**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на выполнение работ по**

категорированию объектов критической информационной инфраструктуры Фонда социального страхования Российской Федерации

1. Полное наименование работ

Выполнение работ по категорированию объектов критической информационной инфраструктуры Фонда социального страхования Российской Федерации.

2. Заказчик

Фонд социального страхования Российской Федерации.

3. Основание для выполнения работ

Основанием для выполнения работ являются:

* Федеральный закон от 26 июля 2017 г. № 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»;
* 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»;
* иные нормативные правовые акты Президента Российской Федерации, Правительства Российской Федерации, ФСТЭК России и ФСБ России, выпущенные в рамках их полномочий по регулированию сфер защиты информации и обеспечения безопасности критической информационной инфраструктуры.

4. Плановые сроки начала и окончания работ

Срок начала работ – дата заключения контракта.

Срок окончания работ – не позднее 02 декабря 2019 года.

Плановые сроки начала и окончания работ приведены в разделе 12 настоящего Технического задания.

5. Перечень используемых терминов и определений

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

**Безопасность критической информационной инфраструктуры** – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

**Значимый объект критической информационной инфраструктуры** – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

**Информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Исполнитель** – организация, выбранная Заказчиком на основании результатов запроса предложений для выполнения работ, предусмотренных настоящим Техническим заданием.

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

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

**Критическая информационная инфраструктура** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Субъекты критической информационной инфраструктуры** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

**ФСС, Фонд, Заказчик**  – Фонд социального страхования Российской Федерации.

6. Общие сведения

Фонд социального страхования Российской Федерации (Фонд, Заказчик) управляет средствами государственного социального страхования Российской Федерации.

Фонд является специализированным финансово-кредитным учреждением при Правительстве Российской Федерации.

Фонд осуществляет свою деятельность в соответствии с законодательством Российской Федерации, в том числе в соответствии с Положением о Фонде социального страхования Российской Федерации, утвержденным Постановлением Правительства Российской Федерации от 12 февраля 1994 г. № 101 «О Фонде социального страхования Российской Федерации».

Автоматизация процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности Заказчика в основном реализована в Федеральной государственной информационной системе Единая интегрированная информационная система «Соцстрах» (ЕИИС «Соцстрах»), сведения о которой опубликованы в Федеральной государственной информационной системе координации информатизации по адресу <https://portal.eskigov.ru/fgis/104>. Основные вычислительные мощности ЕИИС «Соцстрах» расположены в центральном аппарате Фонда и центрае обработки данных в г. Москва. Пользователями ЕИИС «Соцстрах» являются сотрудники Фонда, его региональных отделений, филиалов, центров реабилитации и подведомственных учреждений, а также внешие пользователи, включая страхователей и получателей социальных услуг.

Заказчик является владельцем и оператором иных, помимо ЕИИС «Соцстрах», информационных (автоматизированных) систем, включая Комплексную автоматизированную систему Административно-хозяйственной деятельности, систему электронного документооборота, Удостоверяющий центр Фонда социального страхования Российской Федерации.

Дополнительные общие сведения о деятельности Фонда опубликованы по адресу <http://fss.ru/>.

7. Цель и задачи выполнения работ

Основной целью выполнения работ является категорирование объектов критической информационной инфраструктуры (далее - КИИ) Заказчика, являющегося субъектом КИИ.

В ходе выполнения работ должны быть решены следующие задачи:

* определение перечня объектов КИИ и предоставление его в ФСТЭК России;
* категорирование объектов КИИ;
* предоставление в ФСТЭК России сведений о результатах категорирования объектов КИИ;
* подтверждение ФСТЭК России сведений о результатах категорирования объектов КИИ.

8. Требования к составу и содержанию работ

Для решения достижени поставленной цели быть решены следующие задачи:

* формирование перечня процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности Заказчика, субъекта КИИ;
* выявление критических процессов Заказчика, т.е. процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка, выраженным в показателях критериев значимости;
* формирование перечня объектов КИИ Заказчика, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, формирование перечня объектов КИИ, подлежащих категорированию;
* рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации;
* анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ;
* оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ;
* категорирование объектов КИИ;
* подготовка проектов документов для предоставления в ФСТЭК России сведений о результатах категорирования объектов КИИ.

