Согласовано Минэнерго России (исх. от 31.07.2019 № ЧА-8630/15)	Согласовано ФСТЭК России (исх. от 26.08.2019 № 240/25/4048)

Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса

Москва, 2019

АННОТАЦИЯ

Настоящие методические рекомендации в соответствии с положениями Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ) предназначены для субъектов топливно-энергетического комплекса (далее – ТЭК) в сферах электроэнергетики, нефтедобывающей, нефтеперерабатывающей, нефтехимической, газовой, угольной, сланцевой и торфяной промышленности, а также нефтепродуктообеспечения, теплоснабжения и газоснабжения в части категорирования объектов критической информационной инфраструктуры (далее – КИИ).

Настоящие методические рекомендации не распространяются на Министерство энергетики Российской Федерации и иные государственные органы Российской Федерации.

Методические рекомендации направлены на детализацию и стандартизацию процедуры категорирования объектов критической информационной инфраструктуры ТЭК. Предполагается, что в субъектах ТЭК изучены нормативные документы, регламентирующие процедуру категорирования, в связи с чем содержание указанных документов подробно не рассматривается.

Категорирование объекта ТЭК в соответствии с Федеральным законом от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» не является основанием для не проведения процедуры категорирования в соответствии с Федеральным законом № 187-ФЗ.

Методические рекомендации предназначены для членов комиссий по категорированию, создаваемых субъектами ТЭК, и их работников, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры.

Методические рекомендации разработаны на основании материалов, представленных субъектами ТЭК, и не содержит информацию ограниченного доступа.

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются термины и соответствующие им определения, введенные действующими нормативными правовыми актами Российской Федерации, а также государственными стандартами и методическими документами.

Автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

Безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

Значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

Комиссия по категорированию – постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры;

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;

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

Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

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.

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

АСУ ТП	Автоматизированная система управления технологическими процессами
ГО и ЧС	Гражданская оборона и чрезвычайные ситуации
ЕГРЮЛ	Единый государственный реестр юридических лиц
ИНН	Идентификационный номер налогоплательщика
ИА	Исполнительный аппарат
ИС	Информационная система
ИТ	Информационные технологии
ИТКС	Информационно-телекоммуникационная сеть
КЗ	Контролируемая зона
КИИ	Критическая информационная инфраструктура
КПП	Код причины постановки на учет
ТЭК	Топливно-энергетический комплекс
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие методические рекомендации детализируют и стандартизируют процедуру категорирования объектов КИИ, принадлежащих на праве собственности, аренды или на ином законном основании государственным учреждениям, российским юридическим лицам и/или индивидуальным предпринимателям и используемых ими для осуществления видов деятельности в сфере топливно-энергетического комплекса.

Общий порядок осуществления категорирования определен Правилами категорирования объектов КИИ Российской Федерации (далее – Правила) и Перечнем показателей критериев значимости объектов КИИ Российской Федерации и их значений (далее – Перечень), утвержденными постановлением Правительства Российской Федерации от 08 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 – постановление № 127) в редакции Постановления Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».

Методические рекомендации применяются субъектами ТЭК для:

- определения процессов в рамках видов деятельности, осуществляемых субъектами ТЭК;
- выявления управленческих, технологических, производственных, финансово-экономических и/или иных процессов в рамках осуществления видов деятельности субъекта ТЭК, нарушение и/или прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее – критические процессы) из числа типовых процессов субъекта ТЭК;
- определения информационных систем (далее – ИС), информационно-телекоммуникационных сетей (далее – ИТКС) и автоматизированных систем управления технологическими процессами (далее – АСУ ТП), которые обрабатывают информацию, необходимую для обеспечения критических процессов, и/или осуществляют управление, контроль или мониторинг критических процессов (далее совместно именуемых объекты КИИ), из числа типовых ИС, ИТКС и АСУ ТП, принадлежащих субъектам ТЭК;

- формирования перечня объектов КИИ, подлежащих категорированию (далее – перечень объектов КИИ);
- оценки для каждого объекта КИИ в соответствии с перечнем объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов;
- присвоения каждому из объектов КИИ одной из категорий значимости либо принятия решения об отсутствии необходимости присвоения ему одной из категорий значимости;
- подготовки сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ.

Общая схема работ по категорированию объектов ТЭК в соответствии со ст. 7 Федерального закона № 187-ФЗ представлена на рис. 1.

Рисунок 1. Общая схема категорирования

В соответствии с ч. 1 ст. 7 Федерального закона № 187-ФЗ «категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения».

Процедуры категорирования объектов КИИ условно разделяются на первичную и последующие.

Первичная процедура категорирования объектов КИИ обуславливается вступлением в силу Федерального закона № 187-ФЗ и подзаконных нормативных актов. В ходе выполнения первичной процедуры категорирования объектов КИИ формируется перечень объектов КИИ субъекта КИИ, подлежащих категорированию, который впоследствии утверждается и направляется во ФСТЭК России.

