Приложение 1 к распоряжению Департамента информационных технологий города Москвы
от _____ 2019 г.
№ _____

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОПРЕДЕЛЕНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И КАТЕГОРИЙ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Содержание

Перечень сокращений

В настоящем документе используются сокращения, приведенные в таблице 1.

Таблица 1 − Перечень сокращений

Сокращение	Обозначение
АСУ	Автоматизированная система управления
ИС	Информационная система
ИСиР	Информационные системы и ресурсы
ИТКС	Информационно-телекоммуникационная сеть
КИИ	Критическая информационная инфраструктура
ЛВС	Локальная вычислительная сеть
ОКВЭД	Общероссийский классификатор видов экономической деятельности
ОКОГУ	Общероссийский классификатор органов государственной власти и управления
РФ	Российская Федерация
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных

Перечень терминов

В настоящем документе используются термины, приведенные в таблице 2.

Таблица 2 − Перечень терминов

Термин	Определение	Источник
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	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Безопасность информации	Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Безопасность критической информационной инфраструктуры	Состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Вредоносное программное обеспечение	компьютерная программа, предназначенная для нанесения вреда (ущерба) владельцу (пользователю) компьютерной информации, хранящейся на средстве вычислительной техники, путем ее несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на средств защиты, или для получения доступа к вычислительным ресурсам самого средства вычислительной техники с целью их несанкционированного использования	Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения»
Государственные информационные системы	Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Термин	Определение	Источник
Доступ к информации	Возможность получения информации и ее использования	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Доступность информации (ресурсов информационной системы)	Состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005 Техническая защита информации. Основные термины и определения
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	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Информационно-телекоммуникационная сеть	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
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	ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Термин	Определение	Источник
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	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
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	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Конфиденциальность информации	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Критическая информационная инфраструктура	Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Нарушитель безопасности информации	Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации	ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
Несанкционированный доступ к информации	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.	Руководящий документ Защита от несанкционированного доступа к информации Термины и определения

Термин	Определение	Источник
	Примечание: Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.	Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.
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	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Объект критической информационной инфраструктуры	Информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Оператор информационной системы	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Распространение информации	Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
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,	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Термин	Определение	Источник
	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, создающих потенциальную или реально существующую опасность нарушения безопасности информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

1 Общие положения

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.

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 городу Москве в лице органов исполнительной власти города Москвы, государственных учреждений города Москвы и иных организаций, подведомственных органам исполнительной власти города Москвы (далее – ИСиР ОИВ/организации) к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры органа исполнительной власти города Москвы (далее – Перечень объектов ОИВ) или Перечень объектов критической информационной инфраструктуры подведомственной Департаменту организации (далее – Перечень организации), 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 законодательства, 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[1] России. 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».

[1] Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Важно: Постановлением Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018г. № 127» для государственных органов и государственных учреждений установлен срок по формированию и утверждению перечня объектов критической информационной инфраструктуры, подлежащих категорированию – до 1 сентября 2019 г.

2 Нормативные ссылки

Настоящие Методические рекомендации разработаны с учетом требований законодательства Российской Федерации:

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

– 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»;

– Постановление Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»;

– Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

– Информационное сообщение ФСТЭК России по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 24 августа 2018 г. № 240/25/3752;

– Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.;

– Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры;

– Информационное сообщение ФСТЭК России о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры российской федерации от 4 мая 2018 г. № 240/22/2339.

3 Основные мероприятия по определению оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры

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

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

- здравоохранения;
- 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.

2) российское юридическое лицо и (или) индивидуальный предприниматель, который обеспечивает взаимодействие указанных систем или сетей. ***(Важно:*** *к государственным органам и государственным учреждениям не применимо.***)**

3.1. Определение сфер деятельности организации.

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

При этом, ФСТЭК России был предложен метод, основанный на определение сферы деятельности организации в соответствии с:

- ОКВЭД и ОКОГУ;

– лицензиями, сертификатами и иными разрешительными документами на виды деятельности;

– учредительными документами, уставами, положениями организации, где прописаны основные и вспомогательные виды деятельности.

Соответственно, если в любом из данных источников присутствует указание на рассматриваемые сферы деятельности, то по мнению ФСТЭК России, присутствуют признаки того, что организация является субъектом КИИ.

1. В Лицензиях / Уставе / кодах ОКВЭД и ОКОГУ организации выявляем деятельность в областях, соответствующих 187-ФЗ.
2. Анализируем область функционирования используемых ИСиР (Распоряжения Правительства Москвы по созданию ИСиР, государственные программы, проектную документацию на создание ИСиР и подобное).
3. Определяем ИСиР, используемые для реализации соответствующего вида деятельности, указанного в уставе, лицензии или ОКВЭД.
4. Анализируем на предмет принадлежности данных ИСиР Организации (право собственности, аренда, договор пользования, хозяйственного ведения, право оперативного управления и т. д.).

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

Пример 1

ГКУ ИАЦ в сфере здравоохранения города Москвы

Код ОКВЭД 72.1 «Научные исследования и разработки в области естественных и технических наук» и код ОКОГУ 2300229 «Органы исполнительной власти субъектов Российской Федерации / - здравоохранения»

Необходимо выявить ИСиР автоматизирующие процессы в сферах науки и здравоохранения.

Пример 2

АО «Электронная Москва» имеет лицензии Роскомнадзора на следующие услуги связи:

Услуги связи по предоставлению каналов связи

Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации

Услуги на телематические услуги связи

Необходимо выявить ИСиР автоматизирующие процессы оказание услуг связи.

