Техническое заданием

на оказание услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования системы мониторинга инженерных конструкций мостового перехода «Фрунзенский» через реку Самару с выходом на автомобильную дорогу «Автодорожный маршрут “Центр-Поволжье-Урал” г.о. Самара. 1 этап (очередь)» и мостового перехода «Кировский» через реку Самару

Сокращение	**Обозначение**
СМИК	Система мониторинга инженерных конструкций (СМИК) мостового перехода «Фрунзенский» через реку Самару с выходом на автомобильную дорогу «Автодорожный маршрут “Центр-Поволжье-Урал” г.о. Самара. 1 этап (очередь)» и мостового перехода «Кировский» через реку Самару.
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ПО	Программное обеспечение
Категорирование	Обследование и определение категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования
КИИ	Критическая информационная инфраструктура
ОКИИ	Объект критической информационной инфраструктуры
ИС	Информационная система
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления технологическим процессом
МУБИ	Модель угроз безопасности информации
НПА	Нормативно-правовой акт
АРМ	Автоматизированное рабочее место
ЭВМ	Электронная вычислительная машина
Заказчик	ПАО «Ростелеком»
Государственный заказчик	Министерство транспорта и автомобильных дорог Самарской области

В рамках настоящего технического задания Исполнитель выполняет обследование и определение категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК.

1. СРОКИ ОКАЗАНИЯ УСЛУГ.

1.1. Услугу по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологическому сопровождению процедуры категорирования СМИК Исполнитель производит однократно в период с даты заключения договора до 15.07.2026г.

2. ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ.

2.1. Для оказания услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического

сопровождения процедуры категорирования СМИК Исполнитель, либо соисполнителя организация, должны иметь:

– Лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, в т.ч., выполнению работ и оказанию следующих услуг, предусмотренных п. 4 «Положения о лицензировании деятельности по технической защите конфиденциальной информации», утвержденного Постановлением Правительства РФ от 03.02.2012 №79:

– а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

– в средствах и системах информатизации;

– в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

– в помещениях со средствами (системами), подлежащими защите;

– в помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

– б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– в) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации:

– средств и систем информатизации;

– помещений со средствами (системами) информатизации, подлежащими защите;

– защищаемых помещений;

– д) работы и услуги по проектированию в защищенном исполнении:

– средств и систем информатизации;

– помещений со средствами (системами) информатизации, подлежащими защите;

– Лицензия ФСБ на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

2.2. В период оказания услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК и после их окончания Исполнитель (соисполнитель) не должен разглашать и использовать информацию, которая может стать ему известной в ходе оказания услуг. Исполнитель (соисполнитель) несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

2.3. Отправка сообщений, запросов в адрес Заказчика, содержащих информацию о Заказчике в части информационной безопасности, результатов оказания услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК, допускается только с использованием почтового отправления с курьерской доставкой.

2.4. По факту окончания оказания услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК и передачи результата услуг Исполнитель направляет в адрес Заказчика АКТ об уничтожении информации, полученной от Заказчика в ходе оказания услуг в области информационной безопасности, а также результатов оказания услуг, с направлением распорядительного документа Исполнителя, о назначении ответственного лица за уничтожение информации в рамках данного Договора.

3. ТРЕБОВАНИЕ БЕЗОПАСНОСТИ.

3.1. При оказании услуг персонал Исполнителя обязан соблюдать и обеспечивать соблюдение требования техники безопасности, экологической безопасности оказываемых услуг, действующих норм пожарной и электробезопасности, охраны труда, в том числе работы на высоте, пребывания на проезжей части и др.

3.2. В течение 10 (десяти) дней с даты подписания контракта Исполнитель предоставляет исчерпывающий перечень лиц, планируемых к допуску в зону транспортной безопасности по форме, предоставляемой Заказчиком.

4. ПОРЯДОК ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ИЗДЕЛИЯ.

4.1. Все оказываемые услуги должны производиться после ознакомления обслуживающего персонала с Рабочей документацией шифра:

- ПИР-87-3-33-15-СМ-СМИК-Э для м.п. «Фрунзенский»;
- 0607/25/1651/24-СМ – для м.п. «Кировский».