Последующие процедуры категорирования производятся в случаях:

а) создания нового объекта КИИ или перехода на праве собственности, аренды или ином законном основании во владение и (или) эксплуатацию субъектом КИИ уже существующего объекта КИИ;

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

в) изменения объекта КИИ, не являющегося значимым объектом КИИ, в результате которого такой объект стал значимым, на основании которых ему должна быть присвоена определенная категория значимости;

г) проведения периодического пересмотра установленной категории значимости или отсутствия необходимости назначения одной из категорий значимости объекта КИИ, осуществляемого (не реже, чем один раз в 5 лет)

д) изменения показателей критериев значимости объектов КИИ или их значений.

2. ОТНЕСЕНИЕ ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ, РОССИЙСКОГО ЮРИДИЧЕСКОГО ЛИЦА И (ИЛИ) ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ К СУБЪЕКТАМ КИИ

Отнесение любого государственного учреждения, российского юридического лица и/или индивидуального предпринимателя к субъектам КИИ осуществляется исходя из его соответствия первым двум условиям (одновременно) или третьему условию:

1. Государственное учреждение, российское юридическое лицо и/или индивидуальный предприниматель осуществляет один или несколько из основных видов своей деятельности в одной или нескольких сферах (областях) деятельности, предусмотренных п. 8 ст. 2 Федерального закона № 187-ФЗ.
2. Государственному учреждению, российскому юридическому лицу и/или индивидуальному предпринимателю принадлежат на праве собственности, аренды или на ином законном основании любые ИС, ИТКС и АСУ ТП.
3. Российское юридическое лицо и/или индивидуальный предприниматель обеспечивает взаимодействие ИС, ИТКС и АСУ ТП, принадлежащих государственному учреждению, российскому юридическому лицу и/или индивидуальному предпринимателю, осуществляющему свою деятельность в одной или нескольких сферах (областях) деятельности, предусмотренных п. 8 ст. 2 Федерального закона № 187-ФЗ.

Если одно из первых двух условий и третье условие не выполняются, то государственное учреждение, российское юридическое лицо и/или индивидуальный предприниматель не является субъектом КИИ, если условия выполняются (одновременно первые два условия или третье условие), то является субъектом КИИ.

Область применения методических рекомендаций в отношении субъектов ТЭК как субъектов КИИ уточняется следующим образом:

- сферой деятельности, предусмотренной п. 8 ст. 2 Федерального закона № 187-ФЗ является энергетика или топливно-энергетический комплекс;
- в качестве субъектов КИИ рассматриваются государственные учреждения, российские юридические лица и/или индивидуальные предприниматели, при этом не учитывается, является ли субъект ТЭК государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и/или стратегическим акционерным обществом, стратегическим предприятием.

3. КОМИССИЯ ПО КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КИИ

Для проведения мероприятий по категорированию в соответствии с п. 11 Правил решением руководителя субъекта КИИ создается ***постоянно действующая комиссия по категорированию***. Состав комиссии определен пунктами 11, 11.1, 11.2 и 12, руководитель комиссии определяется в соответствии с п. 13 Правил.

Форма приказа о создании комиссии приведена в приложении 1.

Рекомендуемый состав комиссии.

1. Председатель комиссии по категорированию объектов КИИ
2. Заместитель председателя комиссии
3. Член комиссии - ответственный за ГО и ЧС
4. Член комиссии - ответственный за предоставление экономических показателей
5. Член комиссии - ответственный за выполнение процесса / владелец процесса
6. Член комиссии - ответственный за ИС, ИТКС, АСУ ТП
7. Член комиссии - ответственный за обеспечение безопасности объектов КИИ
8. Член комиссии - аналитик (группа аналитиков)
9. Член комиссии - ответственный по направлению информационной безопасности
10. Член комиссии - ответственный по направлению информационных технологий
11. Другие члены комиссии, определенные п. 11 Правил.

В состав комиссии по категорированию могут включаться представители Министерства энергетики Российской Федерации по согласованию с данным министерством.

4. ОПРЕДЕЛЕНИЕ ПРОЦЕССОВ В РАМКАХ ВИДОВ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМЫХ СУБЪЕКТОМ КИИ

В настоящем документе под процессом понимается последовательность связанных действий или задач, необходимых для достижения определенного результата.

Все процессы субъекта КИИ, предлагается условно подразделить на следующие группы:

- основные (операционные) – процессы, непосредственно ориентированные на оказание услуги и/или производство товара и обеспечивающие получение дохода для субъекта КИИ. Так, например, для электроэнергетики, согласно Федерального закона от 26 марта 2003 г. № 35-ФЗ «Об электроэнергетике», эти процессы обеспечивают:
  - работу в сферах оптового и розничного рынков электрической энергии и мощности;
  - оказание услуг по передаче электрической энергии;
  - оперативно-технологическое управление;
  - коммерческий учет электрической энергии (мощности).
- управления – процессы, отвечающие за управление деятельностью субъекта КИИ;
- поддержки функционирования – процессы, предназначенные для обеспечения основных процессов субъекта КИИ необходимыми ресурсами и создающими инфраструктуру компании;
- развития – процессы совершенствования деятельности субъекта КИИ, нацеленные на получение прибыли в долгосрочной перспективе (совершенствование производства продукции / услуги, технологии производства или оказания услуг, внедрение нового оборудования, а также инновационные процессы).

