СОГЛАСОВАНО
Заместитель генерального директора по безопасности ПАО «МРСК Волги»

_____ В.Б. Пономарев
«30» 04 2018 г.

УТВЕРЖДАЮ
Заместитель генерального директора - главный инженер ПАО «МРСК Волги»

_____ О.Г. Павлов
«30» 04 2018 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на выполнение
научно-исследовательских работ и технологических работ (НИРиТР)

«Разработка мероприятий по обеспечению кибербезопасности вновь строящихся и реконструируемых цифровых подстанций. Разработка функциональных требований безопасности, требований доверия к безопасности для цифровых подстанций»

2018 год

Используемые сокращения:

АРМ – Автоматизированное рабочее место;
АПКШ – Аппаратно-программный комплекс шифрования;
АСДУ – Автоматизированная система диспетчерского управления;
АСТУ – Автоматизированная система технологического управления;
АСУ ТП – Автоматизированная система управления технологическими процессами;
АУ – Аппарат управления,
ДА – Детектор атак;
ИБ – Информационная безопасность;
ИА – Исполнительный аппарат;
ИТ – Информационные технологии;
КИИ – Критическая информационная инфраструктура;
КСОиУИБ – Комплексная система обеспечения и управления информационной безопасностью электросетевого комплекса;
КП- Критический процесс;
МЭ – Межсетевой экран;
НИРиТР – Научно-исследовательские и технологические работы;
ОКИИ (объект критической информационной инфраструктуры) – Информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления субъекта критической информационной инфраструктуры;
ОРД – Организационно-распорядительные документы;
ОТР – Основные технические решения;
ПАО «МРСК Волги», Общество – Публичное акционерное общество «Межрегиональная распределительная сетевая компания Волги»;
ПС – Электрическая подстанция;
ПТК – Производственно-технологический комплекс;
РЗАиПА – Релейная защита и противоаварийная автоматика;
РП – Распределительная электрическая подстанция;
РЭС – Район электрических сетей;
СЗИ – Средства защиты информации;
СКЗИ – Средство криптографической защиты информации;
СОИБ – Средства обеспечения информационной безопасности;
ТЗ – Техническое задание;
ТСП – Технологическая сеть передачи данных;
ТП – Технологический процесс;
ФСБ России – Федеральная служба безопасности Российской Федерации;
ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации;
ЦОД – Центр обработки данных;
ЦУС – Центр управления сетью;
CD – Compact Disc;
DVD – Digital Versatile Disc;
USB – Universal Serial Bus.

1. Основание для проведения работ

1.1. Программа инновационного развития ПАО «МРСК Волги» на 2016 – 2020 гг. с перспективой до 2025 года, утвержденная решением СД Общества (Протокол № 28 заседания СД Общества от 03.04.2017).

1.2. Программа научно-исследовательских, опытно-конструкторских и технологических работ (Программа НИОКР) ПАО «МРСК Волги».

2. Название проводимых работ

2.1 Выполнение научно-исследовательских и технологических работ (далее – **НИРиТР**) по теме **«Разработка мероприятий по обеспечению кибербезопасности вновь строящихся и реконструируемых цифровых подстанций. Разработка функциональных требований безопасности, требований доверия к безопасности для цифровых подстанций»**.

2.2 В рамках работы разрабатывается комплекс организационно-технических мероприятий по обеспечению выполнения требований законодательства Российской Федерации, определяющих порядок обеспечения безопасности объектов критической информационной инфраструктуры (далее – ОКИИ) Заказчика (включаемых в их состав новых объектов защиты) на этапе их проектирования, нового строительства и реконструкции (включая подстанции, в том числе подстанций выполненных с применением элементов и по технологиям «цифровых подстанций», и сопутствующих систем для сбора и передачи информации на вышестоящий уровень) (далее – электросетевых объектов), и обрабатываемой на них защищаемой законом информации.

2.3 Заказчиком настоящих работ является ПАО «МРСК Волги» (далее – **Заказчик**).

3. Срок исполнения работ

3.1. Начало разработки: **со дня заключения договора.**

3.2. Окончание разработки: **31.10.2020 г.**

4. Цель работ

4.1. Разработка мероприятий по обеспечению кибербезопасности электросетевых объектов, в том числе:

– **Разработка модели угроз безопасности информации для инфраструктуры электросетевых объектов:** разработка критериев оценки отнесения электросетевых объектов к критической информационной инфраструктуры (далее – КИИ) Заказчика (в том числе, включения их в существующие объекты КИИ), разработка методики определения уровня значимости объектов КИИ, проведение обследования инфраструктуры типовых объектов КИИ Заказчика, в которые предполагается включения новых объектов защиты, определение угроз информационной безопасности, вносимых в существующие объекты КИИ при введении новых объектов защиты, разработка модели угроз безопасности информации для типовых объектов КИИ;

– **Разработка требований к системе защиты информации для технологического сегмента критической инфраструктуры Заказчика:** разработка типовых технических решений и типовой архитектуры по обеспечению информационной безопасности технологического сегмента КИИ Заказчика, разработка технического задания на создание (модернизацию, реконструкцию) комплексной системы защиты КИИ Заказчика, разработка Стандартов организации по обеспечению кибербезопасности технологического сегмента КИИ Заказчика, разработка плана мероприятий (дорожной карты) по оптимизации инфраструктуры электросетевых объектов с точки зрения обеспечения эффективной защиты их от киберугроз, описание комплекса технических средств и организационных мер информационной защиты.

4.2. Работа выполняется с целью реализации требований законодательства Российской Федерации в области защиты информации, снижения рисков возникновения аварийных и нештатных ситуаций, связанных с киберугрозами и, как следствие, повышение уровня надёжности функционирования инфраструктуры объектов электроэнергетики.

5. Актуальность и область применения результатов работ

5.1. Передовые технологий при строительстве и реконструкции объектов электроэнергетики, позволяют электросетевым компаниям обеспечивать высокую доступность и надежность оказываемых услуг. В то же время, особенности применения информационных технологий, могут повлечь за собой реализацию различных угроз, в том числе и киберугроз безопасности для деятельности электросетевых компаний.

5.2. В качестве предпосылок для формирования киберугроз объектов электроэнергетики, могут служить:

– разнородность и сложность инфраструктуры, связанная с применением оборудования и программного обеспечения различного происхождения (в том числе отечественного и иностранного);

– территориальная разрозненность объектов, взаимодействие между которыми осуществляется посредством каналов связи общего пользования;

– человеческий фактор, который может привести к ошибкам при настройке и эксплуатации высокотехнологичных и сложных элементов информационной инфраструктуры.