5. КАТЕГОРИРОВАНИЕ СМИК

5.1. Основанием для оказания услуг является Федеральный закон от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5.2. Исчерпывающий перечень оборудования СМИК, программно-аппаратная составляющая и данные о сетевом взаимодействии передаются Исполнителю после заключения Договора. Состав оборудования СМИК указан в п. 4 и п. 5 настоящего Задания.

5.3. Места расположения оборудования СМИК указаны в таблице № 1.

Таблица № 1

№	Элемент системы	Место расположения
1	Сервер СМИК	в границах г.о. Тольятти
2	АРМ оператора СМИК	в границах г.о. Самара
3	Абсолютный линейный энкодер (тензометр)	в границах г.о. Самара
4	Измеритель угла наклона цифровой (инклинометр) типа IND3	в границах г.о. Самара
5	Струнный датчик деформации (тензометр) SVWG-D01	в границах г.о. Самара
6	ГНСС приемник EFT M1 Plus	в границах г.о. Самара

7	Датчик комплексный параметров атмосферы IWS-2	в границах г.о. Самара
8	Датчик состояния поверхности дорожного полотна	в границах г.о. Самара

5.4. Состав услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК указан в Таблице № 2.

Таблица № 2

№ п/п	Наименование услуг	Документы по результатам оказанных услуг
1	Обследование (аудит) СМИК	- Отчет об аудите
2	Разработка модели угроз безопасности информации (МУБИ) на СМИК.	- Проект МУБИ на СМИК; - Заключение с рекомендациями по повышению информационной безопасности СМИК
3	Организационно-методологическое сопровождение категорирования объекта критической информационной инфраструктуры	– Проект Перечня критических процессов; – Проект Перечня объектов КИИ, подлежащих категорированию; – Проект акта о категорировании объекта КИИ; - Проект Сведений о результатах присвоения объекту КИИ одной из категории значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий

5.5. Сбор сведений выполняется очно, с выездом специалистов Исполнителя на адреса расположения элементов СМИК, осуществляется в формате интервьюирования ответственных специалистов, а также в результате натурных обследований СМИК.

5.6. Интервьюируемые специалисты Заказчика, Государственного заказчика обеспечивают актуальность, достоверность и полноту предоставляемой Исполнителю информации.

6. ТРЕБОВАНИЯ К ОБЪЕМУ ОКАЗЫВАЕМЫХ УСЛУГ ПО КАТЕГОРИРОВАНИЮ

6.1. Оказание услуг включает в себя следующие мероприятия:

6.1.1. Обследование (аудит) систем и сервисов, эксплуатируемых Государственным Заказчиком, и выявление объектов КИИ.

Обследование (аудит) систем и сервисов проводится с учетом требований нормативных и методических документов, на основании которых должен быть оказан комплекс услуг, указанных в разделе 7 настоящего ТЗ, и включает в себя:

- сбор сведений о СМИК (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими системами и сервисами, наличие и характеристики доступа к сетям связи);

- сбор сведений о распорядительных документах в области обеспечения информационной безопасности;

- выявление объектов КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности Государственного заказчика;

- определение состава информации, обрабатываемой СМИК;

- сбор сведений о взаимодействии СМИК с другими объектами КИИ и (или) о зависимости функционирования СМИК от других таких объектов;

- определение угроз безопасности информации в отношении СМИК, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на схожих объектах;

- определение соответствия объекта КИИ перечням типовых отраслевых объектов КИИ.

Результатом оказания услуги является направленный на утверждение Заказчику Отчет об аудите, содержащий следующие сведения:

– перечень выявленных критических процессов;

– перечень выявленных объектов КИИ;

– перечень ИС, АС, АСУ ТП субъекта КИИ;

– перечень объектов КИИ подлежащих категорированию и отчет по порядку определения перечня ОКИИ подлежащих категорированию;

– сведения об объектах КИИ, подлежащих категорированию, в том числе:

а) наименования, места (адреса) размещения, сферы (области) деятельности и назначение;

б) архитектура объекта КИИ;

в) применяемые программные и программно-аппаратные средства;

– сведения о взаимодействии (наличие и порядок) объектов КИИ с другими объектами КИИ;

– сведения о наличии и характеристиках доступа к сетям связи, в том числе сведений о взаимодействии СМИК, и сетей электросвязи, наименованиях сетей электросвязи и способах взаимодействия;

– сведения о мерах и средствах, используемых для обеспечения безопасности СМИК, в том числе организационных и технических мерах;

– сведения о применяемых Государственным заказчиком средствах защиты информации.