В случае, если применение вышеописанного подхода к выявлению процессов субъекта ТЭК представляется затруднительным, возможно использование другого подхода, основанного на методологии Enhanced Telecom Operations Map® (eTOM). Модель eTOM определяет архитектуру бизнес-процессов операторов телекоммуникационных услуг, но может быть применена и в других областях, в том числе в топливно-энергетическом комплексе.

Описание процессов в соответствии с данной моделью представлено на рис. 2.

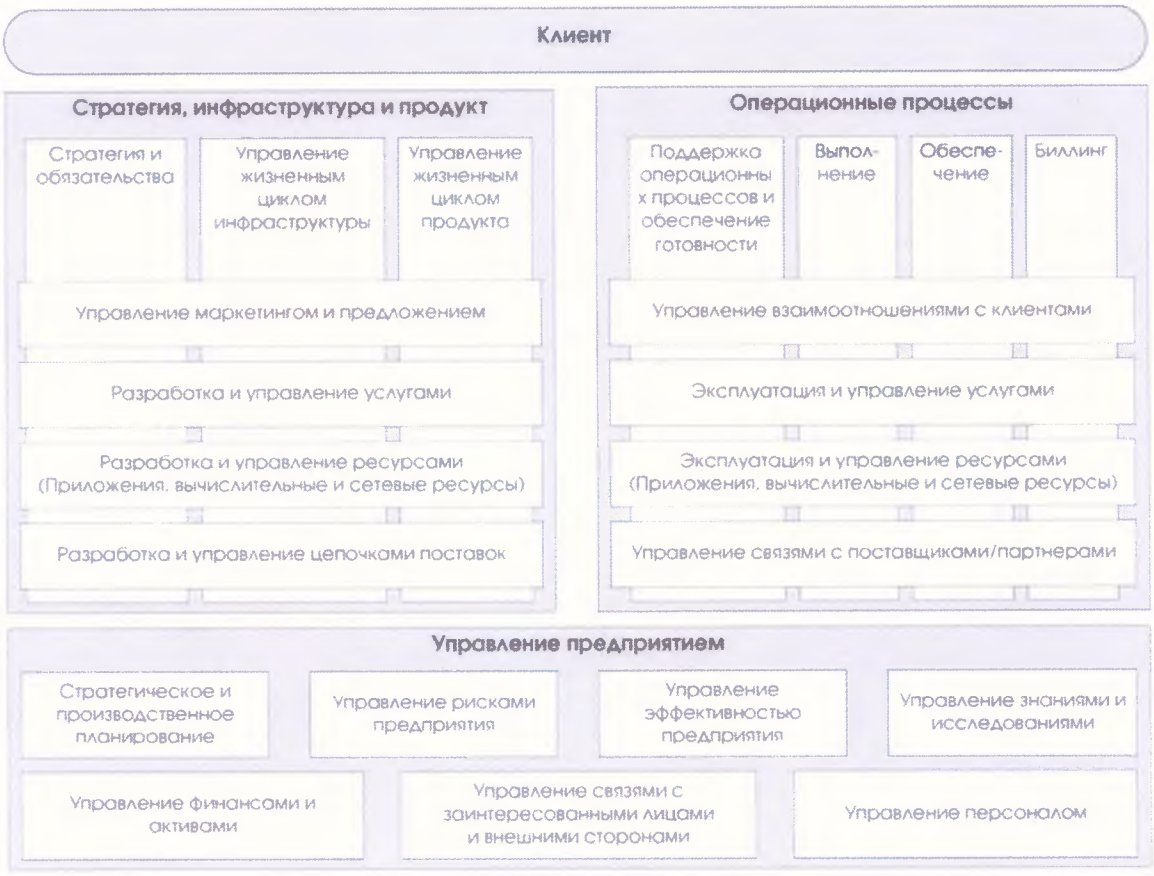

Рисунок 2. Описание процессов предприятия

Определение ***исходных данных для категорирования*** осуществляется на основании действий, предусмотренных п. 5 Правил:

а) определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ;

б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов 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 (далее - критические процессы);

в) определение объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

г) формирование перечня объектов КИИ, подлежащих категорированию (далее - перечень объектов).

В соответствии с п. 14.3 Правил необходимо оценивать критичность процессов с учетом масштаба последствий от нарушения или прекращения функционирования предприятия ТЭК.

Для субъектов ТЭК критичность функциональных процессов также определяется в соответствии с подпунктом «г» п. 10 Правил.

Для описания процессов рекомендуется использовать формулировки, описывающие сам процесс, а не дублировать названия обеспечивающих их ИС, ИТКС и АСУ ТП.

5. ВЫЯВЛЕНИЕ КРИТИЧЕСКИХ ПРОЦЕССОВ В РАМКАХ ВИДОВ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМЫХ СУБЪЕКТОМ КИИ

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.

Необходимо отметить, что к критическим процессам следует относить только те процессы, которые исполняются в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ в областях (сферах), установленных п. 8 ст. 2 Федерального закона № 187-ФЗ, отраженные в уставе субъекта и внесенные в ЕГРЮЛ. В первую очередь должны рассматриваться процессы связанные с основной функциональной деятельностью, обеспечивающие получение прибыли предприятия.