5.3. В общем случае, в качестве киберугроз может рассматриваться потенциально любое несанкционированное/нештатное воздействие на информационную инфраструктуру электросетевого объекта, в результате которого может быть нарушено/прекращено штатное функционирование, как отдельных элементов инфраструктуры электросетевых компаний, так и всей инфраструктуры в целом.

5.4. В силу того, что электросетевые компаний является связующим звеном между различными секторами экономики и социальной сферы Российской Федерации, ущерб от реализации киберугроз может привести к катастрофическим последствиям для отрасли и страны в целом.

5.5. К реализации потенциальных угроз могут привести:

– невыполнение требований законодательства Российской Федерации;

– некорректные настройки оборудования и программного обеспечения;

– уязвимости программного обеспечения и технических средств;

– ошибки обслуживающего персонала;

– несовершенство выстроенной архитектуры объектов КИИ;

– использование устаревшего оборудования и технологий;

– отсутствие регулярных мер по оценке и постоянного совершенствования уровня защищенности инфраструктуры.

Всё перечисленное может способствовать возникновению условий для реализации потенциальных кибератак (в том числе целенаправленных) на инфраструктуру объектов.

5.6. В превентивных целях, следует на постоянной основе принимать самые разные организационные и технические меры, направленные на создание, оценку и поддержание требуемого уровня защищенности инфраструктуры объектов. Принятие соответствующих мер позволит снизить риски возникновения потенциальных киберугроз и реализации кибератак на критическую информационную инфраструктуру, что в свою очередь снижает вероятность возникновения катастрофических последствий, связанных с такими угрозами и атаками.

5.7. Технические и организационные меры должны соответствовать положениям и требованиям нормативных документов, в частности должны применяться:

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;

- Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ;
- Федеральный закон от 21.07.2011 № 256-ФЗ (ред. от 06.07.2016) «О безопасности объектов топливно-энергетического комплекса»;
- Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства Российской Федерации от 08 февраля 2018 г. № 127-П «Об утверждении показателей критериев значимости объектов КИИ РФ и их значений, а также порядка и сроков осуществления их категорирования»;
- Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
- «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007).
- РД. «Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период» (утв. ФСТЭК России 23.04.2011).
- РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации (Гостехкомиссия России, 1992).
- РД. СВТ. СВТ. Защита от несанкционированного доступа к информации
- Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1992).
- РД. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации (Гостехкомиссия России, 1997).
- Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении Требований к системам обнаружения вторжений».
- Приказ ФСТЭК РФ от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении Требований к средствам антивирусной защиты».
- Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 14 марта 2014 г № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
- Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА, № 149/2/7-200 от 27.12.2016 г.

– Временный порядок включения корпоративных центров в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, № 149/2/7-240 от 15.04.2017 г.

– Концепция обеспечения информационной безопасности ПАО «Россети», утверждена распоряжением ПАО «Россети» от 07.02.2018 №45.

5.8. Так же могут учитываться требования, изложенные в проектах нормативных актов:

– Проект приказа ФСТЭК России «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»;

– Проект приказа ФСБ России «Об утверждении порядка реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак на значимых объектах КИИ РФ»;

– Проект приказа ФСБ России «Об утверждении перечня сведений, предоставляемых в ГосСОПКА, и порядка их предоставления»;

– Проект приказа ФСБ России «Об утверждении порядка доступа к информации, содержащейся в ГосСОПКА»;

– Проект приказа ФСБ России «Об утверждении требований к техническим средствам ГосСОПКА»;

– Проект приказа ФСБ России «Об утверждении технических условий установки и эксплуатации технических средств ГосСОПКА».

6. Краткое описание результатов работ

6.1. Разработка представляет собой комплекс взаимосвязанных научно-исследовательских и технологических работ, направленных на разработку мероприятий по обеспечению кибербезопасности вновь строящихся и реконструируемых электросетевых объектов, а также уже существующих объектов КИИ, в состав которых они будут входить, включая:

6.1.1. Разработка классификатора электросетевых объектов КИИ по функциональному назначению и всем возможным уровням значимости для каждого класса.

6.1.2. Разработка частных моделей угроз безопасности информации и моделей нарушителя для вновь создаваемых (модернизируемых, реконструируемых) электросетевых объектов.

6.1.3. Разработка методики корректировки модели угроз и нарушителя объекта КИИ с учетом частной модели угроз и нарушителя, включаемого в объект КИИ объекта электроэнергетики;

6.1.4. Разработка технических и функциональных требований безопасности и условий среды функционирования для типовых архитектур объектов КИИ, с учетом специфики информационной инфраструктуры, количественного и качественного состава АСУ, информационных систем и информационно-телекоммуникационных сетей, а также особенностей различных технологических и организационных процессов, связанных с проектированием, внедрением, эксплуатацией объектов КИИ технологического сегмента КИИ Заказчика.

6.1.5. Разработка вариантов построения типовой архитектуры системы защиты объектов КИИ критической информационной инфраструктуры Заказчика, оформленные в виде проектов стандартов организации.

6.1.6. Разработка плана мероприятий (дорожной карты) по приведению технологического сегмента критической информационной инфраструктуры Заказчика в соответствие с требованиями к обеспечению защиты информации.

6.1.7. Разработка методологии периодических анализа и оценки функционирования значимого объекта и его подсистемы безопасности, включая анализ и устранение уязвимостей и иных недостатков в функционировании подсистемы безопасности значимого объекта.

6.1.8. Разработка Стандартов организации (нормативно-технических документов) по обеспечению кибербезопасности технологического сегмента КИИ Заказчика:

- Руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры Цифровой сети.
- Руководящие указания по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики (ИА, Филиал РСК, Дисп. пункт ПО, Дисп. пункт РЭС, ПС 35-220 кВ, РП, ТП 6-20/0,4 кВ).
- Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры (ИА, Филиал РСК, Дисп. пункт ПО, Дисп. пункт РЭС, ПС 35-220 кВ, РП, ТП 6-20/0,4 кВ).
- Руководящие указания по установлению параметров и характеристик программных и программно-аппаратных средств, применяемых для обнаружения компьютерных инцидентов, компьютерных атак на информационную инфраструктуру Цифровой сети.