3.2. Определение деятельности в организации по обеспечению взаимодействия объектов КИИ

В качестве обеспечения взаимодействия объектов КИИ может рассматриваться:

– предоставление вычислительных мощностей для объектов КИИ и каналов взаимодействия с ними (ЦОД);

– предоставление телекоммуникационных услуг, в рамках которых осуществляется взаимодействие объектов КИИ;

– предоставление иных информационных услуг для обеспечения взаимодействия с объектами КИИ.

Частными случаями таких субъектов являются операторы сетей связи или ИС, предназначенных для обеспечения работы государственных ИС или взаимодействия с объектами энергетического комплекса — для данных лиц ответственность за обеспечение взаимодействия объектов КИИ указывается в документации на системы/каналы связи, а также в их обязанностях.

В более неопределенных случаях, когда Организация предоставляет вычислительные мощности и каналы связи для широкого круга заказчиков, детальной информации о том, что инфраструктура может использоваться для организации взаимодействия КИИ, может не быть. Однако, незнание данной информации не освобождает организацию от ответственности.

1. Проводим анализ наличия объектов инфраструктуры, находящейся в собственности Организации, которая используется в интересах сторонних лиц и для организации информационного взаимодействия систем, не принадлежащих самой Организации.

Пример 3

Права собственника и оператора АИС СУДИР возложены на ДИТ.

При этом, СУДИР обеспечивает предоставление доступа к информационным системам и ресурсам, принадлежащих другим ОИВ города Москвы на основе централизованного управления учетными данными участников информационного взаимодействия и реализации технологии однократной аутентификации пользователей информационных систем города Москвы

2. В случае выявления соответствующих объектов инфраструктуры, уточняем наличие у Организации явных поручений на уровне законодательных актов и нормативных требований (Распоряжения Правительства Москвы и т.д.), возлагающих на Организацию обязанности по обеспечению информационного взаимодействия между сторонними ИСиР. В случае наличия указанных обязательств, запрашиваем владельцев сторонних ИСиР (ОИВ и их организаций) об отнесении данных систем к объектам КИИ (включена ли данная ИСиР в Перечень объектов КИИ, подлежащих категорированию сторонней организации). В случае положительного ответа, Организация признается субъектом КИИ.

3. В случае наличия инфраструктуры Организации, которая используется для информационного обмена сторонними ИСиР, делается запрос владельцам данных

систем об их отнесении к объектам КИИ (включена ли данная ИСиР в Перечень объектов КИИ, подлежащих категорированию сторонней организации). В случае положительного ответа, делается уточнение наличия компонентов инфраструктуры и сетей передачи данных, используемых для указанного взаимодействия и находящихся в собственности Организации. В случае положительного заключения Организация признается субъектом КИИ.

4. Организация рассматривает свою инфраструктуру (или ее часть, непосредственно задействованную в обеспечении взаимодействия объектов КИИ) в качестве объекта КИИ.

Пример 4

Организация владеет и обслуживает ЦОД, в котором размещаются ИСиР ОИВ Москвы, в сфере транспорта или здравоохранения.

Выявлено, что некоторые из размещаемых в ЦОД ИСиР относятся к объектам КИИ. Программно-аппаратное обеспечение компонентов ИС является собственностью ОИВ Москвы, в сфере транспорта или здравоохранения. При этом, для взаимодействия между данными ИС, а также с внешними системами и пользователями используются каналы передачи данных и коммутационное оборудование ЦОД, которые принадлежат Организации. В данном случае ***Организация является субъектом КИИ****, как обеспечивающая взаимодействие объектов КИИ.*

ВАЖНО: *Сеть электросвязи Организации, непосредственно задействованная в обеспечении взаимодействия объектов КИИ, не должна рассматриваться в качестве объекта КИИ и в Перечень объектов КИИ, подлежащих категорированию, не включается.*

Пример 5

Организация предоставляет услуги технической поддержки и сопровождения ОИВ Москвы, в сфере транспорта или здравоохранения.

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

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

Результат:

Заключение Рабочей группы о наличии/отсутствии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры и рекомендаций по включению их в Перечень объектов с последующим установлением одной из категорий значимости объектов критической информационной инфраструктуры, либо об отсутствии оснований для отнесения ИСиР

ОИВ/организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации.

Заключение об отсутствии оснований может оформляться по консолидированной форме на все ИСиР ОИВ/организации сразу, форма заключения Рабочей группы об отсутствии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации приведена в Приложении 1.

Но желательно оформление отдельного заключения о наличии/отсутствии оснований по каждой информационной системе ОИВ/организации в отдельности. Форма заключения Рабочей группы об отсутствии оснований для отнесения ИС ОИВ/организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации приведена в Приложение 2. Форма заключения Рабочей группы о наличии оснований для отнесения ИС ОИВ/организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации приведена в Приложении 3.

4. Мероприятия по инвентаризации и категорированию объектов КИИ

4.1. Инвентаризация объектов КИИ

В случае принятия решения о наличии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры, необходимо провести предварительный анализ угроз безопасности информации и реализованных меры по обеспечению безопасности. Провести предварительную оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов в ИСиР в соответствии с перечнем показателей критериев значимости, утвержденных ПП-127. Сформировать предложение Рабочей группы о присвоении данной ИСиР категории значимости либо об отсутствии необходимости присвоения одной из таких категорий, а также перечень необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Подготовленные материалы служат основаниями для принятия окончательных решений Комиссией по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры.

В соответствии с ПП-127, категорированию подлежат объекты КИИ, которые обеспечивают 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 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

4.1.2 Формирование перечня процессов

Анализируется устав и учредительные документы, иные положения организации, где прописаны основные и вспомогательные виды деятельности, имеющиеся лицензии, сертификаты и иные разрешительные документы на виды деятельности — из них выписываются все указанные функции и виды деятельности.

