или предоставления соответствующей информации и т.д.) или к отклонению значений параметров реализации указанных функций (полномочий) от проектных (штатных) режимов (нарушение сроков реализации полномочий, временный переход на бумажный документооборот, возможность реализации полномочий с привлечением дополнительных ресурсов и т.д.).
7	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации	Актуален для процессов, • реализуемых во исполнение международных договоров; • реализуемых в рамках преддоговорных условий; • реализация которых способна оказать влияние на переговоры или подписание планируемого к заключению международного договора.
III. Экономическая значимость		
8	Возникновение ущерба субъекту КИИ, который является государственной корпорацией, ГУП, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием[8]	Актуален для процессов: 1. Являющихся источниками доходов указанных субъектов (остановка производства, транспортного процесса и т.д.); 2. Нарушение которых способны повлечь причинение прямого финансового ущерба (техногенные катастрофы, пожары, взрывы, затопления и т.д.).
9	Возникновение ущерба бюджетам Российской Федерации	Актуален для процессов, связанных с производственной деятельностью, оказанием услуг или иной деятельностью, являющейся источником пополнения бюджета в виде налогов, акцизных и иных

[8] В соответствии с перечнем стратегических предприятий и стратегических акционерных обществ, утвержденным Указом Президента Российской Федерации от 4 августа 2004 г. N 1009 "Об утверждении перечня стратегических предприятий и стратегических акционерных обществ".

№	Показатель	Критерий оценки актуальности показателей
		платежей. Должны рассматриваться любые процессы, нарушение которых приведет к уменьшению каких-либо выплат в бюджеты РФ: остановка производства, транспортного процесса и т.д. Нарушение процессов, связанных непосредственно с проведением выплат в бюджеты РФ (бухгалтерские процессы и процессы перевода денежных средств) не влечет прямого ущерба, так как выплаты в любом случае будут осуществлены (позже или с использованием бумажных носителей и иных форм отчетности), данные процессы не стоит относить к критическим по данному критерию
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	Актуален для процессов: 1. связанных с реализацией проведения клиентами операций по банковским счетам и (или) без открытия банковского счета, нарушение которых может привести к прекращению указанных операций или к отклонению значений параметров указанных операций от проектных (штатных) (сбои в транзакциях, увеличение времени обработки транзакций и т.д.); 2. связанных с реализацией операций, осуществляемых: • системно значимой кредитной организацией[9]; • оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем[10]; • системно значимой инфраструктурной организацией финансового рынка[11], нарушение которых может привести к прекращению указанных операций или к отклонению значений параметров указанных операций от проектных (штатных) (сбои в транзакциях, увеличение времени обработки транзакций и т.д.)

[9] В соответствии с Указанием Банка России от 22 июля 2015 г. N 3737-У «О методике определения системно значимых кредитных организаций»

[10] В соответствии со ст. 22 Федерального закона от 27 июня 2011 г. 161-ФЗ «О национальной платежной системе»

[11] В соответствии с Указанием Банка России от 25 июля 2014 г. № 3341-У «О признании инфраструктурных организаций финансового рынка системно значимыми»

№	Показатель	Критерий оценки актуальности показателей
IV. Экологическая значимость		
11	Вредные воздействия на окружающую среду	Актуален для процессов, связанных с технологическими операциями и производством, нарушение которых может оказать непосредственное негативное воздействие на окружающую среду: ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия. Примеры критических процессов: обогащение руды, производство серной кислоты, утилизации отходов термической обработкой, транспортировка нефтепродуктов, контроль состояния и поставка фильтров для производства, налив, хранение и транспортировка нефтепродуктов. Примеры смежных процессов, которые могут не являться критичными: обеспечение физической безопасности и контроль доступа (СКУД), видеонаблюдение, электроснабжение (если его подача ведет к безопасному останову производства без соответствующих последствий). При оценке актуальности показателя для процесса необходимо рассматривать максимально негативный сценарий развития нарушения процесса, 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, например системы РАС и ПАЗ не рассматриваются как фактор, снижающий риск, а Физические блокировки и ограничители можно принимать в расчет)
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка		
12	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра)	Актуален для процессов, связанных с обеспечением функционирования пунктов управления (ситуационных центров), нарушение которых может привести к прекращению функционирования пунктов управления (ситуационных центров) или к отклонению значений параметров функционирования от проектных (штатных) режимов (нарушение сроков реагирования, частичное нарушение импортируемой в ситуационный центр информации, ограничение числа пользователей ситуационного центра и т.д.).
13	Снижение показателей государственного оборонного заказа, выполняемого	Актуален для процессов, связанных с выполнением оборонного заказа, нарушение которых может привести к снижению объемов продукции или к увеличению времени выпуска продукции данного

№	Показатель	Критерий оценки актуальности показателей
	(обеспечиваемого) субъектом критической информационной инфраструктуры	заказа (технологические, производственные процессы и процессы, поддерживающие их: поставка сырья, транспорт и т.д.). Данный показатель актуален для организаций, непосредственно выполняющих (обеспечивающих) государственный оборонный заказ[12]: головных исполнителей поставок продукции по государственному оборонному заказу, исполнителей, участвующих в поставках продукции по государственному оборонному заказу, участников кооперации головного исполнителя. Для организаций, которые не относятся к указанным лицам, но которые изготавливают какие-либо компоненты или предоставляют услуги, которыми в свою очередь пользуются указанные организации для выполнения государственного оборонного заказа, данный показатель не является актуальным
14	Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	Актуален для процессов, связанных с обеспечением функционирования информационных систем в области обеспечения обороны страны, безопасности государства и правопорядка, нарушение которых может привести к прекращению функционирования указанных систем или к отклонению значений параметров функционирования данных систем от проектных (штатных) режимов. В общих случаях рассматриваются непосредственно процессы: • управления и сопровождения указанных систем; • предоставления доступа к указанным системам; • информационного обеспечения указанных систем
15	Процесс обеспечивает функционирование объектов КИИ, принадлежащих другим субъектам	Актуален для процессов обеспечения функционирования объектов КИИ, принадлежащих другим субъектам

Выявление критических процессов проводится экспертно, сформированной комиссией по категорированию на основании сведений о деятельности организации, запрашиваемых дополнительных сведений для конкретных показателей. Результаты выявления критических процессов приводятся в таблице ниже.

[12] в соответствии с Федеральным законом от 29.12.2012 N 275-ФЗ «О государственном оборонном заказе»

№	Показатель	Актуальность для процессов[13]									
		П1	П2	П3	П4	П5	П6	П7	П8	П9	П10
1	Причинение ущерба жизни и здоровью людей (человек)										
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения										
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры										
4	Прекращение или нарушение функционирования сети связи										
5	Отсутствие доступа к государственной услуге										
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										
8	Возникновение ущерба субъекту КИИ, который является государственной корпорацией, ГУП, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием										
9	Возникновение ущерба бюджетам Российской Федерации										

[13] Да/нет

№	Показатель	Актуальность для процессов[13]									
		П1	П2	П3	П4	П5	П6	П7	П8	П9	П10
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										
11	Вредные воздействия на окружающую среду										
12	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра)										
13	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры										
14	Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка										
15	Процесс обеспечивает функционирование объектов КИИ, принадлежащих другим субъектам										

№	Показатель	Актуальность для процессов[13]									
		П1	П2	П3	П4	П5	П6	П7	П8	П9	П10
Критичность процесса											

3. Определение объектов критической информационной инфраструктуры

В таблице ниже приведен сводный перечень объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов.

№	Критические процессы	Наименование объекта	Тип объекта (ИС / АСУ ТП / ИТС)	Ответственный за объект
О1	П1			
О2				
О3				
О4				
О5	П2			
О6				
О7	П3			
О8				
О9				
О10				
О11				
О12				

4. Информация об объектах КИИ

В данном разделе приводится сводная информация об объектах КИИ, определенных в предыдущем пункте. Данная информация используется для заполнения указанной формы, а также для анализа сведений о потенциальных нарушителях безопасности и потенциальных угрозах ИБ.

4.1 *Информация об Объекте О1*[14]

Общие сведения об объекте КИИ		
1.1	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	
1.2	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
1.4	Назначение объекта	
1.5	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	
1.6	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	
1.7	Роль объекта (управление процессом, информационное обеспечение процесса, мониторинг и контроль процесса)	
1.8	Состав информации, подлежащей защите	
Сведения о взаимодействии объекта КИИ и сетей электросвязи		

[14] Заполняется для каждого объекта КИИ, подлежащего категорированию

2.1	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	
2.2	Наименование оператора связи и (или) провайдера хостинга	
2.3	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
2.4	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	
Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ		
3.1	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	
3.2	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	
3.3	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	
3.4	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	
3.5	Использование отчуждаемых носителей	
3.6	Использование терминального доступа пользователей	
3.7	Использование технологий удаленного доступа пользователей	

3.8	Использование удаленного доступа администраторов и/или разработчиков	
3.9	Использование грид-вычислений	
3.10	Использование виртуализации	
3.11	Использование беспроводного доступа	
3.12	Использование веб-приложений	
3.13	Использование облачных технологий	
3.14	Использование суперкомпьютеров	
3.15	Использование технологий Big Data	
3.16	Использование мобильных устройств	
Функциональная схема объекта КИИ		
Приводится Функциональная схема объекта КИИ		
Сетевая схема объекта КИИ		
Приводится Сетевая схема объекта КИИ (L2/L3)		

5. Анализ возможных действий нарушителей в отношении объектов КИИ

В данном разделе приводится перечень типов возможных нарушителей и их характеристики: 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. Данные ниже приведены в качестве примера и основаны на проекте Методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (могут быть использованы иные модели на усмотрение субъектов КИИ) - из них необходимо выбрать актуальные типы нарушителей и соответствующие им характеристики, актуальные для рассматриваемого случая.