(Названия разрабатываемых стандартов организации могут быть скорректированы по согласованию с Заказчиком. Порядок оформления стандартов организации согласовывается с заказчиком дополнительно.).

7. Общие требования и технические параметры

7.1. Общие требования:

7.1.1. В рамках выполнения работ необходимо провести НИРиТР по разработке мероприятий по обеспечению кибербезопасности технологического сегмента критической информационной инфраструктуры (КИИ) Заказчика:

7.1.1.1 Разработать модели угроз безопасности информации для технологического сегмента КИИ Заказчика (этап 1), в том числе:

- Исследование особенностей технологического сегмента КИИ Заказчика, в том числе с учетом основных направлений развития электросетевого комплекса.
- Проведение анализа угроз информационной безопасности для технологического сегмента КИИ.
- Разработка методики оценки уровней значимости ОКИИ, включая предложения по типизации ОКИИ в зависимости от функционального назначения и уровня значимости.
- Разработка методологии периодической оценки соответствия инфраструктуры электросетевых объектов требованиям информационной защиты.
- Разработка программы проведения обследования (сбора исходных данных) ОКИИ в технологическом секторе КИИ. Согласование программы проведения обследования с Заказчиком.
- Проведение обследования ОКИИ технологического сегмента Заказчика.
- Построение модели угроз безопасности информации для ОКИИ технологического сегмента.

7.1.1.2 Разработать требования к комплексной системе обеспечения и управления информационной безопасностью КИИ (этап 2), в том числе:

- Разработка перечня технических и организационных мер защиты ОКИИ технологического сегмента.
- Разработка требований к функционалу средств защиты ОКИИ технологического сегмента, нейтрализующих выявленные угрозы.

– Разработка требований к порядку разработки (проектирования) типовой архитектуры комплексной системы обеспечения и управления информационной безопасностью.

– Разработка требований к эксплуатации комплексной системы обеспечения и управления информационной безопасностью.

– Разработка технико-экономического сравнения реализации комплексной системы обеспечения и управления информационной безопасностью.

– Разработка основных технических решений (ОТР) по созданию комплексной системы обеспечения и управления информационной безопасностью.

– Разработка типовых технических решений и типовой архитектуры по обеспечению информационной безопасности технологического сегмента КИИ Заказчика, в том числе для цифровых подстанций с применением оборудования с непосредственным жидкостным охлаждением, позволяющие снизить уровень шума и зависимость от внешних неблагоприятных факторов окружающей среды.

– Разработка рекомендаций по распределению обязанностей и ответственности по обеспечению безопасности между структурными подразделениями Заказчика.

– Разработка рекомендаций по требуемым изменениям функционала и кадрового состава подразделений Заказчика.

– Разработка рекомендаций по квалификационным требованиям к работникам Заказчика для обеспечения функционирования и эксплуатации комплексной системы обеспечения и управления информационной безопасностью.

– Разработка Стандартов организации по обеспечению кибербезопасности технологического сегмента КИИ Заказчика. Рассылка Стандартов на согласование Заказчику. Сбор и анализ замечаний и предложений по Стандартам от Заказчика.

– Свод замечаний и предложений с указанием принятых и отклоненных замечаний, с обоснованием отклонения. Доработка Стандартов по результатам рецензирования. Представление Заказчику итоговых редакций Стандартов.

7.1.1.3 Разработать методику обеспечения всех этапов жизненного цикла объектов защиты и ОКИИ (этап 3), в том числе:

– Разработка программы и методик испытаний средств защиты информации электросетевых объектов.

– Проведение проверки разработанных технических решений и типовой архитектуры на предмет совместимости с ПО ПТК ОКИИ в форме стендовых испытаний.

– Разработка рекомендаций по приемке, вводу и выводу из эксплуатации комплексной системы обеспечения и управления информационной безопасностью.

– Разработка плана мероприятий (дорожной карты) по приведению КИИ технологического сегмента Заказчика в соответствие с требованиями к обеспечению защиты информации.

– Подготовка документов необходимых для защиты интеллектуальной собственности, полученной в ходе выполнения работы, в объеме и в соответствии с требованиями действующего законодательства Российской Федерации.

– Подготовка отчет по НИР в соответствии с ГОСТ 7.32-2001

– Подготовка презентации по теме НИР.

7.1.2 Представить Заказчику результаты работ по НИР в соответствии с условиями настоящего Технического задания.

7.1.3 Перечень работ и отчетных материалов, представляемых Заказчику по итогам выполнения работ, указаны в разделе 9 настоящего Технического задания.

7.2. Технические параметры

7.2.1. Работы по формированию требований к защите инфраструктуры электросетевых объектов должны выполняться с учетом требований законодательных актов, указанных в п.5.7 настоящего ТЗ.

7.2.2. Определение угроз информационной безопасности для технологического сегмента критической информационной инфраструктуры Заказчика, необходимо выполнять согласно следующим требованиям:

- Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее - архитектура значимого объекта), а также особенностей функционирования значимого объекта.
- Анализ угроз безопасности информации должен включать:
  - выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
  - анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
  - определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
  - оценку возможных последствий от реализации (возникновения) угроз безопасности информации.
- В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации, в том числе персональным данным.
- По результатам анализа угроз безопасности информации могут быть разработаны рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.
- Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.
- Описание каждой угрозы безопасности информации должно включать:
  - источник угрозы безопасности информации;
  - уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;
  - возможные способы (сценарии) реализации угрозы безопасности информации;
  - возможные последствия от угрозы безопасности информации.
- Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.
- Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085. При определении угроз безопасности информации должны учитываются структурно-функциональные характеристики инфраструктуры электросетевых объектов, в том числе включающие наличие уровней (сегментов) АСУ ТП, состав АСУ ТП, физические, логические, функциональные и технологические взаимосвязи в автоматизированной системе управления, взаимодействие с

иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, режимы функционирования АСУ ТП, а также иные особенности ее построения и функционирования.

- По результатам определения угроз должна быть разработана модель угроз безопасности информации, в том числе включающая рекомендации по корректировке структурно-функциональных характеристик АСУ ТП / АСТУ и инфраструктуры в целом, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

- Разработку требований к системе защиты инфраструктуры электросетевых объектов необходимо выполнять с учетом:

– особенностей построения и функционирования объектов КИИ;

– вариантов уровней значимости объектов КИИ;

– выявленных актуальных угроз безопасности информации.

