ПРАВИТЕЛЬСТВО МОСКВЫ
ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ

СОГЛАСОВАНО

Главный внештатный специалист
По информационным технологиям,
заместитель директора по развитию
информационных технологий
ГБУЗ «НИИ СП им. Н.В. Склифосовского
Департамента здравоохранения города
Москвы»
_____И.А. Тыров

Директор ГБУ «НИИОЗММ
Департамента здравоохранения города
Москвы»
д.э.н., профессор
_____Е.И. Аксенова

РЕКОМЕНДОВАНО

Экспертный совет по науке
Департамента здравоохранения города
Москвы № _____

«____»_____2020 г

.

По определению объектов КИИ и категорий значимости объектов КИИ в медицинских учреждениях Департамента здравоохранения города Москвы

Методические рекомендации № ____

Москва 2020

УДК _____
ББК _____

Организация-разработчик: Государственное бюджетное учреждение города Москвы «Научно-исследовательский институт организации здравоохранения и медицинского менеджмента Департамента здравоохранения города Москвы»

Составители:

Махров Игорь Николаевич – начальник отдела информационной безопасности ГБУ «НИИОЗММ ДЗМ».

Жуков Алексей Михайлович – начальник отдела научно-медицинских цифровых решений «НИИ НДХиТ»

Печикин Евгений Валерьевич – специалист по защите информации отдела информационной безопасности ГБУ «НИИОЗММ ДЗМ».

Предназначение. Методические рекомендации предназначены для руководителей и сотрудников отделов информационной безопасности, отделов информационных технологий учреждений здравоохранений Департамента здравоохранения города Москвы с целью установления единых требований к оформлению документов по определению объектов критической информационной инфраструктуры и категорированию значимости объектов КИИ.

ISBN _____

Содержание

Введение

Настоящий документ содержит методические рекомендации по отнесению информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании, подведомственных Департаменту Здравоохранения города Москвы учреждениям (далее – ИС) к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры (далее – Перечень, с последующим установлением одной из категорий значимости объектов критической информационной инфраструктуры, либо решений об отсутствии оснований для их отнесения к объектам критической информационной инфраструктуры, в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

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 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
ИБ	Информационная безопасность
ИС	Информационная система
ИСиР	Информационные системы и ресурсы
ИТС	Информационно-телекоммуникационная сеть
КИИ	Критическая информационная инфраструктура
КСПД	Корпоративная Сеть Передачи Данных
ЛВС	Локальная вычислительная сеть
ОКВЭД	Общероссийский классификатор видов экономической деятельности
ОКОГУ	Общероссийский классификатор органов государственной власти и управления
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. Перечень нормативных документов, на которые необходимо ориентироваться при работе с КИИ

1 Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ).

2 Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

3 Постановление Правительства РФ №127 от 08.02.2018 «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» (ПП 127).

4 Приказ ФСТЭК России №236 от 22.12.2017 «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».

5 Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

2. Общая информация

С 01 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187ФЗ «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 ПП-127).

В соответствии с требованиями 187-ФЗ, субъект КИИ обязан 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 187-ФЗ «к субъектам критической информационной инфраструктуры относятся государственные органы и учреждения, а также 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».

У каждого субъекта КИИ есть объекты КИИ:

- информационные системы;
- автоматизированные системы управления технологическими процессами;
- информационно-телекоммуникационные сети.

Если разделить работу с КИИ на крупные шаги, то можно получить следующий порядок:

Первый шаг. Необходимо создать внутреннюю комиссию по категорированию.

Второй шаг. На этом этапе собираются исходные данные, проводится обследование и на основании полученных данных, комиссия формирует перечень объектов КИИ, подлежащих категорированию и присваивает категорию значимости. Согласно ПП-127, выделяют три категорий значимости три, первая самая высокая.

Категории значимости присваиваются исходя из показателей критериев значимости[1], которых пять:

[1] Постановление 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”

- социальная;
- политическая;
- экономическая;
- экологическая;
- значимость для обеспечения обороны страны, безопасности государства и правопорядка.

После утверждения и согласования перечня объектов КИИ подлежащих категорированию с Департаментом здравоохранения г .Москвы, субъект КИИ в течении **десяти рабочих дней** обязан направить Перечень во ФСТЭК России. С момента утверждения Перечня, на проведение процедур категорирования отводится максимум один год. Если объект КИИ не подпадает под один из показателей критериев значимости, то у него отсутствует необходимость присвоения категории значимости, но тем не менее предприятие является субъектом КИИ, у которого отсутствуют критически значимые объекты КИИ.

Результатом второго шага является «Акт категорирования объекта КИИ», который подписывается членами комиссии и утверждается руководителем субъекта КИИ. Акт должен содержать полные сведения об объекте КИИ и хранится субъектом до последующего пересмотра критериев значимости.

3. Определение признаков оснований для отнесения ИС к объектам критической информационной инфраструктуры

В соответствии с определением в 187-ФЗ, субъект КИИ – это 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**;
- **науки**;
- транспорта;
- связи;
- энергетики;
- банковской сфере и иных сферах финансового рынка;
- топливно-энергетического комплекса;
- атомной энергии;
- оборонной промышленности;
- ракетно-космической промышленности;
- горнодобывающей промышленности;
- металлургической промышленности;
- химической промышленности.

4. Мероприятия этапа «Аудит и категорирование»

№ п/п	Наименование мероприятия	Состав работ
1	Создание комиссии по категорированию	Необходимо создать постоянно действующую комиссию по категорированию объектов.
2	Определение процессов	Необходимо определить управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".
3	Выявление критических процессов	Необходимо выявить процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.
4	Определение объектов КИИ	Необходимо определить объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов.
5	Формирование перечня объектов КИИ	Необходимо сформировать перечень объектов КИИ, подлежащих категорированию.
6	Сбор исходных данных об объекте КИИ	Необходимо собрать следующие сведения: а) сведения об объекте КИИ (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами КИИ, наличие и характеристики доступа к сетям связи); б) процессы, которые обеспечивают управленческие, технологические, производственные, финансово- экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ; в) состав информации, обрабатываемой объектами КИИ, сервисы по управлению, контролю или мониторингу, предоставляемые объектами КИИ; г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект КИИ (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации); д) сведения о взаимодействии объекта КИИ с другими объектами КИИ и (или) о зависимости функционирования объекта КИИ от других таких объектов.
7	Анализ угроз	Необходимо:

		выявить группы угроз безопасности информации в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах КИИ соответствующего типа; рассмотреть возможные действия нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации; проанализировать угрозы безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ.
8	Оценка значимости объектов КИИ	Необходимо провести оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ
9	Присвоение категории значимости объектов КИИ	Необходимо присвоить каждому из объектов КИИ одну из категорий значимости, либо обосновать принятие решения об отсутствии необходимости присвоения им одной из категорий значимости
10	Составление Актов категорирования объектов КИИ.	Необходимо оформление внутренних документов. После подготовки Акта категорирования КИИ, его подписывают все члены комиссии и утверждают у Главного врача. Допускается оформление одного акта на несколько объектов.
11	Подготовка сведений о категорировании объектов КИИ. Оформление документов.	Необходимо подготовить документ «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» в соответствии с требованиями Приказа ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». Форма по 236 приказу делается на каждый объект КИИ.