1. **Внешние нарушители с низким потенциалом**

   Возможные типы нарушителей:

   - Хакеры;
   - Бывшие работники;
   - Операторы сетей связи;
   - Операторы смежных систем, используемых для работы объекта КИИ.

2. **Внешние нарушители со средним потенциалом**

   Возможные типы нарушителей:

   - Хакерские группировки;
   - Конкурирующие организации;
   - Преступные группы (криминальные структуры);
   - Разработчики системного и прикладного ПО, программно-аппаратной платформы без возможности доступа к системе в промышленной эксплуатации.

3. **Внешние нарушители с высоким потенциалом**

   Возможные типы нарушителей:

   - Специальные службы иностранных государств (блоков государств).

4. **Внутренние нарушители с низким потенциалом**

   Возможные типы нарушителей:

   - Посетители, которым предоставляется доступ в ЛВС Организации;
   - Работники Организации, не имеющие санкционированного доступа к объекту КИИ;
   - Работники смежных организаций, которым предоставляется доступ в ЛВС организации (группа компаний, потребители сервисов и т. д.);

- Лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т. д.);
- Лица, обеспечивающие функционирование информационных систем или инфраструктуры оператора (сотрудники ЦОД, ремонтные бригады, электромонтажники и т.д.);
- Пользователи Объекта КИИ.

5. Внутренние нарушители со средним потенциалом

Возможные типы нарушителей:

- Разработчики прикладного ПО системы с возможностью доступа для обновления/поддержки;
- Организации, предоставляющие услуги по сопровождению системы и/или предоставляющие сервисы (мониторинг событий, анализ уязвимостей и т. д.).
- Администратор ИС (в случае выделения в качестве нарушителя, а не доверенного лица);
- Администратор ЛВС (в случае выделения в качестве нарушителя, а не доверенного лица);
- Администратор ИБ (в случае выделения в качестве нарушителя, а не доверенного лица).

6. Внутренние нарушители с высоким потенциалом

Возможные типы нарушителей:

- Определяются в частных случаях для конкретных организаций.

Возможные характеристики нарушителей:

Оснащенность нарушителей:

- обладают доступными в свободной продаже техническими средствами и программным обеспечением, средствами разработки и отладки ПО, аппаратно-программными средствами перехвата и анализа информационного потока;
- обладают специально разработанными техническими средствами и ПО;
- имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок.
- имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее.
- имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

Знания нарушителей:

- обладают информацией о системе, доступной из открытых источников;

- имеют возможность получить информацию об уязвимостях отдельных компонент ИС, опубликованную в общедоступных источниках;
- имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему;
- имеют осведомлённость о мерах защиты информации, применяемых в ИС данного типа;
- имеют возможность получить информацию об уязвимостях отдельных компонент ИС путём проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения;
- имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
- имеет возможность получать дополнительную информацию с помощью методов социальной инженерии
- потенциально обладает данными, передаваемыми в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационно-техническими мерами
- имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе
- имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения

Мотивация нарушителей:

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;
- реализация угроз безопасности информации по идеологическим или политическим мотивам;
- организация террористического акта;
- причинение имущественного ущерба путем мошенничества или иным преступным путем;
- дискредитация или дестабилизация деятельности органов государственной власти, организаций;
- получение конкурентных преимуществ;
- внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;
- любопытство или желание самореализации;
- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- реализация угроз безопасности информации из мести;
- реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

Каналы реализации угроз:

- компоненты системы и съемные носители информации, выносимые за пределы КЗ;
- общедоступные каналы передачи данных, имеющие подключение к ИС;
- каналы связи, по которым осуществляется передача защищаемой информации, выходящие за пределы КЗ;
- сервисы, используемые пользователями ИС: электронная почта, сайты и т. д.
- технические каналы утечки;
- канал утечки за счет электронных устройств негласного получения информации;
- программное обеспечение ИС на стадии его разработки;
- технические средства ИС на стадии их разработки;
- каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);
- реализация атак посредством направленных воздействий на работников организации (социальная инженерия);
- использование штатных средств доступа к ИС;

Возможные нарушения:

- выявление и попытка эксплуатации уязвимостей компонентов ИС;
- попытки перехвата или нарушения целостности трафика, передаваемого по сети связи;
- направленные атаки на получение идентификационных и аутентификационных данных пользователей или непосредственно на механизмы авторизации в ИС;
- информационная разведка средствами социальной инженерии;
- внедрение вредоносного кода;
- блокирование работы сетевых сервисов ИС с помощью удаленных атак (атаки типа «отказ в обслуживании»;
- несанкционированный доступ через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами КЗ;
- внесение ошибок, недекларированных возможностей, программных и аппаратных закладок, вредоносных программ в программное и аппаратное обеспечение ИС на стадии разработки, внедрения и сопровождения;
- непреднамеренное или намеренное воздействие на компоненты ИС и средства обеспечения работоспособности (электропитание, кондиционирование и т.д.);
- нарушение целостности конфигурации компонентов ИС и/или средств защиты;
- нарушение работоспособности аппаратных и/или программных компонентов;
- нарушение работоспособности общесистемного или прикладного ПО, сетевой инфраструктуры и средств защиты;
- несанкционированный доступ к защищаемым данным, обрабатываемым в ИС;
- перехват управления / подмена управляющих команд для компонентов ИС или оборудования, управляемого АСУ.

6. Анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ

В данном разделе проводится анализ возможных угроз безопасности информации объекта КИИ и компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации.

Проведение полного моделирования угроз с детальным анализом всех угроз безопасности информации, содержащихся в БДУ ФСТЭК России на данном этапе не требуется, поэтому предлагается выбрать перечень основных видов угрозы безопасности информации, которые возможны для объекта КИИ. На данном этапе возможно использование перечня угроз, представленного в БДУ ФСТЭК России, но он является излишне детализированным для данной ступени работ.

Необходимо сопоставить реально существующие защищаемые активы объекта КИИ, актуальные свойства безопасности данных активов и выбрать возможные угрозы безопасности для данных активов с учетом его функционально-технических характеристик и возможностей нарушителей безопасности. Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, определяются исходя из перечня возможных угроз безопасности и нарушаемых свойств безопасности защищаемых активов.

Анализ возможных угроз безопасности информации объекта КИИ и компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации проводится **для каждого объекта КИИ, подлежащего категорированию**.

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
Защищаемая информация, обрабатываемая в ИС, данные о производстве и т.д.	Нарушение конфиденциальности	- угроза несанкционированной передачи/распространения данных ограниченного доступа; - угроза внедрения вредоносного ПО; - угроза подмены объектов сетевого доступа; - угроза подмены субъектов сетевого доступа; - угроза создания ложного сетевого маршрута; - угроза несанкционированного доступа с использованием компрометированных / подобранных данных идентификации и аутентификации пользователей и администраторов; - угроза доступа к информации в обход или с использованием ошибок в настройке средств разграничения доступа; - угроза перехвата информации в каналах передачи данных; - угроза реализации атак на беспроводную сеть передачи данных; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО	- несанкционированный доступ к обрабатываемой информации; - утечка данных (нарушение конфиденциальности)
	Нарушение целостности	- угроза несанкционированного или ошибочного изменения/подмены данных в системе; - угроза внедрения вредоносного ПО; - угроза подмены объектов сетевого доступа; - угроза подмены субъектов сетевого доступа; - угроза создания ложного сетевого маршрута; - угроза несанкционированного доступа с использованием компрометированных / подобранных данных идентификации и аутентификации пользователей и администраторов; - угроза доступа к информации в обход или с использованием ошибок в настройке средств разграничения доступа; - угроза модификации данных при их передаче по каналам передачи;	- несанкционированный доступ к обрабатываемой информации; - модификация (подмена) данных - отказ в обслуживании - несанкционированное использование вычислительных ресурсов объекта

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
		- угроза реализации атак на беспроводную сеть передачи данных; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО	
	Нарушение доступности	- угроза несанкционированного удаления данных, обрабатываемых в системе; - угроза нарушения работоспособности системного ПО; - угроза нарушения работоспособности прикладного ПО; - угроза нарушения работоспособности сетевых сервисов; - угроза нарушения работоспособности СУБД; - угроза нарушения работоспособности виртуальной инфраструктуры; - угроза внедрения вредоносного ПО; - угроза проведения атак типа «отказ в обслуживании» на компоненты системы; - угроза проведения атак типа «отказ в обслуживании» на каналы связи; - угроза несанкционированного доступа с использованием компрометированных / подобранных данных идентификации и аутентификации пользователей и администраторов; - угроза занятия вычислительных ресурсов системы; - угроза нарушения режимов функционирования программно-технических средств; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО;	- несанкционированный доступ к обрабатываемой информации; - утрата информации - отказ в обслуживании - нарушение функционирования технических средств, - несанкционированное использование вычислительных ресурсов объекта