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

Для каждой выявленной функции / осуществляемого вида деятельности формируется перечень процессов, реализуемых в рамках этой функции / вида деятельности.

В соответствии с ПП-127, необходимо формировать перечень процессов, с учетом их соотнесения с отраслями / областями деятельности, которые обозначены в 187-ФЗ. Субъекты КИИ определяются через 13 сфер функционирования ИС / АСУ / ИТКС.

Пример 6

Процессы ДИТ в сфере связи:

Постановление Правительства Москвы №105-ПП «Об утверждении Положения о Департаменте информационных технологий города Москвы»

- Создание и эксплуатации городской мультисервисной транспортной сети (ГМТС) Правительства Москвы.

- Организация работ по подготовке технических условий, согласованию и оформлению разрешительной документации для выполнения работ по прокладке волоконно-оптических линий для системы обеспечения безопасности города Москвы и комплексной автоматизированной системы обеспечения безопасности населения города Москвы.

- Утверждение порядка разработки и согласования схемы размещения таксофонов на территории города Москвы.

- Согласование передачи прав пользования, владения, распоряжения линейно-кабельными сооружениями связи и сетями связи и иным движимым и недвижимым имуществом, необходимым для их эксплуатации, находящимся в собственности города Москвы.

- Определение порядка пользования, владения, распоряжения линейно-кабельными сооружениями связи и сетями связи и иным движимым и недвижимым имуществом, необходимым для их эксплуатации, находящимся в собственности города Москвы.

- Утверждение по согласованию с Департаментом городского имущества города Москвы порядка приемки во временную эксплуатацию вновь построенных или реконструированных за счет средств бюджета города Москвы линейно-кабельных сооружений связи и сетей связи и иного движимого и недвижимого имущества, необходимого для их эксплуатации.

- Обеспечение содержания, обслуживания и временной эксплуатации бесхозяйных линейно-кабельных сооружений связи и сетей связи и иного движимого и недвижимого имущества, необходимого для их эксплуатации, до признания прав собственности города Москвы на такое имущество.

- Обращение в уполномоченный орган государственной власти с целью постановки на учет бесхозяйных линейно-кабельных сооружений связи и сетей связи, а также государственной регистрации прав собственности города Москвы на линейно-кабельные сооружения связи и сети связи и иное движимое и недвижимое имущество, необходимое для их эксплуатации, в том числе бесхозяйные линейно-кабельные сооружения и сети связи и иное движимое и недвижимое имущество, необходимое для их эксплуатации.

- Обеспечение выдачи технических условий при строительстве и/или реконструкции линейно-кабельных сооружений и сетей связи, вновь возводимых и/или реконструируемых на территории города Москвы за счет средств бюджета города Москвы.

- Утверждение рекомендуемой формы договора на размещение таксофона.

4.1.3 Определение критичности процессов

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

В связи с тем, что критерии оценки критичности нарушения процессов в ПП-127 явно не заданы, то будем использовать перечень критериев значимости объектов и их значения из Приложения 1 к ПП-127 (минимальные показатели категории значимости). Определяем для каждого рассматриваемого процесса, способно ли его нарушение повлечь последствия, соответствующие, минимальным показателям критериев значимости из ПП-127.

Пример 7

Остановка процесса «Утверждение порядка разработки и согласования схемы размещения таксофонов на территории города Москвы» не приводит к прекращению или нарушению функционирования сетей связи и не приводит к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

4.1.4 Формирование перечня объектов

Для каждого критичного процесса определяется перечень ИСиР, которые осуществляют:

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

Важно:

Обработка – систематическое выполнение операций над данными, необходимыми для обеспечения критического процесса.

Управление – поддержание критического процесса в рабочем состоянии в рамках заданных значений характеристик критического процесса.

Контроль – сравнение (сопоставление) фактических (текущих) значений характеристик критического процесса с заданными значениями этих характеристик.

Мониторинг – постоянное (регулярное) наблюдение за значениями характеристик критического процесса.

Результат:

Сформирован Перечень ИСиР, подлежащих категорированию и оформлен в табличной форме (таблица 3).

Пример 8

№	*Наименование ИСиР*	*Тип ИСиР*	*Назначение*	*Сфера деятельности, в которой функционирует ИСиР*
1	*Система №1*	*Информационная система*	*Мониторинг*	*Связь*
2	*Система №2*	*Информационная система*	*Обработка*	*Здравоохранение*

Комиссия по категорированию принимает окончательное решение о формировании перечня объектов, подлежащих категорированию.

Перечень объектов, подлежащих категорированию оформляется по форме, приведенной в таблице 4, рекомендованной ФСТЭК России. Утверждается и направляется в экспедицию центрального аппарата ФСТЭК России по адресу: 105066, г. Москва, ул. Старая Басманная, д. 17 на бумажном носителе и на электронном носителе информации (формат docx, xlsx). Телефон экспедиции: 8 (495) 696-74-06.

Таблица 4.

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

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

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

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Важно: планируемый срок категорирования не должен превышать 365 календарных дней с момента утверждения перечня объектов, подлежащих категорированию. Для государственных органов и организаций он не может **быть позже 01.09.2020 г.**

4.2. Категорирование объектов КИИ

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

При категорировании осуществляется:

– анализ возможных источников угроз и действий предполагаемых нарушителей;

– анализ возможных угроз и типов компьютерных атак;

– оценка масштаба последствий угроз и соотнесение со значениями показателей категорий;

– определение категории значимости объекта КИИ;

– оформление акта категорирования.