Рекомендуется использовать перечень критериев значимости объектов и их значения из приложения 1 к Постановлению № 127. Соответственно, нужно определить для каждого рассматриваемого процесса, способно ли его нарушение повлечь последствия, определенные в Перечне.

Таким образом, отсекая на данном этапе процессы, нарушение которых не может привести к последствиям, соответствующим показателям значимости, автоматически отсекаются и системы (ИС, ИТКС, АСУ ТП), автоматизирующие данные процессы, так как их нарушение также не должно иметь значимых последствий.

Значения показателей критериев значимости оцениваются комиссионно на основании результатов интервью или иным способом, полученных в ходе обследования. По каждому показателю оценивается возможность наступления указанных видов последствий (возможно/невозможно). По результатам обработки предоставленной информации формируется перечень показателей критериев значимости, применимых для субъекта ТЭК.

Таким образом, критический процесс – процесс, для которого хотя бы по одному из оцениваемых показателей критериев значимости было сделано заключение о возможности соответствующего ущерба.

6. ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ КИИ

Для каждого критического процесса формируется перечень ИС, ИТКС, АСУ ТП, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов.

Для каждого критичного процесса определяется перечень ИС, ИТКС, АСУ ТП, которые осуществляют одну из следующих функций:

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

При формировании перечня членам комиссии рекомендуется:

- сделать запрос ответственным за ИС, ИТКС, АСУ ТП, ответственному за обеспечение безопасности объектов КИИ, ответственному по направлению информационных технологий или ответственному по направлению информационной безопасности с просьбой составить перечень ИС, ИТКС, АСУ ТП субъекта ТЭК;
- сделать запрос ответственному за выполнение процесса с просьбой указать перечень ИС, ИТКС, АСУ ТП, реализующих рассматривающие процессы. К запросу приложить сформированный общий перечень ИС, ИТКС, АСУ ТП;
- проанализировать итоговый перечень ИС, ИТКС, АСУ ТП на законность их владения (принадлежность на праве собственности, аренды или ином законном основании) или использования на законном основании;
- в случае, если ИС, ИТКС, АСУ ТП не принадлежит субъекту ТЭК на праве собственности, аренды или ином законном основании, или если не используется на законном основании, исключить ИС, ИТКС, АСУ ТП из списка;
- если субъект КИИ является юридическим лицом, входящим в состав группы юридических лиц, согласовать итоговый перечень ИС, ИТКС, АСУ ТП с ответственными лицами по линии курирования. Целью согласования является исключение ситуаций, когда однотипные объекты КИИ в рамках одной группы юридических лиц могут иметь необоснованно разные категории значимости.

7. ФОРМИРОВАНИЕ ПЕРЕЧНЯ ОБЪЕКТОВ КИИ, ПОДЛЕЖАЩИХ КАТЕГОРИРОВАНИЮ

Формирование перечня объектов КИИ, подлежащих категорированию, осуществляется субъектом ТЭК исходя из реального состава ИС, ИТКС и АСУ ТП, принадлежащих субъекту ТЭК на праве собственности, аренды или на ином законном основании.

Оформление перечня объектов КИИ осуществляется в соответствии с рекомендуемой ФСТЭК России формой (приведена в Приложении 2, определена Информационным сообщением ФСТЭК России «по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» от 24 августа 2018 г. № 240/25/3752.)

Сформированный перечень объектов КИИ утверждается руководителем субъекта КИИ (президентом, генеральным директором или т.п.) или уполномоченным им лицом.

Отправка сформированного и утвержденного перечня объектов КИИ осуществляется в течение *десяти* рабочих дней с даты его утверждения в адрес федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ (экспедиция центрального аппарата ФСТЭК России): 105066, г. Москва, ул. Старая Басманная, д. 17, на бумажном носителе и на электронном носителе информации в формате файлов электронных таблиц, установленном приказом ФСТЭК России от 21 марта 2019 г. № 59.

Для подведомственных Минэнерго России организаций, перечисленных на официальном сайте minenergo.gov.ru, указанный перечень в соответствии с п. 15 Правил должен быть согласован с Министерством. Для иных предприятий, работающих в сфере ТЭК, согласование перечня не является обязательным.

Дополнительные рекомендации по заполнению формы перечня объектов КИИ субъекта ТЭК, подлежащих категорированию:

1. Если у субъекта ТЭК несколько однотипных объектов КИИ, то указывается каждый объект КИИ в отдельной строке с соответствующим наименованием (строки в перечне объектов КИИ добавляются).

3. Если у субъекта ТЭК несколько однотипных объектов КИИ с одинаковым наименованием, то указывается каждый объект КИИ в отдельной строке с соответствующим наименованием и порядковым/инвентарным номером (строки в перечне объектов КИИ добавляются).

8. ОЦЕНКА МАСШТАБА ВОЗМОЖНЫХ ПОСЛЕДСТВИЙ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ НА ОБЪЕКТАХ КИИ

В соответствии с п. 14 Правил комиссия по категорированию проводит оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объекте КИИ и присвоение каждому из объектов КИИ одной из категорий значимости либо принимает решение об отсутствии необходимости присвоения им одной из категорий значимости.

Полученные в ходе оценки данные, а также присвоенная категория значимости вносится в акт категорирования.