7.2.3. При разработке требований к комплексной системы обеспечения и управления информационной безопасностью необходимо учитывать требования в соответствии с действующими нормативно-техническими документами и правовыми актами, в том числе:

– Требования к идентификации и аутентификации субъектов и объектов доступа.

– Требования к управлению доступом субъектов к объектам.

– Требования к ограничению программной среды.

– Требования к защите машинных носителей информации.

– Требования к регистрации событий безопасности.

– Требования к антивирусной защите.

– Требования к обнаружению (предотвращению) вторжений.

– Требования к контролю (анализу) защищенности информации.

– Требования к целостности автоматизированной системы управления и информации.

– Требования к доступности технических средств и информации.

– Требования к защите среды виртуализации.

– Требования к защите технических средств и оборудования.

– Требования к защите автоматизированной системы и ее компонентов.

– Требования к безопасной разработке прикладного и специального программного обеспечения.

– Требования к управлению обновлениями программного обеспечения.

– Требования к планированию мероприятий по обеспечению защиты информации.

– Требования к обеспечению действий в нештатных (непредвиденных) ситуациях.

– Требования к информированию и обучение персонала.

– Требования к анализу угроз безопасности информации и рисков от их реализации.

– Требования к выявлению инцидентов и реагированию на них (управление инцидентами).

– Требования к управлению конфигурацией автоматизированной системы управления и ее системы защиты.

– Требования и положения политик обеспечения информационной безопасности и прочих смежных стандартов Заказчика.

7.2.4. При разработке типовых технических решений и типовой архитектуры комплексной системы обеспечения и управления информационной безопасностью необходимо:

– определить типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа), входящие в каждый объект КИИ.

– определить методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила

разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ОКИИ.

– определить меры защиты информации, подлежащие реализации в рамках ОКИИ.

– определить параметры настроек программного обеспечения и оборудования, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей в ОКИИ;

– определить виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определить структуру комплексной системы обеспечения и управления информационной безопасностью;

– определить меры защиты информации при информационном взаимодействии ОКИИ с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;

– определить особенности функционирования программного обеспечения и технических средств на каждом из уровней ОКИИ.

7.2.5. Выбор средств защиты информации необходимо производить с учетом их стоимости, совместимости с программным обеспечением и техническими средствами, используемые на объектах КИИ Заказчика, функций безопасности этих средств и особенностей их реализации, а также класса защищенности. Для выбранных средств защиты информации должны быть представлены технико-экономические обоснования.

7.2.6. Порядок внедрении технических средств защиты должен подразумевать, что:

– настройка технических средств защиты проводится в соответствии с проектной и эксплуатационной документацией на систему защиты;

– установка и настройка технических средств защиты информации должна обеспечивать корректность и совместимость выбранных средств защиты информации с программным обеспечением и техническими средствами объектов КИИ Заказчика.

7.2.7. В тестовых зонах должна быть проверена корректность функционирования элементов ОКИИ с комплексной системы обеспечения и управления информационной безопасностью и совместимость выбранных средств защиты информации с программным обеспечением и техническими средствами.

7.2.8. Разрабатываемые Стандарты организации должны включать следующие документы:

– Руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры Цифровой сети.

– Руководящие указания по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики (ИА, Филиал РСК, Дисп. пункт ПО, Дисп. пункт РЭС, ПС 35-220 кВ, РП, ТП 6-20/0,4 кВ).

– Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры (ИА, Филиал РСК, Дисп. пункт ПО, Дисп. пункт РЭС, ПС 35-220 кВ, РП, ТП 6-20/0,4 кВ).

– Руководящие указания по установлению параметров и характеристик программных и программно-аппаратных средств, применяемых для обнаружения компьютерных инцидентов, компьютерных атак на информационную инфраструктуру Цифровой сети.

Названия разрабатываемых стандартов организации могут быть скорректированы по согласованию с Заказчиком. Порядок оформления стандартов организации согласовывается с заказчиком дополнительно.

7.2.9. В разрабатываемых Стандартах организации должны быть учтены и описаны по форме и содержанию организационные меры, для всех этапов жизненного цикла объектов защиты и ОКИИ, в том числе в части:

– реализации отдельных мер защиты информации в ОКИИ в рамках его подсистемы защиты;

– планирования мероприятий по обеспечению защиты информации в ОКИИ;

– обеспечения действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации ОКИИ;

– информирования и обучения персонала ОКИИ;

– непрерывного анализа угроз безопасности информации ОКИИ;

– управления (администрирования) системой защиты информации ОКИИ;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ОКИИ и/или к возникновению угроз безопасности информации, и реагирования на них;

– управления ОКИИ и их системы защиты, в том числе управления конфигурациями;

– контроля (мониторинга) за обеспечением уровня защищенности ОКИИ;

– защиты информации при выводе из эксплуатации ОКИИ: (архивирование информации, содержащейся на ОКИИ с сохранением возможности дальнейшего использования данной информации; уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации, при это должны быть определены условия и требования для уничтожения информации и машинных носителей информации);

– введения ограничений на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации технических средств и программного обеспечения ОКИИ и средств защиты.

7.2.10. По итогам разработки Стандартов организации дополнительно подготовить план мероприятий (дорожной карты) по приведению критической информационной инфраструктуры в соответствие с требованиями к обеспечению защиты информации, в котором:

– должны быть учтены условия и ограничения для инфраструктуры ОКИИ, требования к комплексной системе обеспечения и управления информационной безопасностью;

– должны быть определены критерии несоответствия требованиям защиты;

– должны быть определены требования и порядок привлечения сторонних организаций для выполнения мероприятий по обеспечению защиты КИИ Заказчика;

– должны быть сформированы требования к численности и квалификации персонала, участвующего в эксплуатации комплексной системы обеспечения и управления информационной безопасностью, а также требования в части обеспечения безопасности к персоналу, эксплуатирующему (обеспечивающему функционирование) ОКИИ;

– должно учитываться информирование и обучение действующего персонала;

– должно предусматриваться обеспечение действий в нештатных (непредвиденных) ситуациях в рамках проводимых работ.

7.2.11. В рамках разработки Стандартов организации разработать методологию динамической оценки соответствия комплексной системы обеспечения и управления информационной безопасностью требованиям защиты.

7.2.12. Разработка методологии оценки соответствия комплексной системы обеспечения и управления информационной безопасностью требованиям защиты должна выполняться с учетом организационных и технические требований, предъявляемых к комплексной системе обеспечения и управления информационной безопасностью, сформированных в рамках НИР.