4.2.1 Анализ возможных действий нарушителей

Данная информация получается экспертным путем. В случае, если для рассматриваемой ИСиР существует модель угроз и нарушителей, то используются данные из нее. Также могут использоваться существующие данные из моделей угроз и моделей нарушителей для схожих ИСиР, функционирующих в Организации.

Если для данной ИСиР не разрабатывалась модель угроз и нарушителя, то используем классификацию, приведенную в Приложении 4.

4.2.2 Анализ угроз безопасности информации и типов компьютерных атак

Для каждой ИСиР проводится анализ возможных угроз и их последствий. В случае, если для рассматриваемой ИСиР существует модель угроз и нарушителей, то используются данные из нее. Также могут использоваться существующие данные из моделей угроз и моделей нарушителей для схожих ИСиР, функционирующих в Организации.

Если для данной ИСиР не разрабатывалась модель угроз и нарушителя, то используем классификацию, приведенную в Приложении 5.

4.2.3 Оценка масштаба последствий и соотнесение со значениями показателей категорий

Для рассматриваемой ИСиР необходимо определить возможные последствия нарушений, основываясь на выявленных возможных угрозах ИБ, типах компьютерных атак, назначение ИСиР и автоматизируемого процесса. Для рассматриваемой ИСиР

должны выбираться те типы последствий, которые могут стать следствием реализации вероятных угроз для данной ИСиР. В качестве последствий рассматриваем:

1) причинение ущерба жизни и здоровью людей;

2) прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов обеспечивающие водо-, тепло-, газо- и электроснабжение населения;

3) прекращение или нарушение функционирования объектов транспортной инфраструктуры;

4) прекращение или нарушение функционирования сети связи;

5) отсутствие доступа к государственной услуге;

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

7) нарушение условий международного договора 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, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период);

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

Важно: для периода **2019-2021** это 20 388, 65 млрд. рублей. Соответственно, если оцениваемый ущерб бюджетам РФ менее 20 388,65 млн. рублей, то принимается решение об отсутствии необходимости присвоения категории значимости. В иных случаях необходимо руководствоваться таблицей 5:

Таблица 5.

Категория значимости	**3**	**2**	**1**
Ущерб, млрд. руб	до 1019,43, включительно	от 1019,43 до 2038,86, включительно	более 2038,86

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

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

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 атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия);

12) прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые 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.

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

– договоры на оказание соответствующих услуг (учет количества потребителей и подключаемых территориальных объектов);

– паспорта объектов (систем);

– ТЗ на объекты;

– результаты категорирования объектов транспортной инфраструктуры;

– декларация промышленной безопасности;

– паспорта безопасности опасного производственного объекта;

– декларация безопасности объектов;

– паспорта безопасности объектов топливно-энергетического комплекса;

– результаты категорирования объектов, оказывающих негативное воздействие на окружающую среду;

– результаты классификации сетей электросвязи.

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

Должны быть рассмотрены наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной

инфраструктуры, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба.

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

В случае если показатель критерия значимости неприменим для ИСиР или ИСиР не соответствует ни одному показателю и их значениям (оцененный масштаб ниже минимального показателя критерия значимости), категория значимости данной ИСиР не присваивается.

4.2.4 Определение категории значимости объекта КИИ

Объекту КИИ присваивается категория значимости, соответствующая наивысшему значению из присвоенных категорий при соотнесении возможного ущерба с показателями категорий значимости (самая высокая категория – первая, самая низкая – третья). Форма для оформления результатов предварительного категорирования, проведенного рабочей группой приведена в Приложении 6.

Важно: эта информация используется комиссией по категорированию для принятия и оформления окончательного решения по ИСиР.

Результат:

Собрана в формализованном виде информация по ИСиР, рекомендованных к отнесению к объектам КИИ. Пример оформления приведен в Приложении 7.

4.2.6 Оформление акта категорирования объекта КИИ

Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры.

Допускается оформление единого акта по результатам категорирования нескольких объектов критической информационной инфраструктуры, принадлежащих одному субъекту критической информационной инфраструктуры.

Важно: акт утверждает исключительно руководитель ОИВ/организации. Акт хранится в ОИВ/организации, направлять в ФСТЭК России не требуется.

Форма рекомендуемого акта приведена в Приложении 8.

Пример оформления сведений о результатах категорирования ИСиР для отправки в ФСТЭК России приведена в Приложении 9.

5. Рекомендуемая литература

– Методические рекомендации по категорированию объектов критической информационной инфраструктуры в медицинских организациях Красноярского края от 30.11.2018.

– Методические рекомендации по категорированию объектов критической информационной инфраструктуры. ООО «СТЭП ЛОДЖИК» v2.0, 2019.

– Общие рекомендации «Безопасность объектов критической информационной инфраструктуры организации» Версия 1.0. АРСИБ 2019.

– Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи. ОГО «АДЭ» 2019.

– Приказ Минтранса России от 14.12.2018 № 449 «О создании Комиссии Министерства транспорта Российской Федерации по согласованию перечней объектов критической информационной инфраструктуры подведомственных Минтрансу России службы, агентств, предприятий, учреждений и организаций».

Приложение 1
к Методическим рекомендациям
Форма заключения об отсутствии оснований по отнесению информационных систем и ресурсов к объектам критической информационной инфраструктуры

ЗАКЛЮЧЕНИЕ
об отсутствии оснований по отнесению ИСиР к объектам КИИ

1. Настоящее Заключение составлено Рабочей группой, созданной на основании распоряжения руководителя Департамента информационных технологий города Москвы.