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
		- угроза нарушения доступности данных, которые должны поступать из смежных систем; - угроза создания нештатных режимов работы	
Конфигурация ИС, настройки технологического процесса, управляющие команды в АСУ ТП	Нарушение конфиденциальности	- угроза несанкционированного доступа к конфигурации системы / раскрытия данных технологического процесса; - угроза внедрения вредоносного ПО; - угроза несанкционированного доступа с использованием компрометированных / подобранных данных идентификации и аутентификации пользователей и администраторов; - угроза доступа к информации в обход или с использованием ошибок в настройке средств разграничения доступа; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО.	- несанкционированный доступ к обрабатываемой информации; - утечка данных (нарушение конфиденциальности)
	Нарушение целостности	- угроза несанкционированного изменения / подмены конфигурации, настроек технологического процесса, управляющих воздействий; - угроза несанкционированного изменения / подмены данных, управляющих команд, передаваемых по каналам связи; - угроза внедрения вредоносного ПО; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО.	- несанкционированный доступ к обрабатываемой информации; - несанкционированный доступ к управлению объектом; - модификация (подмена) данных; - нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании модификация (подмена) данных, нарушение функционирования технических

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
			средств, несанкционированное использование вычислительных ресурсов объекта
	Нарушение доступности	- угроза несанкционированного удаления конфигурационных файлов; - угроза блокирования передаваемых управляющих команд; - угроза внедрения вредоносного ПО; - угроза использования недекларированных возможностей / закладок системного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО - угроза создания нештатных режимов работы	- несанкционированный доступ к обрабатываемой информации; - утрата информации; - нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании - модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта
Системное ПО	Нарушение целостности	- угроза несанкционированной модификации системного ПО; - угроза несанкционированной модификации виртуальной инфраструктуры; - угроза внедрения вредоносного ПО; - угроза использования недекларированных возможностей / закладок системного ПО	- несанкционированный доступ к управлению объектом; - модификация (подмена) данных; - нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
	Нарушение доступности	- угроза нарушения работоспособности системного ПО; - угроза нарушения работоспособности виртуальной инфраструктуры; - угроза внедрения вредоносного ПО; - угроза проведения атак типа «отказ в обслуживании» на компоненты системы; - угроза нарушения режимов функционирования программно-технических средств; - угроза использования недекларированных возможностей / закладок системного ПО - угроза создания нештатных режимов работы	- нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании
Прикладное ПО	Нарушение целостности	- угроза несанкционированной модификации прикладного ПО; - угроза несанкционированной модификации сетевых сервисов; - угроза несанкционированной модификации СУБД; - угроза внедрения вредоносного ПО; - угроза использования недекларированных возможностей / закладок прикладного ПО	- несанкционированный доступ к управлению объектом; - модификация (подмена) данных; - нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта
	Нарушение доступности	- угроза нарушения работоспособности прикладного ПО; - угроза нарушения работоспособности сетевых сервисов; - угроза нарушения работоспособности СУБД; - угроза внедрения вредоносного ПО; - угроза проведения атак типа «отказ в обслуживании» на компоненты системы; - угроза использования недекларированных возможностей / закладок прикладного ПО - угроза создания нештатных режимов работы	- нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании
Аппаратные компоненты	Нарушение доступности	- угроза внедрения вредоносного ПО; - угроза проведения атак типа «отказ в обслуживании» на компоненты системы; - угроза занятия вычислительных ресурсов системы;	- нарушение функционирования технических средств; - несанкционированное использование

Актив	Нарушение ИБ	Возможные угрозы безопасности	Типы компьютерных инцидентов
		- угроза нарушения режимов функционирования программно-технических средств; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО - угроза создания нештатных режимов работы	вычислительных ресурсов объекта - отказ в обслуживании
Каналы связи	Нарушение доступности	- угроза несанкционированной модификации сетевых сервисов; - угроза нарушения работоспособности сетевых сервисов; - угроза проведения атак типа «отказ в обслуживании» на каналы связи; - угроза создания ложного сетевого маршрута; - угроза реализации атак на беспроводную сеть передачи данных; - угроза занятия вычислительных ресурсов системы; - угроза нарушения режимов функционирования программно-технических средств; - угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); - угроза использования недекларированных возможностей / закладок системного ПО - угроза создания нештатных режимов работы	- нарушение функционирования технических средств; - несанкционированное использование вычислительных ресурсов объекта - отказ в обслуживании

Для каждого объекта КИИ проводится оценка возможных последствий от актуальных компьютерных инцидентов.

Оценка возможных последствий от актуальных компьютерных инцидентов проводится с учетом развития инцидента по максимальному негативному сценарию, без учета существующих защитных мер (антивирусов, межсетевых экранов, систем противоаварийной автоматики, систем защит и т.д.). Прогноз возможного развития аварии или сбоя делается без учета существующих аварийных систем (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака в целом не рассматривается). Например: системы РАС и ПАЗ не рассматриваются как фактор, снижающий риск. Физические блокировки и ограничители можно принимать в расчет;

Расчет времени нарушения работоспособности из-за компьютерных инцидентов осуществляется с учетом существующих процессов и мер по обеспечению восстановления, результатов тестирования процедур или, как минимум, прогноза восстановления процессов, систем, данных. Идеальным вариантом являются результаты BIA, расчеты DRP, а также требования SLA в случае, если соответствующие услуги оказываются в данном виде.

Примеры:

При оценке последствий от утери данных следует допускать, что вся защищаемая информация будет утеряна и необходимо оценить какой ущерб будет от этого (насколько будут остановлены зависимые процессы, сколько потребуется для перезапуска и возможен ли он?). Если существует процесс резервного копирования, то необходимо сделать оценку времени простоя до предполагаемого восстановления данных и устранения последствий инцидента. Как пример: реагирование на вирусную атаку - 1 час, изоляция/пресечение эпидемии, принятие решения об использовании резервных площадок или иных сценариев - 2 часа, восстановление данных и ввод системы в строй - 3 часа. Соответственно, расчетное прерывание связанных процессов составит 19 часов.

Хакеры взламывают АСУ ТП, изменяют данные техпроцесса и выводят агрегат за пределы допустимых значений. Теоретически последствия могут включать: аварийный останов с необходимостью перезапуска агрегата, необходимость профилактического осмотра, ремонта, замены частей агрегата, необходимость замены агрегата, устранение последствий от аварии в случае развития инцидента в техногенную катастрофу. Так как необходимо рассматривать максимальный

негативный сценарий без учета мер защиты (систем противоаварийной автоматики, систем защит и т.д.), то определяются соответствующие последствия. С учетом наличия физических защит возможно выведения агрегата из строя на время, требуемое для его ремонта (замены, если теоретически возможны такие последствия).

№	Актуальные типы компьютерных инцидентов	Оценка возможных последствий

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

Оценка возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ осуществляется на основании выявленных типов инцидентов для объекта КИИ (см. предыдущий раздел) и анализа возможного ущерба, связанного с данными инцидентами. Оценка возможных последствий осуществляется по каждому из рассчитываемых показателей критериев значимости, приведенных в «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127.

Результаты оценки возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ приводятся в таблицах ниже *(заполняется **для каждого объекта КИИ**)*.

№	Показатель	Оценка	Обоснование оценки	Значение показателя критичности
I. Социальная значимость				
1	Причинение ущерба жизни и здоровью людей (человек)			
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;			
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)			
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры			
	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)			

№	Показатель	Оценка	Обоснование оценки	Значение показателя критичности
4	Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, 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)			
II. 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			
III. Экономическая значимость				
8	Возникновение ущерба субъекту КИИ, который является государственной корпорацией, ГУП, государственной компанией, 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)			
9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)			
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			

№	Показатель	Оценка	Обоснование оценки	Значение показателя критичности
	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, 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)			
IV. Экологическая значимость				
11	Вредные воздействия на окружающую среду			
	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;			
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)			
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
12	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра			
13	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры			
	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 (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)			

Ниже приводятся предложения по проведению оценки возможных последствий в результате возникновения компьютерных инцидентов на объектах КИИ:

1) Причинение ущерба жизни и здоровью людей

Должна оцениваться возможность причинения ущерба жизни и здоровью из-за нарушения ИБ рассматриваемого объекта. При этом, в том числе, 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 (железнодорожные стрелки, светофоры/семафоры, сброс воды на ГЭС и т.д.), 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). Пример: системы РАС и ПАЗ, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки. При этом физические блокировки и ограничители можно принимать в расчет.

При оценке и в качестве обоснования рекомендуется использовать данные:

- паспортов безопасности опасного производственного объекта;
- паспортов безопасности объектов ТЭК;
- декларации промышленной безопасности объекта;
- плана действий по предупреждению и ликвидации чрезвычайных ситуаций природного и техногенного характера;
- результатов категорирования объектов, оказывающих негативное воздействие на окружающую среду.