7.2.13. Методология оценки соответствия комплексной системы обеспечения и управления информационной безопасностью не должна оказывать отрицательного влияния на штатный режим функционирования ОКИИ.

8. Потребность в результатах работ

8.1. Результаты работ планируется использовать для реализации проектов по проектированию и строительству электросетевых объектов, в том числе подстанций (ПС) и подстанций выполненных с применением элементов и по технологиям «цифровых подстанций».

9. Сроки и этапы работ

9.1. Исполнитель обеспечивает предварительное согласование с Заказчиком отчетных материалов по отдельным подэтапам работ, в пределах срока выполнения данного подэтапа работы, но не позднее чем за 10 рабочих дней до срока окончания подэтапа работы, путем направления отчетных материалов Заказчику в электронном виде. Заказчик, в течение 10 рабочих дней с даты получения отчетных материалов, проводит рассмотрение и согласование отчетных материалов. В случае наличия замечаний в отчетных материалах Заказчик направляет их Исполнителю на доработку. Предварительное согласование отчетных материалов и направление замечаний осуществляется посредством направления Заказчиком письма в электронном виде Исполнителю.

Предварительное рассмотрение отчетных материалов проводится путем организации переписки на адреса электронной почты:

От Заказчика – (определяется на этапе заключения договора);

От Исполнителя – (определяется на этапе конкурсных процедур).

9.2. Порядок приемки и передачи результатов работ по этапам указан в разделе 12 настоящего Технического задания.

Примечание: * Промежуточные сроки выполнения работ определяет Участник закупочных процедур на этапе представления конкурсных предложений (заявок), допускается совмещение сроков выполнения отдельных подэтапов работ по решению исполнителя без изменения общего срока этапа работы.

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
1.	**Этап № 1 «Разработать модели угроз безопасности информации для технологического сегмента КИИ Заказчика»**	**со дня заключения договора / 30.04.2019 г.**	
1.1	Исследование особенностей технологического сегмента КИИ Заказчика, в том числе с учетом основных направлений развития электросетевого комплекса.	* / *	Отчет по результатам обследования технологического сегмента КИИ Заказчика.
1.2	Проведение анализа угроз информационной безопасности для технологического сегмента КИИ.	* / *	Реестр возможных деструктивных воздействий на технологический сегмент КИИ и оценка тяжести последствий их реализации.
1.3	Разработка методики оценки уровней значимости ОКИИ, включая предложения по типизации ОКИИ в зависимости от функционального назначения и уровня значимости.	* / *	Методика оценки уровней значимости ОКИИ, включая предложения по типизации ОКИИ в зависимости от функционального назначения и уровня значимости.
1.4	Разработка методологии периодической оценки соответствия инфраструктуры электросетевых	* / *	Методика периодической оценки соответствия инфраструктуры объектов электроэнергетики

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
	объектов требованиям информационной защиты.		требованиям информационной защиты.
1.5	Разработка программы проведения обследования (сбора исходных данных) ОКИИ в технологическом секторе КИИ. Согласование программы проведения обследования с Заказчиком.	* / *	Программа проведения обследования ОКИИ (план-график работ, перечень привлекаемых ресурсов, разделение зон ответственности, описание методов и способов сбора исходных данных).
1.6	Проведение обследования ОКИИ технологического сегмента Заказчика.	* / *	Отчет по результатам обследования ОКИИ технологического сегмента Заказчика.
1.7	Построение модели угроз безопасности информации для ОКИИ технологического сегмента.	* / *	Модель угроз безопасности информации ОКИИ технологического сегмента, включая: - описание ОКИИ; - угрозы безопасности информации; - описание возможностей нарушителей (модель нарушителя); - возможные уязвимости ОКИИ; - описание способов (сценариев) реализации угроз безопасности информации; - описание последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования; - рекомендации по корректировке (оптимизации) структурно-функциональных характеристик ОКИИ, направленные на блокирование (нейтрализацию) угроз безопасности информации.
1.8	Представление Заказчику результатов работ по этапу №1. Прием Заказчиком результатов работ по этапу № 1 (20 рабочих дней).	* / *	Акт приема - передачи выполненных работ по этапу №1.
2.	**Этап № 2 «Разработка требований к комплексной системе обеспечения и управления информационной безопасностью КИИ»**	* / **30.11.2019**	
2.1	Разработка перечня технических и организационных мер защиты ОКИИ технологического сегмента.	* / *	Перечень технических и организационных мер защиты ОКИИ технологического сегмента.

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
2.2	Разработка требований к функционалу средств защиты ОКИИ технологического сегмента, нейтрализующих выявленные угрозы.	* / *	Требования к функционалу средств защиты ОКИИ технологического сегмента, нейтрализующих выявленные угрозы.
2.3	Разработка требований к порядку разработки (проектирования) типовой архитектуры комплексной системы обеспечения и управления информационной безопасностью.	* / *	Требования к порядку разработки (проектирования) типовой архитектуры комплексной системы обеспечения и управления информационной безопасностью.
2.4	Разработка требований к эксплуатации комплексной системы обеспечения и управления информационной безопасностью.	* / *	Требования к эксплуатации комплексной системы обеспечения и управления информационной безопасностью.
2.5	Разработка технико-экономического сравнения реализации комплексной системы обеспечения и управления информационной безопасностью.	* / *	Технико-экономическое сравнение реализации комплексной системы обеспечения и управления информационной безопасностью.
2.6	Разработка основных технических решений (ОТР) по созданию комплексной системы обеспечения и управления информационной безопасностью.	* / *	Основные технические решения (ОТР) по созданию комплексной системы обеспечения и управления информационной безопасностью, включая: - цель и задачи обеспечения защиты информации; - уровни значимости ОКИИ; - перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов Заказчика, которым должна соответствовать комплексная система обеспечения и управления информационной безопасностью; - описание объектов КИИ; - требования к мерам и средствам защиты информации, применяемым в КИИ; - требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями; - требования к поставляемым техническим средствам,