Для удобства использования рекомендации по заполнению формы направления сведений, составленной с учетом вышеупомянутых приказов, приводится в Приложении 3.

Раздел **«Сведения об объекте критической информационной инфраструктуры»** акта категорирования объекта КИИ**.**

П. 1.1 заполняется на основании балансовой ведомости субъекта КИИ.

П. 1.2 заполняется на основании имеющихся сведений об адресах размещения объекта.

В п. 1.3 для предприятий ТЭК указывается «топливно-энергетический комплекс».

В п. 1.4 указывается назначение объекта.

В п. 1.5 указывается тип объекта. С учетом специфики предприятий ТЭК особое внимание должно уделяться АСУ ТП.

В п. 1.6 указывается архитектура объекта.

Раздел **«Сведения о субъекте критической информационной инфраструктуры»** акта категорирования объекта КИИ.

Пп. 2.1, 2.2., 2.3 и 2.6 заполняются на основании сведений, представленных из уставных документов и выписки из ЕГРЮЛ.

П. 2.4 и 2.5 заполняется на основании сведений из приказов о назначении соответствующих должностных лиц.

Раздел **«Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи»** акта категорирования объекта КИИ.

В п. 3.1 указывается категория сети связи, используемая объектом КИИ.

П. 3.2 заполняется на основании сведений из договоров на оказание услуг связи, обеспечивающих объект КИИ.

В п. 3.3 указывается цель взаимодействия с сетью связи.

В п. 3.4 указывается способ взаимодействия с сетью связи.

Раздел **«Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры»** акта категорирования объекта КИИ.

В п. 4.1 указывается наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект КИИ.

В п. 4.2 указывается адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект КИИ.

В п. 4.3. указывается элемент (компонент) объекта, который эксплуатируется указанным юридическим лицом или индивидуальным предпринимателем.

В п. 4.4. указывается ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта.

Раздел **«Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры»** акта категорирования объекта КИИ.

Пп. 5.1 – 5.4 заполняются на основании сведений из балансовой ведомости субъекта КИИ. При описании средств защиты в соответствии с п. 5.4. акта

2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений – определяется с учетом п. 3 Паспорта безопасности объекта ТЭК.

3. Прекращение или нарушение функционирования объектов транспортной инфраструктуры – определяется в соответствии с п. 1 Паспорта безопасности ТЭК.

4. Прекращение или нарушение функционирования сети связи – не применяется.

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

II. Политическая значимость

6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). Под прекращением или нарушением функционирования государственного органа в части невыполнения возложенной на него функции (полномочия) с учетом положений федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ в настоящих методических рекомендациях рассматривается ситуация невозможности для государственного органа реализации возложенных на него функций (полномочий), закрепленных в соответствующих нормативно-правовых актах Российской Федерации, в результате недоступности услуги электроснабжения, теплоснабжения или снабжения топливом, приобретенной им в рамках государственного контракта для выполнения возложенной на него функции (полномочия), с учетом условий данного контракта. Данный вид негативных последствий может возникнуть только в случае наличия у субъекта ТЭК соответствующего действующего государственного контракта с органом государственной власти.

Данный вид негативных последствий оценивается по уровню органа государственной власти, с которым заключен соответствующий государственный контракт:

- орган государственной власти субъекта Российской Федерации или города федерального значения;
- федеральный орган государственной власти;
- Администрация Президента Российской Федерации, Правительство Российской Федерации, Федеральное Собрание Российской Федерации, Совет

категорирования необходимо исходить из того, что для значимых объектов КИИ рекомендуется использовать сертифицированные средства защиты.

Раздел **«Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры»** акта категорирования объекта КИИ.

В п. 6.1 приводится описание нарушителя.

В п. 6.2 указываются угрозы безопасности объекту КИИ.

Для определения актуальных угроз для систем АСУ ТП рекомендуется использовать базу данных угроз ФСТЭК России (bdu.fstec.ru), а также руководствоваться Информационным сообщением ФСТЭК России от 04 мая 2018 г. № 240/22/2339 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ».

В случае, если на объекте КИИ имеется разработанная «Модель угроз и нарушителя безопасности информации», в которой рассматриваются все имеющиеся на данный момент угрозы безопасности информации, определенные в банке данных угроз безопасности информации ФСТЭК, следует руководствоваться выводами, сделанными в «Модели угроз и нарушителя безопасности информации» для данного объекта КИИ.

Раздел **«Возможные последствия в случае возникновения компьютерных инцидентов»** акта категорирования объекта КИИ.

В п. 7.1 указываются типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак.

Раздел **«Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости»** заполняется следующим образом.

П. 8.1 заполняется на основании решения комиссии.

Раздел 8.2 акта категорирования КИИ заполняется следующим образом.

I. Социальная значимость

1. Причинение ущерба жизни и здоровью людей (человек) – определяется с учетом п. 3 Паспорта безопасности объекта ТЭК.

Безопасности Российской Федерации, Верховный Суд Российской Федерации, Конституционный Суд Российской Федерации.

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 - в соответствии с заключенными договорами с международными обязательствами.