5. Категорирования объектов критической информационной инфраструктуры

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 и сценариев компьютерных атак;
- оценка масштаба последствий угроз и соотнесение со значениями показателей категорий;
- определение категории значимости объекта КИИ.

Комиссия по категорированию с помощью работников, ответственных за обеспечение информационной безопасности в медицинской 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 медицинской организации.

В качестве ориентира можно использовать сведения о потенциальных нарушителях, приведенные в Приложение 5. Данная классификация приведена в виде справочного материала и должна быть адаптироваться под нужды и характеристики организации, применительно к конкретному объекту КИИ. Классификация приведена с учетом «Банка данных угроз информационной безопасности» ФСТЭК России, сформированный итоговый набор может использоваться в дальнейшем для формирования модели нарушителей и модели угроз для значимых объектов КИИ. Для упрощения работы рекомендуется выбирать наборы потенциальных нарушителей для групп объектов, для которых они характерны.

Для рассматриваемого объекта КИИ проводится анализ возможных угроз и их последствий. 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 определить высокоуровневые угрозы и обобщенные сценарии компьютерных атак, которые могут привести к реализации данных угроз.

В качестве ориентира можно использовать классификацию основных типов угроз и компьютерных атак, приведенных в Приложение 6. Данная классификация приведена в виде справочного материала и должна адаптироваться под нужды и характеристики Организации, применительно к конкретному объекту.

Для рассматриваемого объекта КИИ необходимо определить возможные последствия нарушений, основываясь на выявленных возможных угрозах ИБ, сценариях компьютерных атак, назначение объекта КИИ и автоматизируемого процесса. Для рассматриваемого объекта КИИ должны выбираться те типы последствий, которые могут стать следствием вероятных угроз для данного объекта. В качестве возможных последствий предлагается рассматривать последствия, соответствующие показателям значимости из 127- ПП, 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 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 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 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 (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 критической информационной инфраструктуры;
14. прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка.

6. Создание комиссии по категорированию

Для проведения мероприятий по категорированию в соответствии с п. 11 127-ПП решением Главного врача создается комиссия по категорированию. Проект Приказа по созданию комиссии по категорированию объектов КИИ приведен в Приложение 8.

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

Таблица №1

Состав комиссии по категорированию

№	Участники, в соответствии с 127- ПП	Уточнение и примеры
1.	Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо	- Главный врач - Заместитель - Заместитель по безопасности или 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) Заместитель по научной работе 2) Руководители критичных направлений деятельности, процессы которых автоматизируются ИС / АСУ; 3) Руководители ИТ-подразделения; 4) Руководитель отдела автоматизации (АСУ ТП) — в случае наличия; 5) Ответственный за промышленную безопасность на предприятии — в случае наличия; 6) 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) объектов критической информационной инфраструктуры	Руководитель ИБ-подразделения (администратор ИБ в случае отсутствия выделенного подразделения).
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 ГО и ЧС или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций - в случае наличия

Следует отметить, что в состав комиссии по категорированию могут 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.

Комиссию по категорированию возглавляет руководитель субъекта КИИ или уполномоченное им лицо.

Комиссия по категорированию в ходе своей работы:

– определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ;

– выявляет наличие критических процессов у субъекта КИИ;

– выявляет объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;

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

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

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

– устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

7. Определение процессов

Необходимо определить 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.

Перечень процессов (пример):

1. Оказание медицинских услуг и медицинской помощи
   - Стационарная медицинская помощь
   - Амбулаторная медицинская консультативная и лечебная помощь
   - Восстановительное лечение
   - Диагностическая медицинская помощь
   - Высокотехнологическая медицинская помощь
2. Проведение исследований, клинических испытаний, осмотров
3. Фармацевтическая деятельность
4. Деятельность по обороту наркотических средств и психотропных веществ
5. Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия)
6. Сбор, хранение и реализация донорской крови
7. Организация общественного питания
8. Розничная торговля товарами личной гигиены и общего потребления
9. Услуги длительного пребывания пациентов / госпитализации (в т.ч. палаты повышенной комфортности)
10. Проведение конференций, семинаров и иных ученых мероприятий
11. Осуществление автотранспортных услуг
12. Управление персоналом
    - Подбор персонала
    - Кадровый учет
    - Расчёт и начисление заработной платы
    - Организация командировок
    - Обучение работников
13. Бухгалтерский учет
14. Контрольно-пропускной режим
15. Заключение договоров с контрагентами
16. Обслуживание ИТ-инфраструктуры
17. Обслуживание инженерных систем (Электроснабжение; Система отопления; Водопровод; Канализация; Вентиляция и кондиционирование; Системы пожаробезопасности)
18. Работа с обращениями клиентов
19. Претензионная и судебная работа

Данный перечень процессов может быть дополнен медицинской организацией

8. Выявление критических процессов

Необходимо выявить процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка:

Таблица №2

№ п/п	Наименование процесса	Негативные последствия				
		Соц.	Полит.	Эконом.	Эколог.	Оборон.
1.	Оказание медицинских услуг и медицинской помощи					
2.	Проведение исследований, клинических испытаний, осмотров					
3.	Фармацевтическая деятельность					
4.	Деятельность по обороту наркотических средств и психотропных веществ					
5.	Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия)					
6.	Сбор, хранение и реализация донорской крови					
7.	Организация общественного питания					
8.	Розничная торговля товарами личной гигиены и общего потребления					
9.	Услуги длительного пребывания пациентов / госпитализации / стационар (в т.ч. палаты повышенной комфортности)					
10.	Проведение конференций, семинаров и иных ученых мероприятий					
11.	Осуществление автотранспортных услуг (медицинская транспортировка)					
12.	Управление персоналом					
13.	Бухгалтерский учет					
14.	Контрольно-пропускной режим					
15.	Заключение договоров с контрагентами					
16.	Обслуживание ИТ-инфраструктуры					
17.	Обслуживание инженерных систем (пожарная сигнализация, электропитание)					
18.	Работа с обращениями клиентов					
19.	Претензионная и судебная работа					