2. В соответствии с Постановлением Правительства Москвы от 05.04.2011 № 105-ПП «Об утверждении Положения о Департаменте информационных технологий города Москвы», Департамент осуществляет полномочия в следующих сферах деятельности:

- сфера деятельности, связанная с использованием вычислительной техники и информационных технологий;
- деятельность по созданию и использованию баз данных и информационных ресурсов.

3. Сведения, внесенные в Единый Государственный Реестр Юридических Лиц (ЕГРЛ) содержат информацию о следующих видах экономической деятельности по Общероссийскому классификатору видов экономической деятельности (ОКВЭД ОК 029-2014 КДЕС. Ред.2):

- основной вид деятельности: 84.11.21 Деятельность органов государственной власти субъектов Российской Федерации (республик, краев, областей), кроме судебной власти, представительств исполнительных органов государственной власти субъектов Российской Федерации при Президенте Российской Федерации;
- дополнительный вид деятельности: 62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая;
- дополнительный вид деятельности: 63.11.1 Деятельность по созданию и использованию баз данных и информационных ресурсов.

4. Лицензии на виды деятельности, определенных Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» на Департамент не оформлялись.

5. Рабочая группа определила, что ИСиР Департамента не имеют признаков объектов критической информационной инфраструктуры и не функционируют в следующих сферах: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

РАБОЧАЯ ГРУППА СЧИТАЕТ:

Объекты критической информационной инфраструктуры Российской Федерации, принадлежащие на праве собственности, аренды или на ином законном основании городу Москве в лице Департамента – не выявлены. Основания для отнесения ИСиР Департамента к объектам критической информационной инфраструктуры – отсутствуют.

Настоящее Заключение составлено в единственном экземпляре.

Приложение 2
к Методическим рекомендациям
Форма заключения об отсутствии оснований по отнесению информационной системы к объектам критической информационной инфраструктуры

ЗАКЛЮЧЕНИЕ
об отсутствии оснований по отнесению ИС к объектам КИИ

1. Настоящее Заключение составлено рабочей группы по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры (далее – Рабочая группа), созданной на основании распоряжения Департамента информационных технологий города Москвы от 19.04.2019 № 64-16-139/19 «Об утверждении составов рабочих групп по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры» в целях обеспечения принятия решений Департаментом информационных технологий города Москвы (далее – Департамент) об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании городу Москве в лице Департамента, Департаменту (далее – ИСиР Департамента) к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры Департамента (далее – Перечень объектов), 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».

2. Присутствовали 9 из 9 членов рабочей группы. Кворум имеется

3. Рабочая группа определила в отношении автоматизированной информационной системе «Наименование ххх» (далее - АИС «ххх»), что согласно п. 2.1. Постановления Правительства Москвы от хх.хх.2014 № хх5-ПП «Наименование ххх» Департамент осуществляет от имени города Москвы правомочия собственника АИС «ххх». Разделом № 1 в «Положение об автоматизированной информационной системе «Наименование ххх» установлено, что АИС «ххх» создана в целях информационного обеспечения деятельности Департамента строительства города

Москвы Правительство Москвы для обеспечения градостроительной деятельности в городе Москве.

РАБОЧАЯ ГРУППА ПРИНЯЛА РЕШЕНИЕ:

АИС «ххх» функционирует в сфере «Градостроительная деятельность». Основания для отнесения автоматизированной информационной системе «Наименование ххх» к объектам критической информационной инфраструктуры отсутствуют.

Результаты открытого голосования: «За» – 9 голосов, «Против» – 0 голосов, «Воздержалось» – 0 голосов.

Настоящее Заключение составлено в единственном экземпляре.

Приложение 3
к Методическим рекомендациям
Форма заключения об отсутствии оснований по отнесению информационных систем и ресурсов к объектам критической информационной инфраструктуры

ЗАКЛЮЧЕНИЕ
о наличии оснований по отнесению ИСиР к объектам КИИ

1. Настоящее Заключение составлено рабочей группы по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры (далее – Рабочая группа), созданной на основании распоряжения Департамента информационных технологий города Москвы от 19.04.2019 № 64-16-139/19 «Об утверждении составов рабочих групп по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры» в целях обеспечения принятия решений Департаментом информационных технологий города Москвы (далее – Департамент) об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании городу Москве в лице Департамента, Департаменту (далее – ИСиР Департамента) к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры Департамента (далее – Перечень объектов), 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».

2. Присутствовали 9 из 9 членов рабочей группы. Кворум имеется.

3. Рабочая группа выявила технологический процесс мониторинга оказания телекоммуникационных услуг, в том числе услуг связи, рамках выполнения Департаментом полномочий и функций в установленной Положением о Департаменте сфере деятельности.

4. Рабочая группа определила в отношении информационной системы «Полное наименование системы» (далее - ИС «Краткое наименование системы»), что согласно п.2 Постановления Правительства Москвы от хх.хх.2019 № хх-ПП «Об информационной системе «Полное наименование системы» Департамент

осуществляет от имени города Москвы правомочия собственника ИС «Краткое наименование системы». Разделом № 2 в «Положение об информационной системе «Полное наименование системы» установлено, что основной задачей ИС «Краткое наименование системы» является автоматизация процесса непрерывного и качественного оказания телекоммуникационных услуг, в том числе услуг связи пользователям ИС «Краткое наименование системы», что позволяет отнести ИС «Краткое наименование системы» к информационным системам, функционирующим в сфере связи. Дополнительно ИС «Краткое наименование системы» обеспечивает автоматизацию процессов взаимодействия между участниками информационного взаимодействия с целью обеспечения контроля качества оказываемых телекоммуникационных услуг, в том числе услуг связи для нужд органов исполнительной власти города Москвы и подведомственных им организаций города Москвы. Проведенная оценка значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов в ИС «Краткое наименование системы» показала, что компьютерные инциденты в ИС «Краткое наименование системы» не приводят к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка. Результаты оценки значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов в ИС «Краткое наименование системы» приведены в таблице № 1.