Перечень работ, которые должны быть выполнены для решения указанных задач:

* анкетирование ответственных лиц Заказчика об управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности Заказчика;
* анализ полученной информации о процессах Заказчика с целью:
  + выявления критических процессов Заказчика;
  + формирования перечня объектов КИИ, подлежащих категорированию;
* формирование перечня процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности Заказчика;
* формирование перечня процессов с учетом сведений о критичности процессов субъекта КИИ;
* определение перечня объектов КИИ Заказчика, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
* формирование перечня объектов КИИ, подлежащих категорированию;
* разработка проекта приказа о создании Комиссии по категорированию объектов КИИ;
* сбор информации об объектах КИИ Заказчика с целью:
  + определения состава реализованных организационных и технических мер защиты информации;
  + определения мест и способов хранения, обработки, передачи и уничтожения информации;
  + уточнения информации о размещении, архитектуре и структуре объекта КИИ;
* обследование действующих процессов и процедур обеспечения информационной безопасности объектов КИИ;
* определение акутальных угроз и нарушителей безопасности объектов КИИ;
* категорирование объектов КИИ (с участием членов Комиссии по категорированию);
* разработка проектов Актов категорирования для каждого объекта КИИ;
* подготовка сведений о результатах категорирования, по форме, определенной ФСТЭК России;
* устранение замечаний ФСТЭК России к сведениям о результатах категорирования (при наличии).

По результатам выполнения работ Заказчику должны быть предоставлены документы, перечень которых приведен в разделе 9 настоящего Технического задания.

9. Состав документации, предъявляемой по окончании работ

По результатам выполнения работ должны быть разработаны следующие документы:

* «Проект Приказа о создании Комиссии по категорированию объектов КИИ»;
* «Перечень критических процессов Заказчика»;
* «Перечень объектов КИИ, подлежащих категорированию».
* «Отчет об обследовании объектов КИИ Заказчика, подлежащих категорированию», содержащий:
  + сведения об объектах КИИ Заказчика (включая их наименования, места размещения, область деятельности, назначение, связанные критические процессы, информацию об архитектуре и составе объектов КИИ, а также прочие сведения, состав которых определен требованиями ФСТЭК России);
  + сведения о взаимодействии объектов КИИ между собой и с сетями электросвязи;
  + сведения о действующих процессах и процедурах обеспечения безопасности объектов КИИ, о реализованных организационных и технических мерах защиты информации;
* «Модель угроз и нарушителей безопасности объекта КИИ», для объектов КИИ Заказчика;
* Проект «Акта категорирования объекта КИИ», для каждого объекта КИИ Заказчика;
* Сведения о результатах категорирования объектов КИИ Заказчика, представленные по форме, определенной ФСТЭК России.

Состав и содержание отчетных документов могут быть изменены по согласованию Заказчика и Исполнителя.

Отчетные документы предоставляются Заказчику в электронном виде в формате приложений Microsoft Office и на бумажном носителе.

10. Порядок контроля и приемки работ

Приемка работ осуществляется на основании предоставляемых Заказчику документов согласно разделу 9 настоящего Технического задания.

Замечания направляются по электронной почте Исполнителю не позднее 10 рабочих дней после предоставления итоговой версии отчетных документов.

11. Требования к квалификации

Требования к квалификации Исполнителя:

* наличие у Исполнителя лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации;
* наличие у Исполнителя лицензии ФСБ России 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).

12. Календарный план

| Этап | Наименование этапа | Срок выполнения работ | Отчетные материалы |
| --- | --- | --- | --- |
| 1 | Проведение категорирования объектов КИИ | Не позднее 02 декабря 2019 года | * Проект Приказа о создании Комиссии по категорированию объектов КИИ * Перечень критических процессов Заказчика * Перечень объектов КИИ, подлежащих категорированию * Отчет об обследовании объектов КИИ Заказчика, подлежащих категорированию * Модель угроз и нарушителей безопасности объектов КИИ * Проекты Актов категорирования объектов КИИ * Сведения о результатах категорирования объектов КИИ Заказчика, представленные по форме, определенной ФСТЭК России |