Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Национальная программа
«Цифровая экономика Российской Федерации»

Федеральный проект «Информационная безопасность»

Выполнение работ по созданию киберполигона для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ современным практикам обеспечения безопасности

На 34 листах

Москва, 2019

1 Общие сведения

1.1 Полное наименование работ: Создание киберполигона для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ современным практикам обеспечения безопасности.

1.2 Сокращенное наименование работ: Создание киберполигона.

1.3 Перечень нормативно-правовых документов, на основании которых создается Киберполигон:

– Стратегия национальной безопасности, утвержденная Указом Президента Российской Федерации от 31 декабря 2015 года № 683;

– Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ № 646 от 5 декабря 2016 г.;

– Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»;

– Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества на 2017–2030 годы»;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

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

– Паспорт федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»;

– Положение о банке данных угроз безопасности информации, утвержденного приказом ФСТЭК России от 16 февраля 2015 г. № 9;

– Постановление Правительства РФ от 12 октября 2019 г. № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на создание киберполигона для обучения и тренировки

специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности».

1.4 Плановые сроки выполнения работ по созданию Киберполигона не должны превышать сроков, указанных в настоящем техническом задании (далее – ТЗ).

1.5 Источник и порядок финансирования определяется Правилами предоставления субсидий из федерального бюджета российскому юридическому лицу на создание киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности (далее – Правила предоставления субсидии) и Соглашением о предоставлении субсидии в соответствии с типовой формой, утвержденной Министерством финансов Российской Федерации.

1.6 Порядок оформления и предъявления Заказчику результатов работ должен соответствовать требованиям настоящего ТЗ. Результаты работ предъявляются Заказчику в сроки и порядке, определенном Правилами предоставления субсидии, в объёме и в соответствии с требованиями настоящего ТЗ.

2 Назначение и цели создания Киберполигона

2.1 Назначение Киберполигона

2.1.1 Назначением Киберполигона является повышение уровня обеспечения информационной безопасности Российской Федерации.

2.2 Цели создания Киберполигона

2.2.1 Системное развитие кадрового потенциала Российской Федерации в области информационной безопасности и формирование практических навыков защиты от реализации угроз информационной безопасности и компьютерных атак у учащихся, специалистов, руководителей в области ИТ и ИБ.

2.2.2 Стимулирование обмена лучшими практиками обеспечения информационной безопасности между организациями Российской Федерации.

2.2.3 Повышение уровня защищённости программного и аппаратного обеспечения информационной и промышленной автоматизированной инфраструктуры организаций Российской Федерации, в том числе объектов КИИ, включая программное обеспечение в составе Единого реестра российских программ для ЭВМ.

2.2.4 Совершенствование методического и нормативного обеспечения процессов информационной безопасности организаций в Российской Федерации.

2.3 Результаты работ

2.3.1 В результате выполнения работ Исполнителем должна быть создана технологическая, методологическая и организационная инфраструктура Киберполигона, позволяющая обеспечить решение следующих задач:

– повышение уровня практической подготовки в выявлении компьютерных атак, расследования инцидентов информационной безопасности, взаимодействии между подразделениями, внедрении превентивных мер по предупреждению компьютерных атак у учащихся, специалистов, экспертов и руководителей в сфере информационных технологий, информационной безопасности и систем промышленной автоматизации;

– проведение кибер-учений, соревнований и практических тренировок по информационной безопасности для учащихся, специалистов, экспертов и руководителей в сфере информационных технологий, информационной безопасности и систем промышленной автоматизации;

– тестирование программного обеспечения, оборудования, элементов автоматизированных систем и систем промышленной автоматизации, включая компоненты АСУ ТП и Промышленного Интернета, на реализацию функций информационной безопасности;

– проведение открытых соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации;

– наполнение Банка данных угроз и уязвимостей ФСТЭК России.

2.3.2 Результатом выполнения работ в рамках предоставляемой субсидии должен являться результат «Введен в эксплуатацию и функционирует киберполигон для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности», а именно:

– по мероприятию «Создание киберполигона, реализованного в том числе с использованием облачных технологий, для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» в рамках создания Киберполигона:

- создан 1 киберполигон для не менее 2 информационных технологических инфраструктур, эмулирующих корпоративные сети организаций кредитно-финансовой системы Российской Федерации (далее – «ИТ-киберполигон»), в составе не менее 50 виртуальных машин, эмулирующих серверное оборудование не менее 100 рабочих станций, 10 инфраструктурных и 3 прикладных сервисов в каждой инфраструктуре;
- создан 1 киберполигон для не менее 1 индустриальной инфраструктуры (автоматизированной системы управления технологическим процессом) энергетического сектора (далее – «Индустриальный киберполигон») в составе не менее 50 виртуальных машин, эмулирующих серверное оборудование не менее 50 рабочих станций, 5 инфраструктурных и 3 прикладных сервисов, системы моделирования энергосистем, релейной защиты и автоматики, мониторинга переходных процессов, управления технологическим процессом, диспетчерского управления, коммерческого учета электроэнергии;
- обеспечено функционирование киберполигона в 2019-2021 годах;