Компьютерные инциденты в ИС «Краткое наименование системы» могут привести к:

– несанкционированному или ошибочному изменению/подмене данных в системе;

– блокированию данных, обрабатываемых в системе (блокирование доступа, шифрование данных и т.д.);

– несанкционированному или ошибочному удалению данных;

– недоступности данных, которые должны поступать из смежных систем.

Возможные нарушители для ИС «Краткое наименование системы»:

– внешний, с низким потенциалом;

– внутренний, с низким потенциалом;

– внутренний, с средним потенциалом.

Нарушителями при проведении компьютерных атак на ИС «Краткое наименование системы» могут быть предприняты следующие действия:

– компрометация данных идентификации и аутентификации;

– модификация данных при их передаче по каналам связи;

– 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 разграничения доступа);

– направленные атаки на пользователей (фишинг и иные методы социальной инженерии).

Таблица № 1.

№	Показатель	Значение показателя	Обоснование
1	Причинение ущерба жизни и здоровью людей	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, влияющих на жизнь и здоровье людей
2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, обеспечивающих функционирование объектов обеспечения жизнедеятельности населения
3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, обеспечивающих функционирование объектов транспортной инфраструктуры
4	Прекращение или нарушение функционирования сети связи	Не применимо	ИС «Краткое наименование системы» система мониторинга, не влияющая на прекращение или нарушение функционирования контролируемой сети связи
5	Отсутствие доступа к государственной услуге	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на доступность государственных услуг
6	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования государственного органа
7	Нарушение условий международного договора РФ, срыв переговоров или подписания	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая соблюдение условий международных договоров РФ

№	Показатель	Значение показателя	Обоснование
	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, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период)	Показатель и его значения не применимы к объекту	Не применимо для Департамента, как ОИВ субъекта Федерации
9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации,	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на выплаты в бюджет РФ

№	Показатель	Значение показателя	Обоснование
	осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)		
10	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн.	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» не обеспечивает проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций. ДИТ города Москвы не является 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

№	Показатель	Значение показателя	Обоснование
	единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)		
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 атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия)	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не оказывающая какие-либо воздействия на окружающую среду. Управление объектами, способными оказать негативное воздействие на окружающую среду.
12	Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра	Показатель и его значения не применимы к объекту	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования пунктов управления.
13	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	Показатель и его значения не применимы к объекту	Не применимо для Департамента, как ОИВ субъекта Федерации
14	Прекращение или нарушение	Показатель и его значения не	ИС «Краткое наименование системы» система мониторинга оказания

№	Показатель	Значение показателя	Обоснование
	функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	применимы к объекту	телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС в области обеспечения обороны страны, безопасности государства и правопорядка

РАБОЧАЯ ГРУППА ПРИНЯЛА РЕШЕНИЕ:

1. ИС «Краткое наименование системы» функционирует в сфере «Связь». Основания отнесения информационной системы «Единая система мониторинга» к объектам критической информационной инфраструктуры в наличии.

2. Необходимость присвоения категории значимости ИС «Краткое наименование системы» отсутствует.

Результаты открытого голосования: «За» – 5 голосов, «Против» – 4 голоса, «Воздержалось» – 0 голосов.

Настоящее Заключение составлено в единственном экземпляре.

Приложение 4
к Методическим рекомендациям
Сведения о потенциальных нарушителях

Сведения о категориях нарушителей

№	Категория нарушителя	Потенциал нарушителя	Оснащенность	Знания	Мотивация
1	Внешний	Низкий	Общедоступные программные (программно-аппаратные) средства	Отсутствие знаний о структуре ОКИИ, системе безопасности ОКИИ. Не обладает специальными знаниями по реализации угроз безопасности.	–Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики; –дискредитация или дестабилизация деятельности органов государственной власти, субъектов КИИ; –идеологические или политические мотивы; –конкурентная борьба; –материальная (имущественная); –любопытство; –месть; –хулиганство.
2	Внешний	Средний	Общедоступные программные (программно-аппаратные) средства, специализированные программные (программно-аппаратные) средства	Знание о структуре ОКИИ, системе безопасности ОКИИ. Обладает специальными знаниями по реализации угроз безопасности.	
3	Внешний	Высокий	Общедоступные программные (программно-аппаратные) средства, специализированные программные (программно-аппаратные) средства, средства изготовленные на заказ	Знание чувствительной информации об ОКИИ (проектная, конструкторская и эксплуатационная документация, способах и средствах по обеспечению безопасности). Обладает специальными знаниями по реализации угроз безопасности, по выявлению и эксплуатации новых уязвимостей	

№	Категория нарушителя	Потенциал нарушителя	Оснащенность	Знания	Мотивация
4	Внутренний	Низкий	Общедоступные программные (программно-аппаратные) средства	Слабая осведомленность о мерах защиты о мерах защиты	
5	Внутренний	Средний	Общедоступные программные (программно-аппаратные) средства, специализированные программные (программно-аппаратные) средства	Знание о структуре ОКИИ, системе безопасности ОКИИ. Обладает специальными знаниями по реализации угроз безопасности.	
6	Внутренний	Высокий	Общедоступные программные (программно-аппаратные) средства, специализированные программные (программно-аппаратные) средства, средства изготовленные на заказ	Знание чувствительной информации об ОКИИ (проектная, конструкторская и эксплуатационная документация, способах и средствах по обеспечению безопасности). Обладает специальными знаниями по реализации угроз безопасности, по выявлению и эксплуатации новых уязвимостей	