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
			программному обеспечению, средствам защиты информации; - функции Заказчика по обеспечению защиты информации в КИИ; - стадии (этапы работ) создания комплексной системы обеспечения и управления информационной безопасностью; - требования к отчетной документации.
2.7	Разработка типовых технических решений и типовой архитектуры по обеспечению информационной безопасности технологического сегмента КИИ Заказчика в том числе для цифровых подстанций с применением оборудования с непосредственным жидкостным охлаждением, позволяющие снизить уровень шума и зависимость от внешних неблагоприятных факторов окружающей среды.	* / *	Типовые технические решения и типовые архитектура по обеспечению информационной безопасности КИИ Заказчика.
2.8	Разработка рекомендаций по распределению обязанностей и ответственности по обеспечению безопасности между структурными подразделениями Заказчика.	* / *	Рекомендации по распределению обязанностей и ответственности по обеспечению безопасности между структурными подразделениями Заказчика
2.9	Разработка рекомендаций по требуемым изменениям функционала и кадрового состава подразделений Заказчика.	* / *	Рекомендации по требуемым изменениям функционала и кадрового состава подразделений Заказчика.
2.10	Разработка рекомендаций по квалификационным требованиям к работникам Заказчика для обеспечения функционирования и эксплуатации комплексной системы обеспечения и управления информационной безопасностью.	* / *	Рекомендации по квалификационным требованиям к работникам Заказчика для обеспечения функционирования и эксплуатации комплексной системы обеспечения и управления информационной безопасностью.
2.11	Разработка Стандартов организации по обеспечению кибербезопасности технологического сегмента КИИ Заказчика. Рассылка Стандартов на согласование Заказчику. Сбор и анализ замечаний и предложений по Стандартам от Заказчика.	* / *	Проект Стандартов организации по обеспечению кибербезопасности КИИ Заказчика.

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
2.12	Свод замечаний и предложений с указанием принятых и отклоненных замечаний, с обоснованием отклонения. Доработка Стандартов по результатам рецензирования. Представление Заказчику итоговых редакций Стандартов.	* / *	Стандарты организации по обеспечению кибербезопасности КИИ Заказчика.
2.13	Представление Заказчику результатов работ по этапу №2. Прием Заказчиком результатов работ по этапу № 2 (20 рабочих дней).	* / *	Акт приема - передачи выполненных работ по этапу №2.
3.	**Этап №3 «Разработка методики обеспечения всех этапов жизненного цикла объектов защиты и ОКИИ»**	* / **31.10.2020**	
3.1	Разработка программы и методик испытаний средств защиты информации электросетевых объектов.	* / *	Программа и методика испытаний средств защиты информации электросетевых объектов.
3.2	Проведение проверки разработанных технических решений и типовой архитектуры на предмет совместимости с ПО ПТК ОКИИ в форме стендовых испытаний.	* / *	Протокол проверки разработанных технических решений на предмет совместимости с ПО ПТК ОКИИ в форме стендовых испытаний.
3.3	Разработка рекомендаций по приемке, вводу и выводу из эксплуатации комплексной системы обеспечения и управления информационной безопасностью.	* / *	Рекомендации по приемке, вводу и выводу из эксплуатации комплексной системы обеспечения и управления информационной безопасностью.
3.4	Разработка плана мероприятий (дорожной карты) по приведению КИИ Заказчика в соответствие с требованиями к обеспечению защиты информации.	* / *	План мероприятий (дорожная карта) по приведению КИИ Заказчика в соответствие с требованиями к обеспечению защиты информации.
3.5	Подготовка документов необходимых для защиты интеллектуальной собственности, полученной в ходе выполнения работы, в объеме и в соответствии с требованиями действующего законодательства Российской Федерации.	* / *	Документы необходимые для защиты интеллектуальной собственности, полученной в ходе выполнения работы, в объеме и в соответствии с требованиями действующего законодательства Российской Федерации.
3.6	Подготовка отчет по НИРиТР в соответствии с ГОСТ 7.32-2001	* / *	Отчет по НИРиТР.
3.7	Подготовка презентации по теме НИРиТР.	* / *	Презентация по теме НИРиТР.

№ п/п	Наименование этапов работ по договору	Сроки выполнения (начало/ окончание)	Форма и вид отчетных материалов
3.8	Представление Заказчику результатов работ по этапу №3. Прием Заказчиком результатов работ по этапу № 3 (20 рабочих дней).	* / *	Акт приема - передачи выполненных работ по этапу №3.

10. Результаты работ

10.1. По Этапу № 1:

10.1.1. Отчет по результатам обследования объектов технологического сегмента КИИ Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.2. Реестр возможных деструктивных воздействий на технологический сегмент КИИ и оценка тяжести последствий их реализации в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.3. Методика оценки уровней значимости ОКИИ, включая предложения по типизации ОКИИ в зависимости от функционального назначения и уровня значимости в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.4. Методика периодической оценки соответствия инфраструктуры объектов электроэнергетики требованиям информационной защиты в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.5. Программа проведения обследования ОКИИ (план-график работ, перечень привлекаемых ресурсов, разделение зон ответственности, описание методов и способов сбора исходных данных) в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.6. Отчеты по результатам обследования типовых ОКИИ технологического сегмента Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.1.7. Модель угроз безопасности информации ОКИИ технологического сегмента, в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf), включая:

- описание ОКИИ;
- угрозы безопасности информации;
- описание возможностей нарушителей (модель нарушителя);
- возможные уязвимости ОКИИ;
- описание способов (сценариев) реализации угроз безопасности информации;
- описание последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования;
- рекомендации по корректировке (оптимизации) структурно-функциональных характеристик ОКИИ, направленные на блокирование (нейтрализацию) угроз безопасности информации.

10.2. По Этапу № 2:

10.2.1. Перечень технических и организационных мер защиты ОКИИ технологического сегмента в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.2. Требования к функционалу средств защиты ОКИИ технологического сегмента,

нейтрализующих выявленные угрозы в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.3. Требования к порядку разработки (проектирования) типовой архитектуры комплексной системы обеспечения и управления информационной безопасностью в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.4. Требования к эксплуатации комплексной системы обеспечения и управления информационной безопасностью в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.5. Технико-экономическое сравнение реализации комплексной системы обеспечения и управления информационной безопасностью в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.6. Основные технические решения (ОТР) по созданию комплексной системы обеспечения и управления информационной безопасностью, в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf), включая:

- цель и задачи обеспечения защиты информации;
- уровни значимости ОКИИ;
- перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов Заказчика, которым должна соответствовать комплексная система обеспечения и управления информационной безопасностью;
- описание объектов КИИ;
- требования к мерам и средствам защиты информации, применяемым в КИИ;
- требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
- функции Заказчика по обеспечению защиты информации в КИИ;
- стадии (этапы работ) создания комплексной системы обеспечения и управления информационной безопасностью;
- требования к отчетной документации.