Для данного критерия существуют некоторые пограничные ситуации, которые субъект должен оценивать в каждом отдельном случае:

Использование медицинского оборудования:

- позволяет ли оборудование установить параметры воздействия, превышающие предельно допустимые для человека и способные причинить вред здоровью? Отображаются ли данные параметры с помощью изолированных приборов и способен ли медицинский персонал выявить отклонения до проведения процедуры?
- используется ли медицинское оборудование как автоматическая система, передающая управляющее воздействие для проведения каких-либо воздействий на людей без участия медицинского персонала с возможностью проверки действий (собран материал – сделан анализ – введено лекарство)?

Использование медицинских систем:

- Используется ли исключительно электронный документооборот, без контроля и проверки медицинским персоналом состояния пациентов, противопоказаний и т.д.?

Производство транспортных средств и иной продукции, отказ которой может повлечь угрозу для жизни людей:

- Реализован ли процесс тестирования и контроля качества?

– Возможен ли выпуск не протестированной бракованной продукции, в результате эксплуатации/использования которой может возникнуть угроза для жизни и здоровья людей?

Системы пожаротушения:

– возможна ли активация систем пожаротушения, опасных для людей, с физической изоляцией помещений (блокирование дверей без возможности выхода), в которых может находиться персонал?
– есть ли аварийные системы и механизмы?

Системы оповещения, диспетчеризации спасателей, аварийных служб и т.д.:

– в общем случае нарушение работ соответствующих систем само по себе не ведет к человеческим жертвам – люди могут умереть от травм, катастроф и т.д., но не непосредственно от отказа данных систем, поэтому данный критерий рекомендуется не считать актуальным для подобных объектов.

2) Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения

Должна оцениваться возможность нарушения или ухудшения условий обеспечения жизнедеятельности населения: водо-, тепло-, газо- и электроснабжения населения. Данный критерий касается систем управления соответствующими объектами снабжения, способных передавать управляющие воздействия на исполнительные устройства, а также систем мониторинга их состояния, если на основании данных мониторинга могут приниматься управляющие решения в автоматизированном режиме.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы объектов снабжения: нарушение параметров техпроцесса, выдача команд останова, сбои или нарушение работоспособности управляющих или исполнительных механизмов и т.д.

Масштаб возможного ущерба относительно территории, на которой возможно нарушение обеспечения жизнедеятельности населения оценивается на основании сведений об объектах (районах), подключенных к рассматриваемому объекту снабжения.

Масштаб возможного ущерба относительно количества людей, условия жизнедеятельности которых могут быть нарушены оценивается на основании сведений о числе потребителей, подключенных к рассматриваемому объекту

снабжения (на основании сведений распределяющих компаний, расчетных центров, сведений о населении подключенных объектов/районов и т.д.).

Так как в критерии не указана рассматриваемая длительность нарушения функционирования, то оценке подлежит в том числе кратковременный сбой в работе (кратковременный сбой подачи водоснабжения, электроэнергии и т.д.).

В рассматриваемых масштабах нарушение объектов обеспечения жизнедеятельности самого субъекта не попадает в критичные значения, то есть аварии на котельной предприятия, на локальных распределительных щитах, канализации и т.д. не являются достаточным фактором, если они не повлекли последствия в более обширном масштабе.

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). Пример: системы РАС и ПАЗ, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки. При этом физические блокировки и ограничители можно принимать в расчет.

3) Прекращение или нарушение функционирования объектов транспортной инфраструктуры

Должна рассматриваться возможность нарушения функционирования объектов транспортной инфраструктуры (определение см. в 16-ФЗ от 09.02.2007 «О транспортной безопасности»). Данный критерий касается систем, осуществляющих управление (способные передавать управляющие воздействия на исполнительные устройства) и мониторинг (если на основании данных мониторинга могут приниматься управляющие решения в автоматическом режиме) данными объектами транспортной инфраструктуры (например: железнодорожными стрелками, авиадиспетчеризация, управление шлюзами трубопроводом и т.д.). Прежде всего - это объекты средств управления движением в терминологии 16-ФЗ.

Должны рассматриваться инциденты, из-за которых возможно нарушение функционирования объектов транспортной инфраструктуры: нарушение параметров процессов управления, диспетчеризации, выдача команд останова или неверных

команд управления, сбои или нарушение работоспособности управляющих или исполнительных механизмов и т.д.

Масштаб возможного ущерба относительно территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг должен оцениваться на основании паспорта объекта транспортной инфраструктуры и сведений о статусе управляемого объекта транспортной инфраструктуры, функционирование которого может быть нарушено. Так как в критерии не указана рассматриваемая длительность нарушения функционирования, то рассмотрению подлежит в том числе кратковременный сбой в работе (кратковременный сбой в работе светофоров во всем районе города).

Масштаб возможного ущерба относительно количества людей, для которых могут быть недоступны транспортные услуги, должен оцениваться на основании паспортных и / или статистических данных о пропускной способности, обеспечиваемой рассматриваемым объектом транспортной инфраструктуры. Время, за которое оценивается указанный показатель определяется как расчетное время восстановления функционирования объекта. В случае, если данные планы отсутствуют, необходима экспертная оценка группы по категорированию и ответственных лиц.

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). Пример: системы РАС и ПАЗ, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки. При этом физические блокировки и ограничители можно принимать в расчет.

4) Прекращение или нарушение функционирования сети связи[15]

Должна оцениваться возможность нарушения функционирования сетей связи, с помощью которых предоставляются услуги связи (в соответствии с 126-ФЗ «О связи»). Данный критерий касается систем управления сетью связи.

[15] Данный пункт рекомендуется оценивать в соответствии с рекомендациями документа «Методические рекомендации по категорированию объектов критической информационной

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы сетей связи: нарушение коммутации, нарушение работоспособности оборудования, атаки типа «отказ в обслуживании», блокирующие доступ к сети связи и т.д.

В рамках данного критерия не стоит рассматривать локальные или корпоративные сети связи, в том числе распределенные, если они не используются для оказания услуг третьим лицам (используются только для собственных нужд).

Масштаб возможного ущерба оценивается в виде числа абонентов, для которых могут стать недоступны услуги связи (на основании сведений о заключенных договорах и имеющихся обязанностей по предоставлению услуг связи, предоставляемых с использованием рассматриваемого объекта КИИ). В случае предоставления услуг не конечным потребителям, а операторам нижнего уровня, необходимо дополнительно запрашивать сведения о числе потребителей услуг второго уровня у данных операторов.

Так как в критерии не указана рассматриваемая длительность нарушения функционирования, то оценке подлежит в том числе кратковременный сбой в работе (кратковременный сбой связи).

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи». В данном документе приведен для полноты

5) Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)

Должна оцениваться возможность нарушения работоспособности или блокирование доступа к системам, реализующим функции предоставления государственных услуг (в соответствии с 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»). Данный критерий касается непосредственно ИС, реализующих предоставление государственных услуг, смежных систем и реестров, используемых данными ИС, а также систем и инфраструктурных сервисов, используемых для сбора и передачи данных/запросов.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных систем: нарушение работоспособности компонентов, удаление, изменение или блокирование данных, сбои или нарушение работоспособности оборудования, атаки типа «отказ в обслуживании», блокирующие доступ к ресурсам и т.д.

Масштаб возможного ущерба оценивается на основании:

- целевого показателя допустимого времени недоступности государственной услуги - максимально допустимого времени предоставления государственной услуги в разделе «Сроки предоставления государственной услуги» частных регламентов предоставления государственных услуг, актуальных для рассматриваемого объекта КИИ;
- требований к системам, непосредственно участвующим в оказании государственных услуг, устанавливаемым в ТЗ и связанных с ним SLA.

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

6) Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)

Должна оцениваться возможность нарушения функционирования государственных органов из-за нарушения функционирования или ограничения доступности рассматриваемого объекта КИИ.

Данный критерий касается в т.ч. ГИС, реализующих полномочия органов государственной власти, а также смежных систем и реестров, используемых ГИС, систем и сетей связи, используемых данными ГИС. Критерий считается актуальным для объектов КИИ, которые непосредственно обеспечивают функционирование органов государственной власти и не могут быть заменены (хотя бы временно) на альтернативные средства, т.к. в подобных случаях нельзя считать, что орган государственной власти не способен выполнять возложенные на него функции (он все еще способен, но с дополнительными затратами или задержками по времени, если они укладываются в допустимые нормы).

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных систем: нарушение работоспособности компонентов, удаление, изменение или блокирование данных, сбои или нарушение работоспособности оборудования, атаки типа «отказ в обслуживании», блокирующие доступ к ресурсам и т.д.

Масштаб возможного ущерба оценивается на основании сведений о целях и назначении рассматриваемого объекта КИИ и типа органа государственной власти, реализация функций которого зависит от данного объекта КИИ:

- орган государственной власти субъекта Российской Федерации или города федерального значения;
- федеральный орган государственной власти[16];
- Администрация Президента РФ, Правительство РФ, Федеральное Собрание РФ, Совет Безопасности РФ, Верховный Суд РФ, Конституционный Суд РФ.