Приложение 5
к Методическим рекомендациям
Угрозы информационной
безопасности и сценарии
компьютерных атак

Угрозы безопасности информации и типы компьютерных инцидентов

Актив организации	Тип компьютерного инцидента	Угрозы безопасности информации
Защищаемая информация, обрабатываемая в ИСиР (государственный информационный ресурс, персональные данные и т.д.). Компоненты ИСиР. Конфигурация ИСиР. Настройки технологического процесса. Управляющие команды АСУ	Несанкционированный доступ к данным в ИСиР. Утечка данных (нарушение конфиденциальности). Модификация (подмена) данных. Отказ в обслуживании. Нарушение функционирования технических средств. Несанкционированное использование вычислительных ресурсов ИСиР.	Угрозы создания нештатных режимов работы. Угрозы доступа в операционную среду. Угрозы непосредственного доступа. Сетевые атаки. Угрозы программно-аппаратного воздействия.

Приложение 6
к Методическим рекомендациям
Форма результатов категорирования информационных систем и ресурсов

Результаты категорирования ИСиР

№	Наименование ИСиР	Рекомендуемая категория	Сведения об ИСиР
1		I	
2		III	
3	Наименование	Без категории	Приложение 7

Приложение 7
к Методическим рекомендациям
Форма сведений об объекте информационных систем и ресурсов

Сведения об объекте ИСиР

№	Параметр	Информация (пояснения по заполнению)
Сведения об ИСиР		
1	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	Указывается наименование ИСиР. 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	В случае, если ИСиР является распределённым, указываются адреса подразделений (обособленных подразделений, филиалов, представительств) ОИВ/организации, 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. № 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

№	Параметр	Информация (пояснения по заполнению)
4	Назначение объекта	Указывается задача / цель функционирования объекта, например: управление работой гидроагрегата, ведение единого учета граждан, записывающихся на прием к врачу в медицинских учреждениях г. Москвы, управление и контроль работы нефтеперерабатывающей установки; единый центр управления технологическими процессами обогатительного завода и т. д.
5	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	Указываются тип ИСиР, должен совпадать с типом, указанным в п.1 при наименовании объекта
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	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	Указываются наименования программно-аппаратных средств и их количество: - 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

№	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 ИСиР не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия. ЛВС Организации также должна указываться, если она не входит в состав объекта КИИ и с ней осуществляется какое-либо взаимодействие
11	Наименование оператора связи и (или) провайдера хостинга	Указывается наименование соответственного юридического лица (нескольких лиц, если сетей электросвязи несколько). В случае, если ИСиР 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 ИСиР 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), протоколов взаимодействия	Указывается соответствующая информация о взаимодействии с сетями электросвязи. В случае, если ИСиР не взаимодействует с сетями электросвязи, указываются сведения об отсутствии такого взаимодействия
Сведения об угрозах безопасности информации ИСиР		
14	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации ИСиР	Указываются сведения о потенциальных нарушителях. 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 или обоснование их неактуальности ИСиР	Указываются основные угрозы безопасности информации.

№	Параметр	Информация (пояснения по заполнению)
		В случае отсутствия актуальных угроз безопасности информации приводится обоснование их неактуальности. Актуально при отсутствии потенциальных нарушителей
16	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Указывается общий перечень типов компьютерных инцидентов. В случае отсутствия, приводится обоснование их неактуальности (возможно при отсутствии потенциальных нарушителей)
Сведения об реализованных мерах по обеспечению безопасности ИСиР		
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. № 239
18	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 рассматриваемой ИСиР (наименования средств защиты информации, реквизиты сертификатов соответствия, если есть). Дополнительно рекомендуется указывать средства защиты, используемые на периметре ЛВС ОИВ/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).

№	Параметр	Информация (пояснения по заполнению)
		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. № 239 реализуют указываемые средства защиты, *например*: - *АВЗ.1, АВЗ.2 — средство антивирусной защиты **** Endpoint Security 10, сертификат ИТ.САВЗ.Б2.ПЗ № ***5;* - *СОВ.1, СОВ.2 — **** Security Gateway версии R77.10, сертификат ИТ.СОВ.С4.ПЗ № ****4;* - *ОДТ.4 — резервное копирование защищаемой информации на отказоустойчивой СХД *****.* В случае неприменения средств защиты информации приводятся сведения об отсутствии средств защиты информации
Сведения о рекомендуемой к присвоению ИСиР категории значимости		
19	Категория значимости рекомендуемая	Указываются категория значимости либо информация о неприсвоении объекту ни одной из таких категорий
20	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	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. *Пример:* 1. *Причинение ущерба жизни и здоровью людей — более 50, но менее или равно 500 (II категория);* 2. *Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений* *а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения — нарушение функционирования объекта не оказывает влияние на нарушение объектов обеспечения жизнедеятельности населения — категория не присвоена;* *б) по количеству людей, условия жизнедеятельности которых могут быть нарушены — нарушение функционирования объекта не оказывает влияние на нарушение*

№	Параметр	Информация (пояснения по заполнению)
		объектов обеспечения жизнедеятельности населения — категория не присвоена
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	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта) и Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Указывается 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. № 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
к Методическим рекомендациям
Форма акта категорирования ИСиР

АКТ
категорирования объекта критической информационной инфраструктуры «Информационная система «Полное наименование системы»

Настоящий акт составлен комиссией, созданной на основании распоряжения Департамента информационных технологий города Москвы от 13.09.2018 № 64-16-309/18 «О создании комиссии по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры» в целях принятия решений Департаментом информационных технологий города Москвы (далее – Департамент) об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании городу Москве в лице Департамента, Департаменту (далее – ИСиР Департамента) к объектам критической информационной инфраструктуры, включению объектов критической информационной инфраструктуры в Перечень объектов критической информационной инфраструктуры Департамента (далее – Перечень объектов), 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».