10.2.7. Типовые технические решения и типовые архитектура по обеспечению информационной безопасности КИИ Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.8. Рекомендации по распределению обязанностей и ответственности по обеспечению безопасности между структурными подразделениями Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.9. Рекомендации по требуемым изменениям функционала и кадрового состава подразделений Заказчика. в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.10. Рекомендации по квалификационным требованиям к работникам Заказчика для обеспечения функционирования и эксплуатации комплексной системы обеспечения и управления информационной безопасностью в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.11. Проект Стандартов организации по обеспечению кибербезопасности КИИ Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.2.12. Стандарты организации по обеспечению кибербезопасности технологического

сегмента КИИ Заказчика в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3. По Этапу № 3:

10.3.1. Программа и методика испытаний средств защиты информации электросетевых объектов в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.2. Протокол проверки разработанных технических решений на предмет совместимости с ПО ПТК ОКИИ в форме стендовых испытаний в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.3. Рекомендации по приемке, вводу и выводу из эксплуатации комплексной системы обеспечения и управления информационной безопасностью в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.4. План мероприятий (дорожная карта) по приведению КИИ технологического сегмента Заказчика в соответствие с требованиями к обеспечению защиты информации в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.5. Документы необходимые для защиты интеллектуальной собственности, полученной в ходе выполнения работы, в объеме и в соответствии с требованиями действующего законодательства Российской Федерации в 1 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.6. Отчет по НИРиТР в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (doc или docx) и AdobeReader (pdf).

10.3.7. Презентация по теме НИРиТР в 3 (трех) экземплярах на бумажном носителе и в 1 (одном) экземпляре в электронном виде в форматах MS Office (ppt или pptx) и AdobeReader (pdf).

11. Требования к оформлению результатов работ

11.1 Исполнитель передает Заказчику отчеты о выполнении работ, оформленные в соответствии ГОСТ 7.32-2001 «Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления».

11.2 При разработке, оформлении и изложении отчетных материалов должны учитываться требования действующих нормативно-технических документов указанных в п.5.7, а также:

– ГОСТ Р 56205-2014 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы»;

– ГОСТ Р 62443-2-1-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы»;

– ГОСТ Р 56498-2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы»;

– ГОСТ Р 15.000-94 «Система разработки и постановки продукции на производство. Основные положения»;

– ГОСТ Р 15.201-2000 «Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки на производство»;

– ГОСТ 2.116-84 «Карта технического уровня и качества продукции»;

– ГОСТ Р 15.011-96 «Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения»;

– ГОСТ 7.32-2001 «Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления»;

– ГОСТ Р 1.4-2004 «Стандарты организации. Общие требования»;

– ГОСТ 2.118-73 «Единая система конструкторской документации. Техническое предложение»;

– ГОСТ 2.103-68 «Единая система конструкторской документации. Стадии разработки»;

– ОСТ 153-00.0-002-98 «Порядок разработки и постановки на производство продукции производственно-технологического назначения для топливно-энергетического комплекса».

11.3 Основной текст отчетных материалов оформляется на русском языке, печатным (машинным) способом с использованием персонального компьютера (ЭВМ).

11.4 Набор текста в отчетных материалах производится в текстовом редакторе Microsoft Office Word в файловых форматах *.doc или *.docx.

11.5 Страницы в отчетных материалах должны соответствовать стандартному формату А4 (210 × 297 мм). В обоснованных случаях допускается использовать другой формат А3 (297 × 420 мм), при этом листы должны быть укомплектованы в едином документе (формате).

11.6 Схемы, графические материалы оформляется с использованием графического редактора AutoCAD и графического редактора Microsoft Visio.

11.7 Все отчетные материалы должны быть продублированы в формате AdobeReader (*.pdf) в цветном виде.

11.8 Текст должен быть кратким, точным, не допускающим различных толкований, логически последовательным. Ошибки, опечатки, графические неточности, помарки, повреждения листов не допускаются. Вносить в текст отчетных материалов отдельные слова, формулы, знаки, буквы, символы, графики, рисунки рукописным способом не допускается.

11.9 Для наглядности и удобства изложения применяют таблицы, графический материал, схемы, формулы.

11.10 В документации должны применяться общепринятые условные обозначения, единицы величин, символы и сокращения.

11.11 В тексте наравне с русским, допускается использовать латинский и греческий алфавит, для обозначения сокращения, формул, величин, символов и т.п.

11.12 Результаты работ (отчетные материалы) на бумажных носителях представляются в виде оформленных сшитых томов. На титульном листе должны быть оригинальные печати организации разработчика и подлинные подписи руководителя организации. На следующей странице должны быть подписи руководителя работ и основных исполнителей.

11.13 Результаты работ в электронном виде представляются на CD (DVD) и USB-накопителе. Стоимость CD (DVD) и USB-накопителя признается незначительной, отдельно не оплачивается и возврату не подлежит.

11.14 Порядок оформления стандартов организации согласовывается с заказчиком дополнительно.

12 Требования к приемке и передаче результатов работ

12.1 Приемка работ осуществляется в сроки указанные в разделе 9 настоящего Технического задания.

12.2 Исполнитель, не позднее, чем за 20 рабочих дней до даты окончания работ в целом по этапу, представляет Заказчику для рассмотрения отчетные материалы, указанные в разделе 10 настоящего Технического задания, на бумажном носителе и в электронном виде (на CD (DVD) и USB-накопителе) с сопроводительным письмом. Заказчик, в течение 20 рабочих дней с даты получения отчетных материалов, проводит рассмотрение и согласование отчетных материалов. В случае наличия замечаний в отчетных материалах Заказчик направляет их Исполнителю на доработку. Направление замечаний осуществляется посредством направления Заказчиком

письма Исполнителю. В случае согласования отчетных материалов Заказчик подписывает Акт приема - передачи выполненных работ.

12.3 Результаты работы подлежат представлению и защите на Научно-Техническом Совете (далее – НТС) ПАО «МРСК Волги» и ПАО «Россети» (по требованию Заказчика) с проведением Исполнителем презентации результатов работ (Исполнитель готовит презентацию и проводит защиту НИОКР). Сроки проведения определяются Заказчиком дополнительно

12.4 Исполнитель должен обеспечить консультирование сотрудников Заказчика по вопросам настоящей работы.