9. Определение объектов КИИ

Определение объектов КИИ (информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления), которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов:

- Оказание медицинских услуг и медицинской помощи
- Проведение исследований, клинических испытаний, осмотров
- Фармацевтическая деятельность
- Деятельность по обороту наркотических средств и психотропных веществ
- Деятельности связанная с использованием источников ионизирующего излучения (рентген, томография, лучевая терапия)
- Сбор, хранение и реализация донорской крови
- Услуги длительного пребывания пациентов / госпитализации / стационар (в т.ч. палаты повышенной комфортности)
- Осуществление автотранспортных услуг (медицинская транспортировка)
- Бухгалтерский учет
- Заключение договоров с контрагентами
- Обслуживание инженерных систем (пожарная сигнализация, электропитание)

Перечень объектов, подлежащий категорированию (примеры):

Информационные системы:

- АС «Стационар»
- МИС «Инфоклинка»
- МИС «Медиалог»
- «М-Аптека»
- «Медкомтех»
- «Экспресс-здоровье»
- «Скрининг новорожденных»
- и т.д

Информационно-телекоммуникационные сети:

- защищенная сеть Департамента здравоохранения;
- защищенная сеть МГФОМС;
- защищенная сеть медицинской организации

Автоматизированные системы управления:

- Автоматизированная система оперативного управления диспетчерской службой скорой медицинской помощи
- АСУ рентген аппаратами
- АСУ томографом
- АСУ лучевой терапия

Должны быть указаны объекты информационной инфраструктуры находящиеся в МО на праве собственности или аренды.

Оборудование типа – Рентгеновский аппарат, МРТ, КТ и т.д. прошедшее регистрацию в Росздравнадзоре относится к медицинским изделиям и в перечне не указываются. В случаях, когда к данному аппарату (несколько аппаратов) подключены специализированные рабочие станции, на которых происходит хранение медицинских данных (или если имеются специализированное сервера, на которые передается медицинская информация с данных аппаратов), то данный сегмент рассматриваем как автоматизированную систему управления.

Форма перечня объектов КИИ в приложении 1 к настоящему документу.

Форма уведомления ФСТЭК России о перечне объектов КИИ в приложении 2 к настоящему документу.

Форма письма для отправки в Департамент здравоохранения г. Москвы о направлении перечня объектов КИИ в приложении 3 к настоящему документу.

Сначала необходимо Перечень направить на согласование в Департамент здравоохранения г. Москвы, после получения ответа из Департамента, утвердить комиссией по категорированию объектов критической информационной инфраструктуры (КИИ), а затем направить в адрес ФСТЭК РФ.

10. Сбор исходных данных об объекте КИИ

На этом этапе необходимо собрать (Приложение7):

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

б) процессы, инфраструктуры; указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной

в) состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);

д) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов.

Объект (пример):

– Медицинская информационная система

1. Сведения об объекте критической информационной инфраструктуры

№	Параметр	Информация (в шаблоне пояснения по заполнению)
Сведения об объекте критической информационной инфраструктуры		
1	Наименование объекта	Медицинская информационная система
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)	г. Москва, ул. _____
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»	Сфера здравоохранения

4	Назначение объекта	Автоматизация информационных процессов, сопровождающих лечебно-диагностическую, хозяйственную и управленческую деятельность
5	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Автоматизация информационных процессов, сопровождающих лечебно-диагностическую, хозяйственную и управленческую деятельность
6	Архитектура объекта (одноранговая сеть, клиентсерверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Клиент-серверная система
7	Программно-аппаратные средства (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	- Серверы: 1 шт. - Пользовательские компьютеры – 600 шт. - Ленточная библиотека
8	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Windows 7, Windows 10 Windows Server 2016 Veritas Backup Exec 12.5
9	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Microsoft SQL server 2016
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	Информационно-телекоммуникационная сеть . Закрытая внутренняя локально вычислительная сеть, без подключения к внешним линиям связи.
11	Наименование оператора связи	Комкор
12	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Передача данных от клиента к серверу
13	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	Проводной
Сведения об угрозах безопасности информации объекта критической информационной инфраструктуры		
14	Сведения о нарушителях безопасности информации объекта КИИ	Приложение 5
15	Основные угрозы безопасности информации объекта КИИ	Приложение 6

16	Возможные сценарии компьютерных 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 Направленные атаки на пользователей (методы социальной инженерии), Эксплуатация уязвимостей системного, прикладного или сетевого ПО.
Сведения об реализованных мерах по обеспечению безопасности объекта критической информационной инфраструктуры		
17	Реализованные организационные меры защиты	Анализ угроз безопасности. Парольная политика. Политики управления доступом. Проведение инструктажей по ИБ. Регламенты ИБ.
18	Применяемые средства защиты информации или сведения об отсутствии средств защиты информации.	- АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат соответствия СФ/СЗИ-0100, №3025, Kaspersky Security Centre 10 сертификат соответствия СФ/СЗИ-0098, СФ/019-3113, №3155, СФ/019-3468 - ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД
Сведения о присвоенной объекту критической информационной инфраструктуры категории значимости		
19	Категория значимости, которая присвоена объекту	Без категории
20	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	Причинение ущерба жизни и здоровью людей - 0; показатель не применим к объекту
Сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ (ФСТЭК России)		
21	Необходимые меры по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ	Объект КИИ не является значимым обязательных мер не установлено

11. Оценка значимости объектов КИИ

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

Объект (пример):

– Медицинская информационная система

Показатель		Значение показателя			
		III категория	II категория	I категория	Без категории
I. Социальная значимость					
1.	Причинение ущерба жизни и здоровью людей (человек)				+
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:				
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;				+
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)				
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:				
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;				
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)				
4.	Прекращение или нарушение функционирования сети связи, оцениваемые:				
	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;				
	б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)				+
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)				+
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 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 снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)				
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого:				
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);				
	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);				
	В) снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)				
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)				
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), оцениваемые:				
	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), оцениваемое в				

	уровне (значимости) пункта управления или ситуационного центра				
13.	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:				
	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);				
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)				
14.	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)				

Решение комиссии по категорированию оформляется актом (Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий), который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.