Определение категории значимости информационной системы «Полное наименование системы» проводилось в соответствии с постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации».

Комиссия решила: отсутствует необходимость присвоения одной из категорий значимости объекту критической информационной инфраструктуры «информационная система «Полное наименование системы».

Сведения об объекте критической информационной инфраструктуры информационная система «Полное наименование системы», результаты анализа оценки в соответствии с перечнем показателей критериев значимости масштаб

возможных последствий в случае возникновения компьютерных инцидентов и определения значения каждого из показателей критериев значимости, обоснование их неприменимости приведены в приложении.

Настоящий Акт составлен в единственном экземпляре.

Приложение к Акту категорирования объекта критической информационной инфраструктуры «Информационная система «Полное наименование системы»

Сведения об объекте критической информационной инфраструктуры «Информационная система «Полное наименование системы», результаты анализа оценки в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов и определения значения каждого из показателей критериев значимости, обоснование их неприменимости

Заполняется в соответствии с Приложениями 3-5, 7 к данным Методическим рекомендациям.

Приложение 9
к Методическим рекомендациям
Форма сведений о результатах
категорирования ИСиР

Сведения о результатах присвоения объекту критической информационной инфраструктуры «Информационная система «Полное наименование системы» одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	информационная система «Полное наименование системы»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	1070** Москва, *** пер.12
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Связь
1.4.	Назначение объекта	Мониторинг параметров услуг связи
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	Информационная система
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Одноранговая сеть

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	Департамент информационных технологий города Москвы
2.2.	Адрес местонахождения субъекта	107078, город Москва ул, Басманная Новая, 10-1
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Министр Правительства Москвы, руководитель Департамента информационных технологий города Москвы
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	Начальник подразделения Z , ФИО
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Подразделение Z, начальник ФИО, (495)********, *****@mos.ru
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	7710878000

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

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при	Выделенная

	помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2.	Наименование оператора связи и (или) провайдера хостинга	АО «ФФФ»
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Контроль параметров услуг связи
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Проводной, протоколы стэка TCP/IP

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	Государственное казенное учреждение «Мос…м»
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	1070** Москва, *** пер.12
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	ЦОД
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	7710878***

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

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	АРМ «Наименование» - 50 шт.
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	ОС «Наименование»
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	ПО «Мониторинг»
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	Антивирусное ПО «Наименование», сертификат соответствия…

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

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Внешние и внутренние, оснащенные в том числе специализированными средствами, с достаточной мотивацией для реализации угроз безопасности информации. Угрозы создания нештатных режимов работы. Сетевые атаки. Угрозы программно-математического воздействия.
6.2.	Основные угрозы безопасности информации или обоснование их	

	неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Несанкционированный доступ к данным. Утечка данных (нарушение конфиденциальности). Модификация (подмена) данных. Нарушение функционирования технических средств. Несанкционированное использование вычислительных ресурсов объекта Реализация угроз может привести к прекращению или нарушению функционирования ИСиР.

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	Необходимость присвоения категории значимости отсутствует
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Показатели не применимы
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	
8.3.1	Причинение ущерба жизни и здоровью людей	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, влияющих на жизнь и здоровье людей
8.3.2	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, обеспечивающих функционирование

		объектов обеспечения жизнедеятельности населения
8.3.3	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС, обеспечивающих функционирование объектов транспортной инфраструктуры
8.3.4	Прекращение или нарушение функционирования сети связи	ИС «Краткое наименование системы» система мониторинга, не влияющая на прекращение или нарушение функционирования контролируемой сети связи
8.3.5	Отсутствие доступа к государственной услуге	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на доступность государственных услуг
8.3.6	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования государственного органа
8.3.7	Нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая соблюдение условий международных договоров РФ
8.3.8	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного	Не применимо для Департамента, как ОИВ субъекта Федерации

	за прошедший 5-летний период)	
8.3.9	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период)	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на выплаты в бюджет РФ
8.3.10	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	ИС «Краткое наименование системы» не обеспечивает проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций. ДИТ города Москвы не является 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
8.3.11	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 атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия)	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не оказывающая какие-либо воздействия на окружающую среду. Управление объектами, способными оказать негативное воздействие на окружающую среду.
8.3.12	Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не

	управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра	влияющая на прекращение или нарушение функционирования пунктов управления.
8.3.13	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры	Не применимо для Департамента, как ОИВ субъекта Федерации
8.3.14	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	ИС «Краткое наименование системы» система мониторинга оказания телекоммуникационных услуг, не влияющая на прекращение или нарушение функционирования ИС в области обеспечения обороны страны, безопасности государства и правопорядка

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

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установлена контролируемая зона. Обеспечен контроль физического доступа к объекту. Утвержден комплект документов по обеспечению безопасности объекта, соответствующий требованиям 17 приказа ФСТЭК России к ГИС класса К3. Объект КИИ не является значимым – обязательных мер не установлено.
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Антивирусная защита (АВЗ) Объект КИИ не является значимым – обязательных мер не установлено.