III. Экономическая значимость

8. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в:

- возникновении непредвиденных издержек, снижающих прибыль;
- нарушении порядка платежей и расчетов с контрагентами, что чревато нарушением ритмичности материально-технического обеспечения и сбыта продукции, штрафами, судебными исками и т.д.
- нарушении своевременности уплаты акцизов, налогов и обязательных взносов во внебюджетные фонды
- нарушении установленных кредитными и инвестиционными договорами с финансовыми институтами ковенант, влияющих на условия привлекаемого финансирования, вплоть до сокращения и отзыва ранее установленных кредитных и инвестиционных лимитов
- разглашении конфиденциальной информации, влияющей на коммерческую деятельность и интересы акционеров
- разглашении закрытой информации, которая в условиях санкционной политики ряда стран по отношении к России может быть использована против российских корпораций, органов власти и управления, финансовых институтов и т.д.

– в соответствии с п. 3 Паспорта безопасности объекта ТЭК.

9. Возникновение ущерба бюджетам Российской Федерации – в соответствии с расчетом недополученных налогов.

10. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно

значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений) - не применяется

IV. Экологическая значимость

11. Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия).

V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка

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

прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации – не применяется.

13. Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры – рассчитывается в случае выполнения государственного оборонного заказа.

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

максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов) – не применяется.

В п. 8.3 приводится обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту.

Раздел **«Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры»** акта категорирования объекта КИИ.

П. 9.1 заполняется на основании сведений из Паспорта безопасности объекта ТЭК, разработанного в соответствии с Приложением к Федеральному закону от 21 июля 2011 г. № 256-ФЗ (ред. от 06 июля 2016 г.) «О безопасности объектов топливно-энергетического комплекса».

В п. 9.2 указываются технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов.

9. ПРИНЯТИЕ РЕШЕНИЯ ОБ УСТАНОВЛЕНИИ КАТЕГОРИИ ЗНАЧИМОСТИ ОБЪЕКТУ КИИ

В соответствии с требованиями Федерального закона 187-ФЗ объекту КИИ присваивается категория значимости.

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, а категория значимости присваивается по наивысшему значению такого показателя.

В случае если ни один из показателей критериев значимости неприменим для объекта КИИ, или объект КИИ не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.

Устанавливаются 3 категории значимости. Самая высокая категория – первая, самая низкая – третья.

В отношении объекта КИИ, создаваемого в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту КИИ с учетом имеющихся исходных данных о критических процессах субъекта ТЭК. Для создаваемого объекта КИИ, категория значимости может быть уточнена в ходе его проектирования.

Для объектов, принадлежащих другому субъекту критической информационной инфраструктуры, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащим субъекту ТЭК, категорирование осуществляется на основе исходных данных, представляемых субъектом КИИ, которому принадлежит технологическое и (или) производственное оборудование.

Решение комиссии по каждому объекту КИИ оформляется отдельным актом.

Форма акта приведена в приложении 4. Акт подписывается членами постоянной комиссии по категорированию. Все акты могут быть утверждены одним приказом руководителя субъекта ТЭК (субъекта КИИ), в этом случае акты будут выступать приложениями к соответствующему приказу, или каждый акт может быть утвержден по отдельности. Субъект КИИ в лице ответственного по направлению информационной безопасности обеспечивает хранение Акта до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости.

Категория значимости может быть изменена в порядке, предусмотренном для категорирования, в случаях, предусмотренных п. 12 статьи 7 Федерального закона № 187-ФЗ.

10. РАССМОТРЕНИЕ РЕЗУЛЬТАТОВ КАТЕГОРИРОВАНИЯ

Рассмотрение результатов категорирования производится в соответствии со схемой, представленной на рис. 3.

Рисунок 3. Схема рассмотрения результатов категорирования

ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

3. Постановление Правительства Российской Федерации от 08 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».

4. Постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».

5. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 459 «Об утверждении Положения об исходных данных для проведения категорирования объекта топливно-энергетического комплекса, порядке его проведения и критериях категорирования».

6. Постановление Правительства Российской Федерации от 21 мая 2007 г. № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера».

7. Приказ Министерства энергетики РФ от 10 февраля 2012 г. № 48 «Об утверждении методических рекомендаций по включению объектов топливно-энергетического комплекса в перечень объектов, подлежащих категорированию».

8. Приказ 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».

ПРИЛОЖЕНИЕ 1

Рекомендуемая форма приказа о создании комиссии по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам ТЭК

№ ____ от __.__.____

ПРИКАЗ
о создании комиссии по категорированию

С целью организации и проведения работ по категорированию объектов критической информационной инфраструктуры

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры, принадлежащих *название субъекта ТЭК* на праве собственности, аренды или ином законном основании.
2. Председателем комиссии назначить *должность, ФИО*, заместителем председателя комиссии назначить *должность, ФИО*.
3. В состав комиссии включить:
   - *должность, ФИО*;
   - – ...
   - *должность, ФИО*.
4. Комиссии в срок до *ДД.ММ.ГГГГ*:
   - определить процессы в рамках осуществления видов деятельности *название субъекта ТЭК*;
   - выявить критические процессы у *название субъекта ТЭК*;
   - выявить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
   - подготовить предложения для включения объектов критической информационной инфраструктуры в перечень объектов критической информационной инфраструктуры, подлежащих категорированию;
   - представить на утверждение перечень объектов критической информационной инфраструктуры, подлежащих категорированию, в срок до *ДД.ММ.ГГГГ*;
   - рассмотреть возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