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

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

Субъект КИИ в течение **10 рабочих дней** со дня утверждения акта направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ, сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Форма сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий в приложении 9 к настоящему документу.

Форма уведомления ФСТЭК России о сведениях об объектах КИИ в приложении 4 к настоящему документу.

Приложение 1 – форма перечня объектов КИИ

УТВЕРЖДАЮ

Главный врач
Наименование МО

_____ФИО

___ _____2019 г.

Перечень объектов критической информационной инфраструктуры ГБУЗ «_____» , подлежащих категорированию

№ 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	МИС «_____»	ИС	Здравоохранение	_____2019	
2	ПАКС «_____»	ИС	Здравоохранение	_____2019	
3	ЛИС «_____»	ИС	Здравоохранение	_____2019	

[1]Указывается 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 2 – форма письма для отправки о ФСТЭК

Начальнику 2 Управления
ФСТЭК России
Шевцову Д.Н.

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

О направлении перечня объектов критической информационной инфраструктуры[1]

Уважаемый Дмитрий Николаевич!

В соответствии с требованиями пункта 15 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127 направляем Вам перечень объектов критической информационной инфраструктуры нашей организации.

№ п/п	Наименование объекта	Тип объекта	Сфера (область) деятельности в которой функционирует объект	Планируемый срок категорирования объекта	Должность, Ф.И.О., контактные данные представителя
1	МИС «_____»	ИС	Здравоохранение	_____2019	Руководитель – Петров П.П. (495)9000009 mail@gkb.ru г. Москва _____
2	ПАКС «_____»	ИС	Здравоохранение	_____2019	
3	ЛИС «_____»	ИС	Здравоохранение	_____2019	

Согласование проводилось в Департаменте здравоохранения г. Москвы №____ от «__» _____ 2019 г. в Приложении к настоящему письму.

Руководитель МО _____ ФИО

[1] Предоставление информации об отсутствии в организации объектов критической информационной инфраструктуры или о том, что организация не является субъектом критической информационной инфраструктуры Российской Федерации в ФСТЭК России в соответствии с законодательством о безопасности критической информационной инфраструктуры Российской Федерации не требуется. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Приложение 3 – форма письма для отправки в ДЗ

Министру Правительства Москвы,
руководителю Департамента
здравоохранения города Москвы

А.И. Хрипуну

О направлении перечня объектов КИИ

Уважаемый Алексей Иванович!

В соответствии с требованиями пункта 15 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127 направляем Вам на согласование предварительный перечень объектов критической информационной инфраструктуры нашей организации.

№ п/п	Наименование объекта	Тип объекта	Сфера (область) деятельности в которой функционирует объект	Планируемый срок категорирования объекта	Должность, Ф.И.О., контактные данные представителя
1	МИС «_____»	ИС	Здравоохранение	_____2019	Руководитель – Петров П.П. (495)9000009 mail@gkb.ru г. Москва _____
2	ПАКС «_____»	ИС	Здравоохранение	_____2019	
3	ЛИС «_____»	ИС	Здравоохранение	_____2019	

Руководитель МО _____ ФИО

Пример заполненного акта категорирования объекта КИИ

УТВЕРЖДАЮ

Главный врач
Наименование МО

_____ФИО

___ _____2019 г.

АКТ
категорирования объекта КИИ

Состав комиссии	Должность	ФИО
Председатель комиссии	Должность	ФИО
Члены комиссии	Должность	ФИО
	Должность	ФИО
	Должность	ФИО
	Должность	ФИО
	Должность	ФИО

Комиссия, рассмотрев следующие исходные данные:

1. Сведения об объекте критической информационной инфраструктуры

Наименование объекта	Медицинская информационная система
Адреса размещения объекта	г. Москва, ул. г. Москва, _____
Сфера (область) деятельности, в которой функционирует объект	Сфера здравоохранения
Назначение объекта	Автоматизация информационных процессов, сопровождающих лечебно-диагностическую, хозяйственную и управленческую деятельность
Тип объекта	Информационная система
Архитектура объекта	Клиент-серверная система

2. Сведения о субъекте критической информационной инфраструктуры

Наименование субъекта	ГБУЗ «_____ ДЗМ»
Адрес местонахождения субъекта	г. Москва, ул. г. Москва, _____

Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Главный врач
Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов	Заместитель главного врача
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) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Отдел Информационных технологий Начальник отдела информационных технологий
ИНН субъекта и КПП его обособленных подразделений	ИНН - _____ КПП- _____

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

Категория сети электросвязи или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Закрытая внутренняя локально вычислительная сеть, без подключения к внешним линиям связи.
Наименования оператора связи	Внутренняя информационно-коммуникационная сеть
Цель взаимодействия с сетью электросвязи	Передача данных от клиента к серверу
Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Проводной, TCP/IP

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

Наименование лица, эксплуатирующего объект	ГБУЗ «_____»
Адрес местонахождения лица, эксплуатирующего объект	г. Москва, ул. г. Москва, _____
Элемент (компонент) объекта, который эксплуатируется лицом	Объект целиком эксплуатируется субъектом

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

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

Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	- Серверы: 1 шт. - Пользовательские компьютеры – 600 шт. - Отказоустойчивая система хранения данных - Ленточная библиотека
Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Windows 7, Windows 10 Windows Server 2016
Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Microsoft SQL server 2016
Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименование 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	- АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат соответствия СФ/СЗИ-0100, №3025, Kaspersky Security Centre 10 сертификат соответствия СФ/СЗИ-0098, СФ/019-3113, №3155, СФ/019-3468 – ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД

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

Категория нарушителя, 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	Приложение 5 (Распечатать и приложить к акту категорирования объекта КИИ)
Основные угрозы безопасности информации или обоснование их неактуальности	Приложение 6 (Распечатать и приложить к акту категорирования объекта КИИ)

7. Возможные последствия в случае возникновения компьютерных инцидентов инфраструктуры

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.

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры.

Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	Без категории
Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	См. пункт Результаты оценки показателей (ниже по тексту) 127- ПП
Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	См. пункт Результаты оценки показателей (ниже по тексту) 127 - ПП

Результаты оценки показателей:

№	Показатель	Выбранное значение	Обоснование[1]
I. Социальная значимость			
1	Причинение ущерба жизни и здоровью людей (человек)	Не применимо	нарушение функционирования объекта не оказывает влияние на возможность причинения ущерба жизни и здоровью людей.