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

[16] федеральные органы исполнительной власти и федеральные суды, кроме ВС РФ и КС РФ

исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака не считается возможной). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

7) Нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ

Должна оцениваться возможность нарушения соответствующих договоров, а также деятельности по подготовке или проведению переговоров, или подписанию международного договора РФ, из-за нарушения функционирования рассматриваемого объекта КИИ.

Данный критерий касается ИС, от работоспособности которых зависит реализация соответствующих договорных обязательств или выполнение предварительных условий, требуемых для заключения соответствующих международных договоров.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных систем, а также нарушение конфиденциальности или целостности данных, 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 или мер защиты (за исключением вариантов, когда данные системы являются неотъемлемой технологической частью системы, на которую атака не считается возможной). Пример:

системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

8) Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, 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)

Критерий актуален для субъектов, являющихся государственными корпорациями, государственными унитарными предприятиями, государственными компаниями, стратегическими акционерными обществами или стратегическими предприятиями

Должна рассматриваться возможность снижения уровня дохода соответствующего субъекта 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 ($t_н$) с учетом возможных нарушителей и

угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления (данные BIA, DRP, SLA, результаты тестирований планов восстановления и т.д.).

2. Оценивается какие процессы будут нарушены из-за нарушения работоспособности объекта КИИ и связанные с ними усредненные дневные потери дохода субъекта (L_{day}):

$$Lday = \frac{\text{суммарный доход, связанный с рассматриваемым процессом за 5-летний период}}{5 * 365}$$

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 ($L_{day}i$).

$$L_{day} = \sum L_{day}i$$

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

$$L = t_н * L_{day}$$

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

Пример:

Сценарий вирусного заражения шифровальщиком.

Следует допускать, что вся важная информация будет утеряна и необходимо оценить какой ущерб будет от этого (насколько будут остановлены, сколько потребуется для перезапуска и возможен ли он?). Если существует процесс резервного копирования, то нужно делать оценку времени простоя до предполагаемого восстановления данных и устранения последствий инцидента. Как пример: реагирование на вирусную атаку - 1 час, изоляция/пресечение эпидемии, принятие решения об использовании резервных площадок или иных сценариев - 5 часов, восстановление данных и ввод системы в строй - 3 часа. Соответственно, нужно определить потери от прерывания процесса на 9 часов.

Сценарий атаки на технологическую систему

Хакеры взламывают АСУ ТП, изменяют данные техпроцесса и выводят агрегат за пределы допустимых значений. Теоретически последствия могут включать: аварийный останов с необходимостью перезапуска агрегата, необходимость профилактического осмотра, ремонта, замены частей агрегата, необходимость замены агрегата – итоговый оцениваемый сценарий должен быть обоснован существующими системами противоаварийной защиты, проведение компьютерных атак на которые невозможно в принципе (механические, электрические в полностью изолированном контуре). То есть, стоит делать расчет потенциальных потерь от выведения агрегата из строя на время, требуемое для его ремонта/замены (если теоретически возможны такие последствия).

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

Должна оцениваться возможность снижения соответствующих выплат 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:

1. Нарушение производства / предоставления услуг субъекта;
2. 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 ($t_н$) с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления (данные BIA, DRP, SLA, результаты тестирований планов восстановления и т.д.).

2. Уточняются среднегодовые выплаты 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 РФ (L_{day}):

$$L_{dayi} = \frac{\text{среднегодовые выплаты в бюджет, связанные с i-м процессом}}{365}$$

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

$$L = t_н * \sum L_{dayi}$$

5. Итоговый ущерб оценивается в процентном соотношении к прогнозируемому годовому доходу федерального бюджета, усредненному за планируемый 3-летний период (для 2019-2021 гг. - 20 388,65 млрд. руб.):

$$L_{\%} = \frac{L}{20\,388\,650\,000\,000} * 100\%$$

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).

Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

Пример:

Для фабрики рассматривается АСУ ТП, автоматизирующее одну из производственных линий.

1. Необходимо сделать оценку влияния данной линии на итоговый объем производимой продукции (если линия уникальна для предприятия, то берется 100%, если нет, то соответствующая доля в объеме).

2. Делается оценка годовых выплат в соответствующий бюджет со всего рассматриваемого производства (учитывается непосредственно выплаты от производства и реализации, смежные выплаты с фонда оплаты труда и т.д. в расчет не берутся).

3. Делается оценка возможного срока нарушения функционирования соответствующей АСУ ТП (например, выведение из строя исполнительных аппаратов или блокирование баз данных в ходе атак) и максимальное возможное время восстановления функционирования (например, месяц на поставку необходимых компонентов и ввод в строй линии производства или 2 дня на восстановление данных из резервных копий и ввод линии в рабочий режим).

4. С учетом указанных сведений делается оценка возможных потерь:

$$L_{\%} = \frac{\text{Выплаты в бюджет от производства}}{365 * 20\,388\,650\,000\,000} * \begin{matrix}\text{коэффициент}\\ \text{влияния объекта на}\\ \text{объем производства}\end{matrix} * \begin{matrix}\text{длительность}\\ \text{нарушения в}\\ \text{днях}\end{matrix} * 100\%$$

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, 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)

Должна оцениваться возможность прекращения или нарушения проведения соответствующих операций из-за нарушения функционирования рассматриваемого объекта.

Данный критерий касается непосредственно банковских ИС, реализующих соответствующие операции, а также инфраструктурных объектов, обеспечивающих работу данных ИС.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы указанных объектов, влекущие:

- нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета;
- нарушение операций, осуществляемых субъектом КИИ, являющимся в соответствии с законодательством РФ системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка.

Данный критерий не привязан к длительности нарушений и оценивается исходя из показателей самого объекта КИИ. Оценка включает в себя расчет среднедневного (по отношению к числу календарных дней в году) количества осуществляемых объектом КИИ операций (млн. единиц). Расчет осуществляется на основании сведений за предыдущий календарный год, а для создаваемых объектов - на основе прогнозных значений. Соответствующие данные получаются из статистики транзакций объекта или из проектной документации на создаваемый объект. Для объектов КИИ, которые обеспечивают работоспособность иных объектов, реализующих транзакции (например, ЛВС банка или ЦОД, в котором размещено несколько АБС), должен проводиться анализ суммарных транзакций, проводимых системами, работоспособность которых обеспечивается. Итоговая оценка ущерба получается посредством деления годовой сумму транзакций на 365 (число дней в году).

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

11) 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.

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 РАС и ПАЗ не рассматриваются как фактор, снижающий риск. Физические блокировки и ограничители можно принимать в расчет.

При оценке и в качестве обоснования рекомендуется использовать данные:

- паспортов безопасности опасного производственного объекта;
- паспортов безопасности объектов ТЭК;
- декларации промышленной безопасности объекта;

- плана действий по предупреждению и ликвидации чрезвычайных ситуаций природного и техногенного характера;
- результатов категорирования объектов, оказывающих негативное воздействие на окружающую среду.

Масштаб возможного ущерба оценивается относительно:

- территории, на которой окружающая среда может подвергнуться вредным воздействиям;
- количества людей, которые могут быть подвержены вредным воздействиям (тыс. человек).

Пример:

Рассматривается система управления установкой сжигания мусоросжигающего завода, расположенного рядом с Москвой:

1. Определяются вероятные последствия нарушения функционирования системы управления: остановка процесса, повышение выбросов вредных веществ в атмосферу из-за нарушения параметров работы (изменение температуры, изменение параметров химической фильтрации).

2. Оценивается потенциальная площадь, подверженная вредным выбросам - территория муниципального образования / внутригородской территории города федерального значения.

3. Оценивается потенциальное количество людей, подверженных поражающему фактору - возможно более 5 млн.

12) Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра

Должна оцениваться возможность нарушения функционирования указанных пунктов управления и ситуационных центров, вызванная нарушением функционирования объекта.

Данный критерий касается объектов (систем, сетей связи), непосредственно обеспечивающих функционирование данных пунктов реагирования и центров.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы объектов, влекущие нарушение функционирования пунктов управления и ситуационных центров.

Данный критерий не привязан к длительности нарушений и оценивается исходя из характеристик (значимости) пункта управления или ситуационного цента, работа которого нарушается:

- пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения;
- пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации;
- пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ, Федерального Собрания РФ, Совета Безопасности РФ, Верховного Суда РФ, Конституционного Суда РФ.

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

13) Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое:

Должна оцениваться возможность нарушения выполнения оборонного заказа, вызванная нарушением функционирования объекта КИИ.

Данный критерий касается субъектов КИИ, являющихся головными исполнителями или исполнителями по государственному оборонному заказу и их объектов КИИ, задействованных в разработке, производстве, поставке продукции по государственному оборонному заказу. Для организаций, выпускающих продукцию двойного назначения и поставляющих ее исполнителю государственного оборонного заказа, данный показатель предлагается считать недействительным, так как на них не распространяются обязательства и ответственность за выполнение

государственного оборонного заказа и они не имеют возможности оценки итогового объема конечной продукции по нему.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы объектов КИИ, влекущие нарушение процессов реализации государственного оборонного заказа. При оценке должны рассматриваться такие последствия как:

1. Нарушение производства;
2. Изменение скорости выпуска продукции.