13 Требования к защите прав на результаты работ

13.1 Заказчику с момента подписания Актов приема-передачи выполненных работ (в отдельности по каждому этапу) переходят исключительные права на объекты интеллектуальной собственности, право собственности на все материальные носители и право на получение патента и свидетельства на объекты интеллектуальной деятельности, полученные в результате выполненных работ. Вознаграждение за переход исключительного права включено в цену договора и отдельно не оплачивается.

13.2 Автор (группа авторов), творческим трудом которого (которых) получены результаты интеллектуальной деятельности, сохраняют за собой право авторства и иные личные неимущественные права, предусмотренные действующим законодательством. Авторские вознаграждения за использование результата интеллектуальной деятельности включено в цену договора и отдельно не оплачивается.

13.3 Исполнитель в рамках выполнения работ обязуется подготовить, согласовать и передать Заказчику необходимые документы для защиты интеллектуальной собственности, полученной в ходе выполнения работы, в объеме в соответствии с требованиями действующего законодательства Российской Федерации.

14. Гарантийное обязательство

14.1. Исполнитель предоставляет гарантийное сопровождение результатам работ в течение 1 (один) года с даты подписания Акта сдачи-приемки результатов работ по НИР. Гарантийное сопровождение заключается в устранении за свой счет выявленных недостатков и/или неточностей в документации, в проведении (без ограничения количества раз) консультирования персонала ПАО «МРСК Волги».

14.2. При обнаружении недостатков и/или неточностей в документации Заказчик направляет Исполнителю письменное уведомление в течение 10 (десяти) рабочих дней с даты их обнаружения.

14.3. Исполнитель обязуется в течение 10 (десяти) рабочих дней со дня получения от Заказчика уведомления направить письменный ответ Заказчику с указанием срока устранения недостатков и/или неточностей.

14.4. Консультирование персонала допускается проводить как в очной форме, так и в устной форме посредством телефонной связи, либо в письменной форме посредством факсимильного сообщения или посредством электронной почты с обязательным направлением, в течение 7 (семи) рабочих дней, оригинала заказным письмом получателю по его юридическому адресу. Для организации консультирования персонала Исполнитель обязуется в течение 10 (десяти) рабочих дней со дня заключения договора представить Заказчику контактную информацию (ФИО, должности, телефон, факс, адрес электронной почты) ответственных работников. В случае изменения контактной информации Исполнитель обязуется в течение 10 (десяти) рабочих дней направить Заказчику актуализированную информацию.

14.5. Гарантийное сопровождение, включая консультирование персонала входит в стоимость договора и отдельно Заказчиком не оплачивается.

15. Требования к подготовке Исполнителем технического предложения в рамках закупочных процедур

15.1. Исполнитель должен предоставить техническое предложение на НИРиТР. В техническом предложении необходимо указать конкретные сроки реализации проекта, используемые подходы к выполнению НИРиТР, привести краткое описание планируемых работ, порядок выполнения работ в указанные сроки. Использование Технического задания Заказчика в качестве технического предложения Исполнителя не допускается.

15.2. Исполнитель должен указать промежуточные сроки выполнения работ в разделе 9 Технического задания и представить заполненный Календарный план выполнения работ (по форме указанной в проекте договора). Предоставление Календарного плана работ без указания сроков подэтапов не допускается.

15.3. Исполнитель должен предоставить заполненную Смету затрат (по форме указанной в проекте договора). В смете должна быть заполнены все работы в соответствии с Календарным планом, сроки выполнения работ и расчет стоимости. Предоставление не заполненной Сметы затрат не допускается.

16. Требования к Исполнителю:

16.1. Исполнитель (коллективный участник) должен обладать следующими лицензиями на весь срок исполнения работ:

16.1.1 Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации (осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации) (Копия лицензии).

16.1.2 Лицензия ФСБ России на осуществление работ, связанных с использованием сведений, составляющих государственную тайну (Копия лицензии).

16.1.3 Лицензия ФСБ России на осуществление деятельности по 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, по следующему перечню выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств на следующие виды работ, предусмотренные пунктом 2, (Копия лицензий).

Информация подтверждается копиями лицензии.

16.2. Наличие опыта проектирования по обеспечению безопасности информации на объектах электроэнергетики в распределенных информационных системах, информационно-телекоммуникационных сетях, автоматизированных системах управления.

Информация подтверждается справкой по форме документации по запросу предложений, с описанием выполненных проектов, а также при наличии копии актов выполненных работ, отзывы заказчиков и (или) иные документы, подтверждающие опыт.

16.3. Дополнительно оценивается наличие у Исполнителя в штате специалистов, имеющих высшее профессиональное образование по направлению подготовки 090100 «Информационная безопасность», включающего перечень специальностей, представленных в «Общероссийском классификаторе специальностей по образованию» (ОК 009-2003, Утвержден Постановлением Госстандарта России от 30 сентября 2003 г. № 276-ст) (информация подтверждается копиями дипломов/свидетельств о переподготовке). (Данное требование не является обязательным и несоответствие Участника закупки данному требованию не будет являться основанием для отклонения заявки такого участника).

Лист согласования к техническому заданию

Рабочая группа по реализации проекта научно-исследовательских работ и технологических работ (НИРиТР) «Разработка мероприятий по обеспечению кибербезопасности вновь строящихся и реконструируемых цифровых подстанций. Разработка функциональных требований безопасности, требований доверия к безопасности для цифровых подстанций»

Председатель Рабочей группы:
Заместитель главного инженера по техническому развитию и эксплуатации _____ К.Г. Филиппов

Заместители председателя Рабочей группы:
Начальник департамента безопасности _____ М.Ф. Пивненко

Начальник департамента технологического развития и инноваций _____ Д.А. Толмачев

Члены Рабочей группы:
Заместитель начальника департамента технологического развития и инноваций _____ Д.В. Багаев

Начальник отдела защиты информации и информационно-аналитической работы департамента безопасности _____ А.Я. Науменко

Начальник отдела внедрения новой техники и технологий департамента технологического развития и инноваций _____ Н.Н. Медведев

Заместитель начальника отдела департамента технологического развития и инноваций _____ А.С. Александров

Ведущий инженер инновационного и научно-технического развития Департамента технологического развития и инноваций _____ С.В. Якименко

Ведущий специалист отдела эксплуатации и развития автоматизированных систем технологического управления Управления автоматизированных систем технологического управления Департамента корпоративных и технологических АСУ _____ Л.В. Щедриков