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

Организационные меры по обеспечению безопасности объекта	Объект КИИ не является значимым - обязательных мер не установлено
Технические меры по обеспечению безопасности объекта	Объект КИИ не является значимым - обязательных мер не установлено

Настоящий акт составлен в единственном экземпляре.

Состав комиссии	Должность	ФИО	Подпись
Председатель комиссии	Должность	ФИО	Подпись
Члены комиссии	Должность	ФИО	Подпись
	Должность	ФИО	Подпись
	Должность	ФИО	Подпись
	Должность	ФИО	Подпись
	Должность	ФИО	Подпись

В случае если будет выявлена категория, в течении десяти рабочих дней, необходимо направить во ФСТЭК России (Приложение 4 – форма уведомления ФСТЭК России «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» в течении десяти рабочих дней направляет сведения о результатах категорирования. Акт категорирования в ФСТЭК не отпраляется.

В течении тридцати дней ФСТЭК России проверяет соблюдение порядка и правильности категорирования и в случае положительного заключения, вносит сведения в реестр значимых объектов КИИ с последующим уведомлением субъекта КИИ в десятидневный срок.

Предоставлять информацию об отсутствии в организации объектов критической информационной инфраструктуры, или о том, что организация не является субъектом КИИ в ФСТЭК России не требуется.

[1] Информация приведена в качестве примера.
В соответствии с разъяснениями ФСТЭК России, 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.

Приложение 4 – форма уведомления ФСТЭК России о сведениях об объектах КИИ

УТВЕРЖДАЮ

Главный врач
Наименование МО

_____ФИО

___ _____2019 г.

О сведениях об объекте
критической информационной инфраструктуры

Уважаемый Дмитрий Николаевич!

В соответствии с требованиями пункта 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных Постановлением Правительства РФ от 8 февраля 2018 г. № 127 направляем Вам сведения о результатах присвоения категорий значимости объекту критической информационной инфраструктуры[1].

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

Руководитель МО _____ ФИО

[1] В соответствии с правилами экспедиции ФСТЭК России, корреспонденция принимается законвертированной, при наличии двух реестров, с печатью организации отправителя. Соответственно, в общий конверт вкладываются:
- общее сопроводительное письмо;
- утвержденные формы (в печатном виде);
- утвержденные формы (копия в электронном виде в формате docx);
- 2 копии реестра описи документов;
- пустой конверт с реквизитами Организации для обратной отправки подписанного реестра со стороны ФСТЭК России.

Сведения о потенциальных нарушителях

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
1	Внешний	Низкий	Хакеры-любители. Бывшие работники	1) Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). 2) Беспроводные каналы передачи данных. 3) Каналы связи, выходящие за пределы контролируемой зоны. 4) Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия)	Должны рассматриваться все основные типы атак, проводимые через внешний периметр ЛВС. Уровень проведения атак — любительский (вредоносное ПО, подбор паролей, атаки на web-ресурсы). Актуальны в случае наличия подключения объекта к сети Интернет (логические ограничения, в том числе средствами межсетевых экранов не считаются ограничивают возможность взлома на 100%)
2	Внешний	Низкий	Операторы сетей связи. Операторы смежных систем, используемых для работы объекта КИИ	1) Нарушение предоставляемых услуг. 2) Нарушение предоставляемых информационных сервисов	Актуальны в случае, если для функционирования объекта необходимы соответствующие услуги связи. Непосредственные атаки можно не рассматривать (т.к. это не категория хакеров). Рассматриваемое нарушение – нарушение функционирования канала связи, а также нарушение конфигурации каналообразующего и маршрутизирующего оборудования

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
3	Внешний	Средний	Хакеры-профессионалы. Конкурирующие организации	1) Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). 2) Беспроводные каналы передачи данных. 3) Каналы связи, выходящие за пределы контролируемой зоны. 4) Отчуждаемые носители информации и мобильные устройства, выносимые за пределы контролируемой зоны.	Должны рассматриваться все основные типы атак, проводимые через внешний периметр ЛВС. Уровень проведения атак – профессиональный (вредоносное ПО, включая адаптированное, проникновение в сеть, APT-атаки и т. д.).
				5) Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия). 6) Внесение закладок при разработке ПО, а также добавление уязвимостей при внесении изменений, обновлений	Актуальны в случае наличия подключения объекта к сети Интернет (логические ограничения, в том числе средствами межсетевых экранов не считаются ограничивают возможность взлома на 100%)
4	Внешний	Средний	Разработчики системного и прикладного ПО, программно-аппаратной платформы без возможности доступа к системе в промышленной эксплуатации	1) Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). 2) Внесение закладок при разработке ПО, а также добавление уязвимостей при внесении изменений, обновлений	Рассматриваемое нарушение – внесение закладок при разработке ПО, а также добавление уязвимостей при внесении изменений, обновлений

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
5	Внешний	Высокий	Хакерские группировки. Специальные службы иностранных государств (блоков государств)	1) Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). 2) Беспроводные каналы передачи данных. 3) Каналы связи, выходящие за пределы контролируемой зоны. 4) Отчуждаемые носители информации и мобильные устройства, выносимые за пределы контролируемой зоны. 5) Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия). 6) Внесение закладок при разработке ПО, а также добавление уязвимостей при внесении изменений, обновлений	Должны рассматриваться все основные типы атак, проводимые через внешний периметр ЛВС. Уровень проведения атак – профессиональный (вредоносное ПО, включая адаптированное, проникновение в сеть, APT-атаки и т.д.). Возможны в том числе атаки на физически изолированные системы – через подключаемые носители, а также атаки с использованием завербованных агентов. Актуальны в случае наличия подключения объекта к сети Интернет (логические ограничения, в том числе средствами межсетевых экранов не считаются ограничивают возможность взлома на 100%)
6	Внутренний	Низкий	Лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т. д.). Лица, обеспечивающие функционирование информационных систем или инфраструктуры оператора (сотрудники	1) Беспроводные каналы передачи данных. 2) Каналы связи, выходящие за пределы контролируемой зоны. 3) Отчуждаемые носители информации и мобильные устройства. 4) Каналы связи, по которым осуществляется передача информации ограниченного доступа. 5) Реализация атак посредством направленных воздействий на	Рассматриваются атаки, связанные с их нахождением в защищаемых помещениях и несанкционированным физическим доступом к оборудованию и системами обеспечения его функционирования (нарушение работы каналов связи, аппаратного обеспечения, систем электропитания, кондиционирования, порча отчуждаемых носителей и т.д.)