Масштаб ущерба, оцениваемый в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции) должен оцениваться для прогнозируемого нарушения, которое может повлечь снижение объема соответствующей продукции.

1. Параметр "заданный период времени" в явном виде не установлен, поэтому предлагается использовать его как срок реализации государственного оборонного заказа. Выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта КИИ ($t_н$) с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления (данные BIA, DRP, SLA, результаты тестирований планов восстановления и т.д.).

2. Для рассматриваемого объекта КИИ рассматриваются имеющиеся контракты (в соответствии с идентификаторами) и указанные в них сроки выпуска продукции (предоставления услуг) (Т) и объем выпускаемой продукции (предоставления услуг).

В случае, если рассматриваемый объект КИИ не является непосредственно производственным объектом, то необходимо рассмотреть объекты, 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 производственных объектов, реализующих продукцию или услуги по государственному оборонному заказу, расчет потерь должен выполняться для каждого подобного объекта и суммироваться.

3. Оценка снижения объема продукции (работ, услуг) осуществляется в процентах от заданного объема продукции: для равномерного распределения выпуска продукции

$$L = \frac{\text{Производительность объекта} * t_н}{\text{Запланированный объем ГО}} * 100\%$$

Масштаб ущерба, оцениваемый в увеличении времени выпуска продукции (работ, услуг) должен оцениваться для прогнозируемого нарушения, которое может повлечь увеличение времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции).

1. Выполняется оценка максимальной оценочной длительности разового нарушения работоспособности объекта КИИ (tн) с учетом возможных нарушителей и угроз безопасности, а также существующих мер резервирования и возможностей по обеспечению непрерывности и восстановления (данные BIA, DRP, SLA, результаты тестирований планов восстановления и т.д.).

2. Для объекта КИИ рассматриваются имеющиеся контракты (в соответствии с идентификаторами) и указанные в них сроки выпуска продукции (предоставления услуг) (Т) и объем выпускаемой продукции (предоставления услуг).

В случае, если рассматриваемый объект КИИ не является непосредственно производственным объектом, то необходимо рассмотреть объекты, 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 производственных объектов, реализующих продукцию или услуги по государственному оборонному заказу, расчет потерь должен выполняться для каждого подобного объекта (или браться минимальное время выпуска заказа).

3. Оценивается процентная задержка выпуска продукции (работ, услуг):

$$L = \frac{t_н}{T} * 100\%$$

Как видно из расчетов, процентные показатели в общем случае будут идентичны. Различия в оценках могут появиться в случае влияния объекта КИИ на несколько различных производственных объектов, реализующих государственный оборонный заказ, а также в случае неравномерного выпуска продукции во времени.

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)

Должна оцениваться возможность нарушения функционирования ИС в области обеспечения обороны страны, безопасности государства и правопорядка[17], связанная с нарушением функционирования объекта КИИ.

Данный критерий касается объектов (систем, сетей связи), непосредственно обеспечивающих функционирование систем обеспечения обороны страны, безопасности государства и правопорядка.

Должны рассматриваться инциденты, из-за которых возможно прекращение или нарушение работы объектов КИИ, влекущие нарушение функционирования систем обеспечения обороны страны, безопасности государства и правопорядка.

Масштаб возможного ущерба оценивается на основании целевого показателя допустимого времени недоступности рассматриваемой системы обеспечения обороны страны, безопасности государства и правопорядка.

Оценка ущерба осуществляется для разового нарушения с наибольшим прогнозируемым воздействием на объект (нарушение доступности соответствующей системы).

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). Пример: системы горячего резервирования оборудования, реализованные в общей информационной сети, не рассматриваются как фактор, снижающий риск, так как на них также возможно проведение компьютерной атаки, при этом, резервные каналы связи, которые могут быть дополнительно введены в эксплуатацию, можно принимать в расчет.

[17] Не распространяется на системы технических средств для обеспечения оперативно-розыскных мероприятий

Приложение 3

ПРОТОКОЛ

Заседания комиссии по категорированию объектов критической информационной инфраструктуры

от _____ 2019 г. №

На основании приказа от «__» _____20__г. №_____, комиссия в составе

Председатель комиссии: *Директор, Джон Голт*

Ф.И.О,. должность

Члены комиссии: *Заместитель директора по безопасности, Дагни Таггарт*

Ф.И.О,. должность

Главный инженер, Хэнк Риарден

Ф.И.О,. должность

Начальник ГО и ЧС, Джеймс Таггарт

Ф.И.О,. должность

Комиссия рассмотрела существующие в ООО «Металлургический завод им. Джона Голта» критические процессы - управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка:

1)
2)
3)
4)

Комиссия рассмотрела информационные системы, автоматизированные системы управления технологическими процессами и информационно-телекоммуникационные системы, принадлежащие ООО «Металлургический завод им. Джона Голта» на правах собственности или иных законных основаниях:

1) ;
2) ;
3) .

Комиссия определила, что рассмотренные информационные системы, автоматизированные системы управления технологическими процессами и информационно-телекоммуникационные системы, принадлежащие ООО «Металлургический завод им. Джона Голта» на правах собственности или иных законных основаниях, не осуществляют обработку информацию, необходимую для указанных критических процессов организации, управление критическими процессами, контроль или мониторинг критических процессов.

Для обработки информации, необходимой для критических процессов организации, управления критическими процессами, контроля или мониторинга критических процессов в ООО «Металлургический завод им. Джона Голта» используются информационные системы, принадлежащие сторонним организациям, категорирование которых ООО «Металлургический завод им. Джона Голта», в соответствии с п.2 Постановления Правительства РФ 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», осуществлять не в праве из-за отсутствия необходимой информации о системах:

1) ;
2) ;
3) .

На основании рассмотренной информации, а также положений Постановления Правительства РФ 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»,

Решено:

В ООО «Металлургический завод им. Джона Голта» отсутствуют объекты критической информационной инфраструктуры, подлежащие категорированию.

Подписи членов комиссии:

Заместитель директора по безопасности, Дагни Таггарт

Главный инженер, Хэнк Риарден

Начальник ГО и ЧС, Джеймс Таггарт

Приложение 4

УТВЕРЖДАЮ

Директор ООО «Металлургический завод им. Джона Голта»
Должность руководителя субъекта КИИ или уполномоченного им лица

_____ ____*Джон Голт*____
Подпись Ф.И.О.

«_____» _____ 20____ г.
Дата утверждения

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

N п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект[2]	Планируемый срок категорирования объекта	Должность, Ф.И.О., контактные данные представителя[3]
1.					
2.					
…					
n.					

[1] Указывется один из следующих типов объекта: ИС (информационная система), АСУ (автоматизированная система управления), ИТС (информационно-телекоммуникационная сеть).
[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 187-ФЗ: здравоохранение, наука, транспорт, связь, энергетика, банковская сфера и финансовый рынок, топливно-энергетический комплекс, атомная энергия, оборонная, ракетно-космическая, горнодобывающая, металлургическая или химическая промышленность.
[3] Указываются должность, Ф.И.О. должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Приложение 5

УТВЕРЖДАЮ

Директор ООО «Металлургический завод им. Джона Голта»

Должность руководителя субъекта КИИ или уполномоченного им лица

_____ ____*Джон Голт*____
Подпись Ф.И.О.

«_____» _____ 20____ г.
Дата утверждения

АКТ
Категорирования объектов критической информационной инфраструктуры

На основании приказа от «__» _____20__г. №_____, комиссия в составе

Председатель комиссии: *Директор, Джон Голт*

Ф.И.О,. должность

Члены комиссии: *Заместитель директора по безопасности, Дагни Таггарт*

Ф.И.О,. должность

Главный инженер, Хэнк Риарден

Ф.И.О,. должность

Начальник ГО и ЧС, Джеймс Таггарт

Ф.И.О,. должность

В соответствии с требованиями Федерального закона от 26.07.2017 г. №187-ФЗ «О безопасности объектов критической информационной инфраструктуры», а также «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127, провела категорирование объектов критической информационной инфраструктуры *ООО «Металлургический завод им. Джона Голт»*.

На основании анализа значений показателей критериев значимости объектов критической информационной инфраструктуры, объектам были присвоены категории значимости, отраженные в Приложении 1.