6.1.2. Разработка Модели угроз безопасности информации с учетом требований нормативных и методических документов, указанных в разделе 7 настоящего ТЗ.

При разработке модели угроз выполняются следующие мероприятия:

- инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

- определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

- оценка способов реализации (возникновения) угроз безопасности информации;

- оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

- оценка сценариев реализации угроз безопасности информации в системах и сетях ОКИИ.

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

Результатом оказания услуги должна являться Модель угроз безопасности информации Государственного заказчика, которая содержит краткое описание архитектуры объекта КИИ, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для объекта КИИ Государственного

заказчика, а так же Заключение с рекомендациями по повышению общесистемной информационной безопасности СМИК.

6.1.3. Организационно-методологическое сопровождение процедуры категорирования объектов КИИ.

В ходе работы по категорированию объекта КИИ проводится:

– выявление критических процессов объекта КИИ Государственного заказчика;

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

– подготовка предложения для включения выявленных ИС, АС, АСУ ТП в перечень объектов КИИ;

– рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иные источники угроз безопасности информации;

– анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;

– оценка в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ, определение значения каждого из показателей критериев значимости или обоснование их неприменимости;

– присвоение каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категорий значимости.

Результатом оказания услуги является направленные на утверждение Заказчику проекты актов категорирования объектов КИИ, содержащие следующие сведения:

– сведения об объекте КИИ (наименование объекта, адреса размещения объекта, сфера (область) деятельности, в которой функционирует объект, назначение объекта, критические процессы, которые обеспечиваются объектом, архитектура объекта);

– сведения о субъекте КИИ;

– сведения о взаимодействии каждого отдельного объекта КИИ и сетей электросвязи;

– сведения о лице, эксплуатирующем объект КИИ;

– сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ;

– сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ;

– возможные последствия в случае возникновения компьютерных инцидентов;

– категория значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;

– организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ.

7. ПЕРЕЧЕНЬ НОРМАТИВНО-ПРАВОВЫХ ДОКУМЕНТОВ

7.1. Исполнитель при оказании услуг по обследованию и определению категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК должен обеспечивать

соблюдение следующих федеральных законов, постановлений Правительства Российской Федерации и нормативных актов:

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

– Указ Президента Российской Федерации от 01.05.2022 г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Постановление Правительства РФ от 08.02.2018 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»;

– Приказ ФСТЭК России от 22.12.2017 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»;

– Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта, утвержденный заместителем Министра транспорта Российской Федерации Д.В. Бакановым 15.05.2023г. и согласованный заместителем директора ФСТЭК России В.С. Лютиковым 05.05.2023 г.;

– Другие действующие на территории Российской Федерации НПА в области оказания услуги в соответствии с настоящим ТЗ.

8. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

8.1. Требования к гарантийным обязательствам в отношении обследования и определения категории значимости объекта критической информационной инфраструктуры и организационно-методологического сопровождения процедуры категорирования СМИК:

8.1.1. Срок гарантийных обязательств, в течение которого Исполнитель обеспечивает устранение недостатков результатов оказания услуги, составляет 24 месяца с даты подписания Акта о приемке оказанных услуг. Срок устранения выявленных гарантийных недостатков определяется Заказчиком, но составляет не менее 5 (пяти) рабочих дней.

8.1.2. В случае изменения НПА, регламентирующих отношения в сфере обеспечения информационной безопасности объектов критической информационный инфраструктуры, в процессе оказания услуги Исполнитель обязан привести результат работ в соответствие с новыми требованиями с учетом требований действующего законодательства. В случае выведения из действия ГОСТ, ФЗ, Приказов и т.п. нормативных документов на основаниях, предусмотренных законодательством Российской Федерации, актуальным документом считается официально его заменяющий.

8.1.3. В случае изменений состава объекта КИИ, правового статуса Заказчика, и прочих изменений в период исполнения контракта, либо в течении срока действия гарантийных обязательств, Исполнитель обязан привести результат работ к фактическому состоянию объекта КИИ.