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
			ЦОД, ремонтные бригады, электромонтажники и т.д.)	работников Организации (социальная инженерия)	
7	Внутренний	Низкий	Пользователи Объекта КИИ	Беспроводные каналы передачи данных. Отчуждаемые носители информации и мобильные устройства. Каналы связи, по которым осуществляется передача информации ограниченного доступа. Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический). Пользовательский интерфейс взаимодействия с системой (права доступа пользователя). Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия)	Легитимные пользователи. В качестве вероятных угроз нужно рассматривать: Заражение вредоносным ПО (как объекты заражения и распространения). Непреднамеренные нарушения при работе в системе и обработке данных Несанкционированные действия в качестве объектов атак типа социальная инженерия Нарушения по личным причинам или из-за недостаточной компетентности
8	Внутренний	Средний	Посетители, которым предоставляется доступ в ЛВС Организации. Работники Организации, не имеющие санкционированного доступа к объекту КИИ. Работники смежных организаций, которым предоставляется доступ	Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). Беспроводные каналы передачи данных. Отчуждаемые носители информации и мобильные устройства.	Должны рассматриваться все основные типы атак, которые могут проводиться изнутри корпоративной ЛВС. Уровень проведения атак — от любительского до профессионального. Сетевые атаки — в случае возможности доступа к объекту или передаваемой информации через

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
			в ЛВС организации (группа компаний, потребители сервисов и т. д.)	4) Каналы связи, по которым осуществляется передача информации ограниченного доступа. Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический). Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия)	КСПД. Вирусные атаки — могут быть как источниками атаки, так и объектами заражения и распространения в ЛВС. Могут сотрудничать с внешними нарушителями высокого потенциала
9	Внутренний	Средний	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.)	1) Информационные сервисы и ресурсы ИС или смежных систем, имеющих подключение к общедоступным каналам передачи данных (Интернет). 2) Беспроводные каналы передачи данных. 3) Каналы связи, выходящие за пределы контролируемой зоны. 4) Отчуждаемые носители информации и мобильные устройства. 5) Каналы связи, по которым осуществляется передача информации ограниченного доступа. 6) Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический). 7) Реализация атак посредством направленных воздействий на работников Организации (социальная инженерия).	Должны рассматриваться: Вирусные атаки — могут быть как источниками атаки, так и объектами заражения и распространения в ЛВС. Нарушение работоспособности при внесении изменений в конфигурацию или непосредственно в ПО, а также оказания услуг (анализ защищенности, сбор и мониторинг событий и т. д.). Могут также рассматриваться и как непосредственные мотивированные нарушители, которые могут проводить атаки на уровне сети и непосредственно самой системы

№	Тип нарушителя	Потенциал нарушителя	Наименование нарушителя	Каналы реализации угроз	Возможные атаки
				8) Внесение закладок при сопровождении компонентов. 9) Нарушение ИБ объектов в ходе предоставляемых услуг/сервисов	
10	Внутренний	Высокий	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)	1) Беспроводные каналы передачи данных. 2) Отчуждаемые носители информации и мобильные устройства. 3) Каналы связи, по которым осуществляется передача информации ограниченного доступа. 4) Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический). 5) Пользовательский интерфейс взаимодействия с системой (права доступа пользователя). 6) Интерфейсы управления объектом (права доступа администратора)	В случае рассмотрения в качестве нарушителей, должны оцениваться возможности, соответствующие привилегированному доступу: управление компонентами и обрабатываемыми данными

Угрозы информационной безопасности и сценарии компьютерных атак

Актив	Нарушение ИБ	Тип угроз	Сценарии атак
Защищаемая информация, обрабатываемая в ИС, данные о производстве и т.д.	Нарушение конфиденциальности	Несанкционированный доступ к данным в ИС	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 (методы социальной инженерии)
		Несанкционированный доступ к данным при их передаче по каналам связи	
		Несанкционированная передача/распространение данных ограниченного доступа	
		Хищение отчуждаемых носителей и устройств	
	Нарушение целостности	Несанкционированное или ошибочное изменение/подмена данных в системе	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. Модификация данных при их передаче по каналам связи. 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)
		Несанкционированное изменение/подмена данных, передаваемых в каналах связи	

Актив	Нарушение ИБ	Тип угроз	Сценарии атак
	Нарушение доступности	Блокирование данных, обрабатываемых в системе (блокирование доступа, шифрование данных и т.д.)	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. Атаки с использованием вредоносного ПО. Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи.
		Несанкционированное или ошибочное удаление данных	
		Недоступность данных, которые должны поступать из смежных систем	Сетевые атаки (нарушение связи с помощью специальных сетевых пакетов, подмена и изменение адресов, таблиц маршрутизации, обход правил разграничения доступа). Направленные атаки на пользователей (фишинг и иные методы социальной инженерии)
Конфигурация ИС, настройки технологического процесса, управляющие команды в АСУ ТП	Нарушение конфиденциальности	Несанкционированный доступ к конфигурации системы, раскрытие данных технологического процесса	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)
	Нарушение целостности	Несанкционированное или ошибочное изменение/подмена конфигурации, настроек технологического процесса, управляющих воздействий	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. Модификация данных при их передаче по каналам связи Атаки с использованием вредоносного ПО Сетевые атаки (нарушение связи с помощью специальных

Актив	Нарушение ИБ	Тип угроз	Сценарии атак
		Несанкционированное изменение/подмена данных, управляющих команд, передаваемых по каналам связи	сетевых пакетов, подмена и изменение адресов, таблиц маршрутизации, обход правил сетевого разграничения доступа и т. д.). Передача подложных команд, перехват управления. Направленные атаки на пользователей (фишинг и иные методы социальной инженерии)
	Нарушение доступности	Несанкционированное удаление конфигурационных файлов	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. Атаки с использованием вредоносного ПО. Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи. 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)
		Блокирование передаваемых управляющих команд	
Компоненты ИС/ АСУ	Нарушение целостности	Внедрение программных или аппаратных закладок в компоненты	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. 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)
		Нарушение конфигурации (целенаправленно или ошибочно) коммутирующего оборудования и т. д.	
		Ошибки коммутации каналов связи	