Подписи членов комиссии:

Заместитель директора по безопасности, Дагни Таггарт

Главный инженер, Хэнк Риарден

Начальник ГО и ЧС, Джеймс Таггарт

Приложение № 1

к акту категорирования объектов КИИ

Результаты категорирования объектов КИИ

№	Наименование объекта КИИ	Присвоенная категория	Сведения об объекте КИИ
1	*Автоматизируемая система управления металлургическим цехом*	I	Приложение 2
2	*Лаборатория сплавов*	III	Приложение 3
3	*Система учета патентов и разработок*	Без категории	Приложение 4

Приложение № 2

к акту категорирования объектов КИИ

Автоматизируемая система управления XXX

№	Параметр	Информация (в шаблоне пояснения по заполнению)
Сведения об объекте критической информационной инфраструктуры		
1	Наименование объекта	Указывается наименование ИС / АСУ ТП / ИТС. Может использоваться произвольное наименование, основные критерии: - оно должно быть уникальным в рамках Организации и однозначно идентифицировать систему; - данное название должно использоваться во всех документах, касающихся данной системы
2	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	В случае, если объект КИИ является распределённым, указываются адреса подразделений (обособленных подразделений, филиалов, представительств) субъекта КИИ, в которых размещаются сегменты объекта КИИ (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства). Достаточная точность указания — уровень здания. В случае, если объект КИИ — ИТС, указывается место расположения сетевого оборудования (активного и пассивного)
3	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Указывается в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности КИИ Российской Федерации»: сфера здравоохранения, науки, транспорта, связи, энергетики, банковская сфера или сфера финансового рынка, топливно-энергетический комплекс, область атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности В случае, если объект функционирует в нескольких сферах — указываются все соответствующие сферы
4	Назначение объекта	Указывается задача / цель функционирования объекта, например: управление работой гидроагрегата, ведение единого учета граждан, записывающихся на прием к врачу в медицинских учреждениях г. Москвы, управление и контроль работы нефтеперерабатывающей установки; единый центр управления технологическими процессами обогатительного завода и т. д.

№	Параметр	Информация (в шаблоне пояснения по заполнению)
5	Тип объекта	Указываются к какому типу относится объект п.1 - информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.
6	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Выбирается тип архитектуры из указанных вариантов или приводится уточнение их вариаций: одноранговая сеть, клиент-серверная система, «тонкий клиент», сеть передачи данных, SCADA-система, распределенная система управления или иная архитектура
7	Программно-аппаратные средства (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	Указываются наименования программно-аппаратных средств и их количество: - пользовательские компьютеры, - серверы, - телекоммуникационное оборудование, - средства беспроводного доступа, - технологическое, производственное оборудование (исполнительные устройства) - иные программно-аппаратные средства
8	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Указываются наименования клиентских, серверных операционных систем, средств виртуализации (при наличии)
9	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Указываются наименования прикладных программ: наименование ERP, SCADA и иных прикладных продуктов, обеспечивающих выполнение функций объекта по его назначению
10	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	Указывается категория сети электросвязи: сеть связи общего пользования, выделенная сеть связи, технологическая сеть связи, присоединенная к сети связи общего пользования, сеть связи специального назначения или другая сеть связи для передачи информации при помощи электромагнитных систем. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. ЛВС (КСПД) Организации также должна указываться, если она не входит в состав объекта КИИ и с ней осуществляется какое-либо взаимодействие

№	Параметр	Информация (в шаблоне пояснения по заполнению)
11	Наименование оператора связи	Указывается наименование каждого юридического лица (оператора электросвязи). В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия
12	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Указывается цель взаимодействия с сетью электросвязи из приведенных вариантов или свой вариант. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия
13	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Указывается соответствующая информация о взаимодействии с сетями электросвязи. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия

Приложение 6

УТВЕРЖДАЮ

Директор ООО «Металлургический завод им. Джона Голта»
Должность руководителя субъекта КИИ или уполномоченного им лица

_____ ____*Джон Голт*____
Подпись Ф.И.О.

«_____» _____ 20____ г.
Дата утверждения

Ограничительная пометка
или гриф секретности
(при необходимости)

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

Наименование объекта критической информационной инфраструктуры

1. Сведения об объекте критической информационной инфраструктуры

1.1	Наименование объекта	Указывается наименование ИС / АСУ ТП / ИТС. Может использоваться произвольное наименование, основные критерии: – оно должно быть уникальным в рамках Организации и однозначно идентифицировать систему; – данное название должно использоваться во всех документах, касающихся данной системы
1.2	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	В случае, если объект КИИ является распределённым, указываются адреса подразделений (обособленных подразделений, филиалов, представительств) субъекта КИИ, в которых размещаются сегменты объекта КИИ (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства). Достаточная точность указания — уровень здания. Допускается указывать размещение ключевого оборудования (серверного сегмента, оборудования ядра сети) в случаях сильно распределенной системы и большого числа клиентских компонентов. В случае, если объект КИИ — ИТС, указывается место расположения сетевого оборудования (активного и пассивного)
1.3	Сфера (область) деятельности, в которой функционирует объект	Указывается в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187–ФЗ «О безопасности КИИ Российской Федерации»: сфера здравоохранения, науки, транспорта, связи, энергетики, банковская сфера или сфера финансового рынка, топливно-энергетический комплекс, область атомной энергии, оборонной, ракетно-космической, горнодобывающей,

		металлургической и химической промышленности. В случае, если объект функционирует в нескольких сферах, указываются все соответствующие сферы
1.4	Назначение объекта	Указывается задача / цель функционирования объекта, например: управление работой гидроагрегата, ведение единого учета граждан, записывающихся на прием к врачу в медицинских учреждениях г. Москвы, управление и контроль работы нефтеперерабатывающей установки; единый центр управления технологическими процессами обогатительного завода и т. д.
1.5	Тип объекта	Указываются к какому типу относится объект п.1.1 - информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.
1.6	Архитектура объекта	Выбирается тип архитектуры из указанных вариантов или приводится уточнение их вариаций: одноранговая сеть, клиент– серверная система, «тонкий клиент», сеть передачи данных, SCADA– система, распределенная система управления или иная архитектура

2. Сведения о субъекте критической информационной инфраструктуры

2.1	Наименование субъекта	Наименование субъекта КИИ — см. раздел Методики - используемые определения.
2.2	Адрес местонахождения субъекта	Юридический адрес Адрес фактического местонахождения субъекта (если отличается)
2.3	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Должность, Ф.И.О. руководителя
2.4	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов. В случае отсутствия такого должностного лица — наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта
2.5	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов	Указываются соответствующие данные, при наличии структурного подразделения, ответственного за обеспечение безопасности значимых объектов: – Наименование подразделения; – Должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии). Или, в случае отсутствия выделенного подразделения – должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение

		безопасности значимых объектов, телефон, адрес электронной почты (при наличии)
2.6	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	Указываются соответствующие ИНН субъекта и КПП его обособленных подразделений (с указанием подразделений)

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

3.1	Категория сети электросвязи или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Указывается категория сети электросвязи (в соответствии с 126-ФЗ): сеть связи общего пользования, выделенная сеть связи, технологическая сеть связи, присоединенная к сети связи общего пользования, сеть связи специального назначения или другая сеть связи для передачи информации при помощи электромагнитных систем. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. ЛВС (КСПД) Организации также должна указываться, если она не входит в состав объекта КИИ и с ней осуществляется какое-либо взаимодействие.
3.2	Наименование оператора связи и (или) провайдера хостинга	Указывается наименование соответственного юридического лица (нескольких лиц, если сетей электросвязи несколько). В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия.
3.3	Цель взаимодействия с сетью электросвязи	Указывается цель взаимодействия с сетью электросвязи: передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия.
3.4	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Указывается соответствующая информация о взаимодействии с сетями электросвязи: тип доступа к сети электросвязи (проводной, беспроводной), используемых протоколов взаимодействия. В случае, если объект КИИ не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия.

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1	Наименование лица, эксплуатирующего объект	Наименование субъекта КИИ — лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта) В случае, если эксплуатацию осуществляет субъект КИИ — указываются его данные
4.2	Адрес местонахождения лица, эксплуатирующего объект	Юридический адрес лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта). Адрес фактического местонахождения субъекта (если отличается) лица, которое эксплуатирует объект КИИ (в случае, если отличается от владельца объекта). В случае, если эксплуатацию осуществляет субъект КИИ — указываются его данные
4.3	Элемент (компонент) объекта, который эксплуатируется лицом	Указываются соответствующие компоненты / сегменты/ зоны ответственности в случае, если эксплуатацией объекта занимается лицо, отличающееся от субъекта КИИ. В случае, если эксплуатацию осуществляет субъект КИИ — указывается «объект целиком эксплуатируется субъектом»
4.4	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	Указываются соответствующие ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений

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

5.1	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	Указываются наименования программно-аппаратных средств и их количество: – АРМ пользователей — x шт., – АРМ администраторов — x шт., – серверы — x шт., – телекоммуникационное оборудование — x шт., – средства беспроводного доступа — x шт., – технологическое, производственное оборудование (исполнительные устройства) — x шт., – иные программно-аппаратные средства — x шт.
5.2	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Указываются наименования клиентских, серверных операционных систем, средств виртуализации (при наличии)
5.3	Наименования	Указываются наименования прикладных программ:

	прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	наименование ERP, SCADA и иных прикладных продуктов, обеспечивающих выполнение функций объекта по его назначению
5.4	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	Указываются сведения о соответствующих средствах защиты информации, используемых для обеспечения ИБ рассматриваемого объекта КИИ (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки). Для упрощения последующих работ лучше сразу уточнять какую из мер приведенной в Приложении к «Требованиям по обеспечению безопасности значимых объектов КИИ РФ», утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239 реализуют указываемые средства защиты, например: – АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат соответствия ФСТЭК № 3025; – СОВ.1, СОВ.2 — Check Point Security Gateway версии R77.10, сертификат соответствия ФСТЭК № 3634; – ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД HP C8R15A. Для средств защиты информации, встроенных в общесистемное, прикладное программное обеспечение, указываются функции безопасности этого программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, иные функции). В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации

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

6.1	Категория нарушителя, краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности,	Указываются сведения о потенциальных нарушителях, например: Внешний нарушитель, обладающий средним потенциалом и высокой мотивацией, высокой квалификацией в области обнаружения и эксплуатации уязвимостей ИС. Данный тип нарушителя обладает следующими возможностями:

	знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	– возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами КЗ; – возможность сбора дополнительной информации о структурно-функциональных характеристиках и мерах защиты информации, применяемых в ИС; – возможность получить информацию об уязвимостях компонентов ИС, а также методах и средствах реализации угроз: • опубликованную в общедоступных источниках; • путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО. Данный тип нарушителя может использовать следующие каналы реализации угроз: – информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет); – беспроводные каналы передачи данных; – каналы связи, выходящие за пределы контролируемой зоны; – отчуждаемые носители информации и мобильные устройства, выносимые за пределы контролируемой зоны; – направленные воздействий на работников Организации (социальная инженерия). Внутренний нарушитель, обладающий низким потенциалом, низкой мотивацией и квалификацией продвинутого пользователя с ограниченными знаниями в области обнаружения и эксплуатации уязвимостей ИС. Данный тип нарушителя обладает следующими возможностями: – самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами КЗ; – сбора дополнительной информации о структурно-функциональных характеристиках и мерах защиты информации, применяемых в ИС; – получать информацию о пользователях и характеристиках ИС; – осуществлять попытки физического или логического доступа к ИС в рамках реализованных мер защиты – получать информацию об уязвимостях компонентов ИС, а также методах и средствах реализации угроз: • опубликованную в общедоступных источниках; • путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного ПО и отдельных программных компонентов общесистемного ПО. Данный тип нарушителя может использовать следующие каналы реализации угроз: – информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет);

		– беспроводные каналы передачи данных; – каналы связи, по которым осуществляется передача информации ограниченного доступа; – каналы связи, по которым осуществляется передача информации ограниченного доступа; – отчуждаемые носители информации и мобильные устройства; – направленные воздействий на работников Организации (социальная инженерия)
6.2	Основные угрозы безопасности информации или обоснование их неактуальности	Указываются основные угрозы безопасности информации. Могут использоваться соответствующие данные из 6 раздела Отчета об обследовании (Анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ). В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности (возможно в случае отсутствия потенциальных нарушителей и каналов реализации угроз)

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак	Указываются типы инцидентов из предложенных или дополняются/уточняются собственными: отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта. В случае отсутствия актуальных угроз безопасности информации указывается невозможность наступления компьютерных инцидентов

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1	Категория значимости объекта	Указываются присвоенная категория значимости или «Отсутствует необходимость присвоения категории значимости»
8.2	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Указывается возможный ущерб **по каждому показателю значимости**. Для показателей, которые неприменимы для объекта приводится соответствующая информация 1. Причинение ущерба жизни и здоровью людей – ***человек*** 2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения - ***территория*** б) по количеству людей, условия жизнедеятельности которых могут быть нарушены **- *тыс. человек***

		3. Прекращение или нарушение функционирования объектов транспортной инфраструктуры а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг ***- территория*** б) по количеству людей, для которых могут быть недоступны транспортные услуги - ***тыс. человек*** 4. Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, 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*** 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) – ***государственный орган*** 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 – ***тип договора*** 8. Возникновение ущерба субъекту КИИ, который является государственной корпорацией, ГУП, государственной компанией, 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 - ***% от годового объема доходов, усредненного за прошедший 5-летний период*** 9. Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры - ***% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период*** 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 - ***количество осуществляемых операций (млн. единиц)*** 11. Вредные воздействия на окружающую среду а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям - ***территория*** б) по количеству людей, которые могут быть подвержены вредным воздействиям - ***тыс. человек*** ***12.*** Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра – ***тип пункта управления (ситуационного центра)*** 13. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры а) в снижении объемов продукции (работ, услуг) в заданный период времени - ***% заданного объема продукции*** б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом - ***% установленного времени выпуска продукции*** 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***
8.3	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	Указывается обоснование **по каждому показателю значимости**: Например[1]: 1. Причинение ущерба жизни и здоровью людей Согласно паспорту безопасности опасного объекта, а также на основании анализа возможных негативных последствий развития инцидентов, связанных с компьютерными атаками, возможен сценарии чрезвычайной ситуации (вывод системы за пределы допустимых параметров работы с последующим возгоранием, а также механическим повреждениям и разрушений оборудования и производственных помещений), который может

[1] Информация приведена в качестве примера. В обосновании каждой оценки необходимо предоставлять полную и достоверную информацию, на основании которой можно будет проверить/подтвердить сделанный вывод и присвоении категории. То есть уточнить как делался расчет, какие компенсационные меры учитывали и почему и т.д.

		возникнуть на объекте, может привести к причинению ущерба жизни и здоровью порядка 40 человек, работающих в цеху или Объект КИИ не связан с процессами, нарушение или прекращение функционирования которых может повлечь причинение ущерба для жизни и здоровья людей 2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения б) по количеству людей, условия жизнедеятельности которых могут быть нарушены Нарушение функционирования объекта не оказывает влияние на нарушение объектов обеспечения жизнедеятельности населения, так как объект КИИ не участвует (не осуществляет управление или мониторинг указанных процессов и не оказывает на них влияние) в каких-либо процессах обеспечения жизнедеятельности населения (в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений) 3. Прекращение или нарушение функционирования объектов транспортной инфраструктуры а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг - территория б) по количеству людей, для которых могут быть недоступны транспортные услуги - тыс. человек Нарушение функционирования объекта не оказывает влияние на нарушение объектов транспортной инфраструктуры, так как объект КИИ не участвует (не осуществляет управление или мониторинг указанных процессов и не оказывает на них влияние) в каких-либо процессах автоматизации объектов транспортной инфраструктуры 4. Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи Объект КИИ не обеспечивает функционирование сетей связи 5. Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги Объект КИИ не обеспечивает доступ к государственной услуге (оператор связи не имеет государственного задания (заказа) или муниципального задания (заказа) на оказание государственной услуги)

		6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) Объект КИИ не обеспечивает функционирование государственных органов 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 Объект КИИ не обеспечивает соблюдение условий международного договора Российской Федерации (оператор связи не нарушает условия международных договоров Российской Федерации) 8. Возникновение ущерба субъекту КИИ, который является государственной корпорацией, ГУП, государственной компанией, 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 Субъект КИИ не является государственной корпорацией, ГУП, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием 9. Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры - % прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период Нарушение функционирования объекта может привести к снижению доходов федерального бюджета на 50 млн. рублей (расчетная сумма выплат налогов, пошлин и иных отчислений в бюджет, которая будет не выплачена из-за остановки производства на прогнозируемый срок в 3 дня) 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 Объект КИИ не обеспечивает проведение банковских операций (оператор связи не является системно значимой

		кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка) 11. Вредные воздействия на окружающую среду а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям Согласно паспорту безопасности опасного объекта, наиболее опасный сценарии чрезвычайной ситуации, который может возникнуть на объекте, может повлечь вредные выбросы в атмосферу в масштабах территории одного муниципального образования б) по количеству людей, которые могут быть подвержены вредным воздействиям Наиболее опасный сценарий чрезвычайной ситуации, который может возникнуть на объекте, приводящий к вредным выбросам в атмосферу, которым будут подвержены 2,5 млн. человек, проживающих в зоне потенциального воздействия Объект КИИ не управляет объектами, способными оказывать негативное воздействие на окружающую среду 12. Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра – тип пункта управления (ситуационного центра) Нарушение функционирования объекта не может привести к прекращению или нарушению (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), так как объект не участвует в управлении или мониторинге процессов пунктов управления (ситуационных центров) 13. Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры а) в снижении объемов продукции (работ, услуг) в заданный период времени б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом Нарушение функционирования объекта не может привести к снижению показателей государственного оборонного заказа, так как объект не задействован в процессах реализации, управления или контроля данных процессов 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 Нарушение функционирования объекта не может привести к прекращению или нарушению функционирования (невыполнению установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, так как объект не задействован в процессах реализации, управления или контроля данных процессов

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

9.1	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Указывается существующий перечень организационных мер защиты, например: – Разработаны документы, регламентирующие обеспечение безопасности объектов КИИ (указать наименования и реквизиты); – Организация и обеспечение безопасности контролируемой зоны; – Учет и контроль съемных носителей – Проведение инструктажей и обучения пользователей по вопросам ИБ – и т.д.
9.2	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Указывается существующий перечень технических мер защиты в соответствии с мерами из Требований по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239: – АВ3.1, АВ3.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат соответствия ФСТЭК № 3025; – СОВ.1, СОВ.2 — Check Point Security Gateway версии R77.10, соответствия ФСТЭК № 3634; – ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД HP C8R15A.