- проанализировать угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;
- оценить в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;
- установить каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принять решение об отсутствии необходимости присвоения им категорий значимости;
- представить на утверждение акты по результатам категорирования;
- представить на утверждение сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

5. Комиссии в своей деятельности руководствоваться положениями действующих нормативно-правовых и методических документов:
   - Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ (ст. 7);
   - Правила категорирования объектов критической информационной инфраструктуры Российской Федерации и Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 127;
   - Методическими рекомендациями по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса.
6. Ознакомить с настоящим приказом председателя и членов создаваемой комиссии.
7. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель субъекта ТЭК *И.О. Фамилия*

ПРИЛОЖЕНИЕ 2

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

_____

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____

Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«____» _____ 20___ г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект[2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					
...					

---

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) 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 3

Рекомендации по заполнению формы направления сведений

1. Сведения об объекте критической информационной инфраструктуры

№	Поле для заполнения	Рекомендации по заполнению
1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	Заполняется в соответствии с наименованием, указанным в проектных и эксплуатационных документах
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	Необходимо указать адреса размещения всех компонентов объекта КИИ, в том числе адреса обособленных подразделений, филиалов, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Указывается одна или несколько из перечня сфер деятельности, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в которой функционирует объект КИИ
1.4.	Назначение объекта	Назначение объекта КИИ указывается в соответствии с рабочей, проектной, эксплуатационной или иной документацией на объект КИИ, а также в соответствии с локальными нормативно-правовыми актами о создании и (или) вводе объекта КИИ в эксплуатацию
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	Указывается тип объекта КИИ – ИС, ИТКС или АСУ ТП
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)	Тип архитектуры определяется в соответствии с рабочей, проектной или эксплуатационной документацией на объект КИИ, фактическим составом технических средств и их взаимосвязью. Для примера, архитектура объекта КИИ может

		быть следующих типов: одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления и др.

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	Указывается полное и краткое наименование субъекта КИИ в соответствии с уставными документами
2.2.	Адрес местонахождения субъекта	Указывается адрес местонахождения субъекта КИИ. Адрес местонахождения определяется в соответствии с уставными документами и ЕГРЮЛ субъекта КИИ
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Указывается полное наименование должности руководителя субъекта КИИ в соответствии с уставными документами и его фамилия, имя и отчество (при наличии)
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	Если функции обеспечения безопасности значимых объектов КИИ возложены на соответствующее должностное лицо из числа работников субъекта КИИ, указывается должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов КИИ. Если функции обеспечения безопасности значимых объектов КИИ в субъекта КИИ ни на кого из работников не возложены, то указывается полное наименование должности руководителя субъекта КИИ в соответствии с уставными документами и его фамилия, имя и отчество (при наличии).
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых	Если ответственность за обеспечение безопасности значимых объектов КИИ возложена на структурное подразделение организации, указывается полное наименование (в соответствии с утвержденной организационно-штатной структурой) структурного подразделения, а также полное наименование (в соответствии с утвержденной организационно-штатной структурой) должности руководителя этого структурного

	объектов, телефон, адрес электронной почты (при наличии)	подразделения, его фамилию, имя и отчество (при наличии), номер телефона и адрес электронной почты (при наличии). Если ответственность за обеспечение безопасности значимых объектов КИИ возложена на штатного специалиста, указывается полное наименование (в соответствии с утвержденной организационно-штатной структурой) должности этого штатного специалиста, его фамилию, имя и отчество (при наличии), а также его номер телефона и адрес электронной почты (при наличии)
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	Указывается ИНН субъекта КИИ и КПП филиалов, представительств, в которых размещаются компоненты объекта КИИ

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

3.1.	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	Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи – указывается категория сети электросвязи. В соответствии с Федеральным законом от 07 июля 2003 г. № 126-ФЗ «О связи» сети электросвязи могут делиться на следующие категории: - сеть связи общего пользования; - выделенная сеть связи; - технологическая сеть связи, а также технологическая сеть связи, присоединенная к сети связи общего пользования; - сеть связи специального назначения Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение
3.2.	Наименование оператора связи и (или) провайдера хостинга	Если рассматриваемый объект КИИ взаимодействует с сетями связи, для каждой из них необходимо указать наименование оператора связи (в соответствии с договором об оказании услуг связи), предоставляющего доступ к данной сети электросвязи.

		Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение. Примечание – Поскольку технологические сети связи – это сети связи предприятия, используемые для обеспечения производственной деятельности, управления технологическими процессами в производстве, для них в качестве оператора указывается наименование субъекта КИИ. В случае, если компоненты объекта КИИ размещаются на площадках провайдеров хостингов, указывается наименование провайдера хостинга. В случае, если для размещения компонентов объекта КИИ не используются сторонние хостинги, дается соответствующее пояснение
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи, необходимо указать цель такого взаимодействия. Цель взаимодействия указывается в соответствии с рабочей, проектной и (или) эксплуатационной документацией на данный объект КИИ. Для примера, могут быть указаны следующие цели взаимодействия: передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), или любая иная цель. Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи, необходимо указать способ взаимодействия (проводной и (или) беспроводной), используемые технологии доступа к сети электросвязи, а также протоколы, по которым осуществляется взаимодействие. Данный пункт заполняется на основании рабочей, проектной и/или эксплуатационной документации на

		данный объект КИИ, а также на основании договора об оказании услуг связи. Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	Если рассматриваемый объект КИИ эксплуатируется только субъектом КИИ, то указывается наименование полное и краткое наименование организации.
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	Если какие-либо компоненты рассматриваемого объекта КИИ эксплуатируются сторонним юридическим лицом, также указывается полное наименование (в соответствии с уставными документами, ЕГРЮЛ) этого юридического лица
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	Если рассматриваемый объект КИИ эксплуатируется только организацией, указывается адрес местонахождения организации.
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	Если какие-либо компоненты рассматриваемого объекта КИИ эксплуатируются сторонним юридическим лицом, также указывается адрес местонахождения (в соответствии с уставными документами, ЕГРЮЛ) этого юридического лица

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 всех программно-аппаратных средств в составе объекта КИИ (без разбиения на какие-либо группы и указания мест размещения), с указанием их количества.
5.2.	Наименование общесистемного программного обеспечения (клиентских,	Указываются наименования и версии клиентских, серверных операционных систем,

	серверных операционных систем, средств виртуализации (при наличии))	средств виртуализации (при наличии), входящих в состав рассматриваемого объекта КИИ общим перечнем (без разбиения на какие-либо группы и указания мест размещения)
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Указываются наименования и версии прикладных программ, обеспечивающих выполнение функций объекта КИИ по его назначению, за исключением прикладных программ, входящих в состав дистрибутивов операционных систем, общим перечнем (без разбиения на какие-либо группы и указания мест размещения)
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки) или сведения об отсутствии средств защиты информации.	Если на рассматриваемом объекте КИИ применяются средства защиты информации, указываются наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки. Если в качестве средств защиты информации используются встроенные в системное и/или прикладное программное обеспечение средства, указываются функции безопасности программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции). Если на объекте КИИ не используются средства защиты информации и их функции не реализованы встроенными средствами системного и (или) прикладного программного обеспечения, дается соответствующее пояснение

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

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности,	Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ (в случае наличия). Во всех случаях указывается тип нарушителя:

	знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	внешний или внутренний. В случае наличия объективных факторов, свидетельствующих о возможности исключения тех или иных положений из описания, по решению Комиссии по описание может быть скорректировано
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ (в случае наличия). Указываются группы угроз, актуальных для объекта КИИ исходя из его структурно-функциональных характеристик, используемых типов технических средств и технологий. В соответствии с критериями, установленными в указанном документе, выбираются группы угроз и конкретные угрозы безопасности с их идентификаторами Банка данных угроз безопасности информации ФСТЭК России, которые указываются при заполнении данного поля

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 (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ

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

8.1.	Категория значимости, которая присвоена объекту либо информация о не присвоении объекту ни одной из таких категорий	Указывается категория в соответствии с результатами категорирования, отраженными в утвержденном Акте соответствующего объекта КИИ
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Заполняется на основании сведений, полученных при выполнении оценки возможного масштаба последствий. Указывается по всем показателям критериев значимости, определенным в Правилах. По неприменимым показателям критериев значимости – указывается факт неприменимости
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	Заполняется на основании сведений, полученных при выполнении оценки возможного масштаба последствий. Указывается по всем показателям критериев значимости, определенным в Правилах. По неприменимым показателям критериев значимости – указывается текстовое обоснование неприменимости

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого 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)	Меры указываются вне зависимости от того, присвоена ли объекту КИИ категория значимости или нет.
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	Меры указываются вне зависимости от того, присвоена ли объекту КИИ категория значимости или нет. Технические меры рекомендуется группировать в соответствии с приказом ФСТЭК России № 239, описывая, что конкретно технически реализовано в рамках той или иной группы мер.

ПРИЛОЖЕНИЕ 4

Рекомендуемая форма акта по итогам категорирования объекта критической информационной инфраструктуры, принадлежащего субъекту ТЭК

Утвержден

приказом № X от ДД.ММ.ГГГГ

АКТ

категорирования объекта критической информационной инфраструктуры

Комиссией по категорированию объектов критической информационной инфраструктуры, принадлежащих *название субъекта КИИ* на праве собственности, аренды или ином законном основании и перечисленных в перечне объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию, утвержденном *ДД.ММ.ГГГГ, должность*,

ПРИНЯТО РЕШЕНИЕ [*выбрать один из двух вариантов*]:

• Присвоить объекту критической информационной инфраструктуры «*наименование объекта КИИ*» *X* категорию значимости.

• Отсутствует необходимость присвоения одной из категорий значимости объекту критической информационной инфраструктуры «*наименование объекта КИИ*».

Сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, приведены в приложении (Приложение 1).

Приложение № 1 к акту
категорирования объекта критической
информационной инфраструктуры

Сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры. [*оформляются в соответствии с приложением 3 настоящих методических рекомендаций*]