Актив	Нарушение ИБ	Тип угроз	Сценарии атак
	Нарушение доступности	Нарушение функционирования компонентов, выведение из строя, перезагрузка, физические воздействия и т. д.	Эксплуатация уязвимостей системного, прикладного или сетевого ПО. Компрометация данных идентификации и аутентификации. Атаки с использованием вредоносного ПО. Атаки типа «отказ в обслуживании» на компоненты системы и каналы связи. Сетевые атаки (нарушение связи с помощью специальных сетевых пакетов, подмена и изменение адресов, таблиц маршрутизации, обход правил сетевого разграничения доступа и т. д.). Передача подложных команд, перехват управления. Направленные атаки на пользователей (фишинг и иные методы социальной инженерии)
		Нарушение работоспособности, сетевые и DoS-атаки на оборудование	
		Физические нарушения каналов связи, обрывы, наводки, недоступность каналов связи провайдера	

Приложение 7 - Сведения об объекте КИИ

к акту категорирования
объекта КИИ

Сведения об объекте КИИ
Информационная система

№	Параметр	Информация (пояснения по заполнению)
Сведения об ИС		
1	Наименование объекта	Указывается наименование ИС. 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 ИС 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

№	Параметр	Информация (пояснения по заполнению)
		обогатительного завода и т. д.
5	Критические процессы (управленческие, технологические, производственные, финансовоэкономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Указываются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции, для обеспечения (управления, контроля) которых используется объект КИИ.
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

№	Параметр	Информация (пояснения по заполнению)
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
11	Наименование оператора связи	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
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
Сведения об угрозах безопасности информации ИС		
14	Сведения о нарушителях безопасности информации ИС	Указываются сведения о потенциальных нарушителях. Используются данные из (Приложение 4: тип, потенциал, наименование, каналы для реализации, возможные атаки). В случае отсутствия потенциальных нарушителей приводится обоснование (например: физически изолированная система, доступ только у доверенных лиц-администраторов, съемные носители не используются)
15	Основные угрозы безопасности информации объекта КИИ	Указываются основные угрозы безопасности информации. Могут использоваться соответствующие данные из 7 раздела (Приложение 6: типы угроз, общий перечень сценариев атак).

№	Параметр	Информация (пояснения по заполнению)
		В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности. Актуально при отсутствии потенциальных нарушителей
16	Возможные сценарии компьютерных атак	Указывается общий перечень сценариев атак из Приложение 6. В случае отсутствия, приводится обоснование их неактуальности (возможно при отсутствии потенциальных нарушителей)
Сведения об реализованных мерах по обеспечению безопасности ИС		
17	Реализованные организационные меры защиты	Указываются реализованные организационные меры защиты. Для упрощения последующих работ лучше сразу указывать в виде мер из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239
18	Применяемые средства защиты информации или сведения об отсутствии средств защиты информации.	Указываются сведения о соответствующих средствах защиты информации, используемых для обеспечения ИБ рассматриваемой ИС (наименования средств защиты информации, реквизиты сертификатов соответствия, если есть). Дополнительно рекомендуется указывать средства защиты, используемые на периметре КСПД (ЛВС) Организации, которые используются для защиты инфраструктуры в целом от внешних нарушителей – с соответствующим уточнением, что для защиты от внешних нарушителей. Для средств защиты информации, встроенных в программное обеспечение, указываются функции безопасности этого программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, иные функции). Для упрощения последующих работ лучше сразу уточнять какую из мер Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017г. N 239 реализуют указываемые средства защиты, *например*: *- АВЗ.1, АВЗ.2 — средство антивирусной защиты Kaspersky Endpoint Security 10, сертификат ИТ.САВЗ.Б2.ПЗ № 3025;* *- СОВ.1, СОВ.2 — Check Point Security Gateway версии R77.10, сертификат ИТ.СОВ.С4.ПЗ № 3634;* *- ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД HP C8R15A.*

№	Параметр	Информация (пояснения по заполнению)
		В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации
Сведения о рекомендуемой к присвоению ИС категории значимости		
19	Категория значимости рекомендуемая	Указываются категория значимости
20	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	Указываются полученные значения по **каждому** из показателей критериев значимости и обоснование полученных результатов. Также приводятся значения показателей в случае, если получены значения ниже нижних показателей. В случае, если показатель не применим к объекту, делается отметка о его неприменимости с соответствующим обоснованием. Приложение 9 раздел 8 (Категория значимости, которая присвоена объекту критической информационной инфраструктуры)
Сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ (ФСТЭК России)		
21	Необходимые меры по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ	Указывается соответствующий перечень необходимых мер, соответствующих рекомендуемой категории значимости, из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239. *Пример:* – *ИАФ.0 Разработка политики идентификации и аутентификации;* – *ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов;* – *ИАФ.2 Идентификация и аутентификация устройств; – и т. д.* В случае, если объекту КИИ не присвоена категория значимости, делается соответствующее указание «Объект КИИ не является значимым – обязательных мер не установлено»

Приложение 8 – форма Приказа

П Р И К А З № ____

г. _____ «___» _____ 2019 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 п. 11 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»,

Приказываю:

1. Создать постоянно действующую 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:
   - в срок до _____ 2019 г. разработать перечень объектов КИИ, подлежащих категорированию;
   - согласовать перечень объектов КИИ, подлежащих категорированию, с Департаментом здравоохранения г. Москвы;
   - в срок до _____ 2019 г. провести категорирование объектов КИИ и оформить решение в виде актов категорирования;
   - направить результаты категорирования в ФСТЭК России в течение 10 рабочих дней со дня утверждения актов, согласно Приказу ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
   - проводить корректировки данных, согласуемых с ФСТЭК России 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.

Главный Врач _____

Форма Приложение № 1
к приказу от _____2019г. №__

С О С Т А В

комиссии по и категорированию объектов
критической информационной инфраструктуры

ФИО	**Должность**
	Председатель Комиссии
	Начальник отдела Заместитель председателя
	Инженер по пожарной безопасности
	Инженер по ГО и ЧС
	Главный Инженер
	Инженер
	Специалист по защите информации секретарь

Форма Приложение №2
к приказу от _____2019г. №__

Положение
о комиссии по категорированию объектов критической информационной инфраструктуры (КИИ)

1. Общие положения

1.1 Настоящее Положение о постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры (далее - Положение) определяет функции, порядок и обеспечение деятельности комиссии по категорированию объектов критической информационной инфраструктуры (далее - Комиссия).

1.2 Комиссия создается для проведения категорирования объектов критической информационной инфраструктуры _____ (далее – учреждение).

1.3 Комиссия является постоянно действующим консультативно-совещательным органом учреждения.

1.4 Комиссия руководствуется в своей деятельности правовыми актами Российской Федерации и настоящим Положением.

1.5 Состав комиссии устанавливается приказом по учреждению.

2. Функции комиссии

2.1 Функциями Комиссии являются:

- определение управленческих, технических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности учреждения;
- выявление наличия критических процессов в учреждении;
- выявление объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, подготовка предложений для включения в перечень объектов;
- рассмотрение возможных действий нарушителей в отношении объектов критической информационной инфраструктуры, а также иных источников угроз безопасности информации;
- анализ угроз безопасности информации которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;
- оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

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

3. Порядок и обеспечение деятельности комиссии

3.1 Заседания Комиссии проводятся по мере необходимости по решению председателя Комиссии.

3.2 Заседание Комиссии считается правомочным при присутствии на нем не менее половины от общего числа членов Комиссии. Присутствие на заседании Комиссии иных лиц, кроме членов Комиссии, допускается с разрешения председателя Комиссии.

3.3 Председатель Комиссии:

- назначает дату, время и место проведения заседаний Комиссии;
- утверждает повестку заседания Комиссии;
- руководит заседанием Комиссии;
- распределяет обязанности между членами Комиссии;
- подписывает акты и иные документы, подготовленные Комиссией;
- пользуется правами члена Комиссии наравне с другими членами Комиссии.

В случае отсутствия председателя Комиссии его полномочия осуществляет один из заместителей председателя Комиссии.

3.4 Секретарь Комиссии:

- координирует деятельность членов Комиссии;
- готовит проекты повесток заседаний Комиссии и представляет на утверждение председателю Комиссии;
- своевременно информирует членов Комиссии о дате, времени, месте и повестке заседаний Комиссии;
- в случае необходимости совместно с членами Комиссии готовит информацию, документы, иные материалы к заседаниям Комиссии;
- в течение 3 рабочих дней с даты проведения заседания Комиссии и в соответствии с ее решением готовит акт и представляет его на подпись председателю Комиссии, заместителю председателя Комиссии, иным членам Комиссии;
- организует и ведет делопроизводство Комиссии.

3.5 Члены Комиссии имеют право:

- участвовать в работе Комиссии;
- участвовать в обсуждении вопросов, включенных в повестку заседания Комиссии, вносить по ним предложения;
- знакомиться с информацией, документами и материалами по вопросам, вынесенным на обсуждение Комиссии, на стадии их подготовки, вносить свои предложения;
- в случае несогласия с принятым решением изложить свое особое мнение в письменном виде, которое прилагается к соответствующему заключению Комиссии.

3.6 Решения Комиссии принимаются простым большинством голосов членов Комиссии как присутствующих на заседании, так и отсутствующих,

выразивших свое мнение в письменном виде и представивших его на заседание Комиссии.

3.7 Каждый член Комиссии имеет один голос. При равенстве голосов принятым считается решение, за которое проголосовал председательствующий на заседании Комиссии.

3.8 Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры. Акт подписывается председателем, заместителем председателя, секретарем и другими членами и утверждается директором учреждения.

3.9 Организационное и материально-техническое обеспечение деятельности Комиссии осуществляет _____

Приложение 9

Сведения о 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

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
Адреса размещения 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. В случае, если объект КИИ — ИТС, указывается место расположения сетевого оборудования (активного и пассивного)
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
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.
Тип объекта	(информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)
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

Наименование субъекта	Наименование субъекта КИИ — лица, которое владеет объектом КИИ
Адрес местонахождения субъекта	Юридический адрес Адрес фактического местонахождения субъекта (если отличается)
Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Должность, Ф.И.О. руководителя
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
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) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Указываются соответствующие данные: – Структурное подразделение, ответственное за обеспечение безопасности значимых объектов; – 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)
ИНН субъекта и КПП его обособленных подразделений	Указываются соответствующие данные: ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта

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

Категория сети электросвязи 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.
Наименования оператора связи	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.
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.
Способ взаимодействия с сетью электросвязи	Указывается соответствующая информация о взаимодействии с сетями электросвязи: тип доступа к сети электросвязи (проводной, беспроводный), используемых технологий доступа, 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

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

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

Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	Указываются наименования программно-аппаратных средств и их количество: – пользовательские компьютеры — 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.
Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Указываются наименования клиентских, серверных операционных систем, средств виртуализации (при наличии)
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

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, если есть). Дополнительно рекомендуется указывать средства защиты, используемые на периметре КСПД (ЛВС) Организации, которые используются для защиты инфраструктуры в целом от внешних нарушителей — с соответствующим уточнением, что для защиты от внешних нарушителей. Для средств защиты информации, встроенных в программное обеспечение, указываются функции безопасности этого программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, иные функции). Для упрощения последующих работ лучше сразу уточнять какую из мер Приложения 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 ИТ.САВЗ.Б2.ПЗ № 3025; – СОВ.1, СОВ.2 — Check Point Security Gateway версии R77.10, сертификат ИТ.СОВ.С4.ПЗ № 3634; – ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД HP C8R15A. 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

Категория нарушителя, 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	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: – 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)
Основные угрозы безопасности информации или обоснование их неактуальности	Указываются основные угрозы безопасности информации. В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности (допускается в случае отсутствия потенциальных нарушителей и каналов реализации угроз)

7. Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак	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

Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	Устанавливаются 3 категории значимости. Самая высокая категория - первая, самая низкая - третья. Если нет категории то пишется без категории
Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения берутся из 127- ПП - Социальная значимость Причинение ущерба жизни и здоровью людей (человек) - Политическая значимость - Экономическая значимость - Экологическая значимость - Значимость для обеспечения обороны страны, безопасности государства и правопорядка
Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту я из 127- ПП

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

Организационные меры по обеспечению безопасности объекта	Указывается соответствующий перечень необходимых организационных мер, соответствующих присвоенной объекту КИИ категории значимости, из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239 В случае, если объекту КИИ не присвоена категория значимости, делается соответствующее указание «Объект КИИ не является значимым — обязательных мер не установлено»
Технические меры по обеспечению безопасности объекта	Указывается соответствующий перечень технических мер, соответствующих присвоенной объекту КИИ категории значимости, из Приложения к Требованиям по обеспечению безопасности значимых объектов КИИ РФ, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. N 239, например: – ИАФ.0 Разработка политики идентификации и аутентификации; – ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов; – ИАФ.2 Идентификация и аутентификация устройств; – и т. д. В случае, если объекту КИИ не присвоена категория значимости, делается соответствующее указание «Объект КИИ не является значимым — обязательных мер не установлено»