– по мероприятию «Создание независимых центров по техническому тестированию программного и аппаратного обеспечения, в том числе средств обеспечения безопасности информации, позволяющих компаниям получить доступ к аналитической информации и результатам независимого тестирования предлагаемых на рынке решений» в рамках создания Киберполигона:

- создано не менее 4 учебно-практических центров по техническому тестированию программного и аппаратного обеспечения в партнерстве с организациями высшего

образования Российской Федерации (далее – Центры киберполигона);

– обеспечено создание условий по использованию киберполигона для отработки практических навыков специалистов и экспертов разного профиля, руководителей в области обеспечения информационной безопасности и информационных технологий на территории федерального государственного автономного образовательного учреждения высшего образования «Дальневосточный федеральный университет».

2.3.3 Создаваемые Центры киберполигона должны быть построены на основе и с использованием общей централизованной инфраструктуры Киберполигона (ИТ-киберполигона, Индустриального киберполигона).

3 Требования к Киберполигону

3.1 Требования к Киберполигону в целом

3.1.1 При создании Киберполигона должны быть созданы:

– полигон для ИТ-инфраструктур – информационных систем (далее – «ИТ-полигон», «ИТ-киберполигон»);

– полигон для индустриальных инфраструктур – АСУ ТП и систем Промышленного интернета (далее – «Индустриальный полигон», «Индустриальный киберполигон»);

– четыре учебно-практических центра по техническому тестированию программного и аппаратного обеспечения с общей централизованной инфраструктурой на базе Киберполигона (ИТ-киберполигона, Индустриального киберполигона) в партнёрстве с организациями высшего профессионального образования.

3.1.2 Настоящее ТЗ определяет функциональные требования, требования к технологической инфраструктуре для каждого элемента Киберполигона.

3.1.3 Требования к вычислительным ресурсам должны быть определены на этапе проектирования для реализации функциональных требований настоящего ТЗ и возможности наращивания вычислительной мощности.

3.1.4 Программные и технические средства Киберполигона должны приоритетно выбираться с учётом возможности наращивания вычислительной мощности и масштабирования его компонентов и подсистем, в том числе, с использованием облачных технологий.

3.1.5 Киберполигон должен размещаться на создаваемой Исполнителем и (или) собственной вычислительной инфраструктуре для создания и обеспечения функционирования киберполигона на территории Российской Федерации.

3.1.6 Создаваемые учебно-практические центры Киберполигона должны быть построены на основе общей централизованной инфраструктуры Киберполигона (ИТ-киберполигона, Индустриального киберполигона).

3.2 Требования к функциям, выполняемых Киберполигоном

3.2.1 Техническая и организационная инфраструктура ИТ-полигона должна обеспечивать выполнение следующих функций:

– отработка практических навыков выявления компьютерных атак, расследования инцидентов информационной безопасности, взаимодействию между подразделениями ИТ и ИБ, внедрению превентивных мер по предупреждению компьютерных атак;

– проведение кибер-учений, соревнований и практических тренировок по информационной безопасности для учащихся, специалистов, экспертов и руководителей в сфере информационных технологи и информационной безопасности;

– тестирование программного обеспечения, оборудования, элементов информационных на реализацию функций информационной безопасности, защищённость и отсутствие уязвимостей;

– тестирование средств защиты информации на реализацию функциональных возможностей, защищённость и наличие уязвимостей;

– проведение открытых соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации;

– проверка и информирование об угрозах информационной безопасности уровня веб-приложений;

– наполнение Банка данных угроз и уязвимостей ФСТЭК России.

3.2.2 Техническая и организационная инфраструктура Индустриального полигона должна обеспечивать выполнение следующих функций:

– отработка практических навыков выявления компьютерных атак, расследования инцидентов информационной безопасности, взаимодействию между подразделениями ИТ и ИБ, внедрению превентивных мер по предупреждению компьютерных атак на кибер-физические системы;

– исследование и тестирование компонентов АСУ ТП и промышленного Интернета, СЗИ и технических решений по защите информации, в том числе моделирование атак и кибер-физических последствий;

– проведения кибер-учений, практических тренировок, обучений и соревнований для специалистов и экспертов разного профиля в области информационной безопасности систем промышленной автоматизации;

– исследования, тестирования и выявления уязвимостей и недекларированных возможностей в СЗИ, компонентах АСУ ТП и Промышленного Интернета;

– организацию работу сторонних исследователей в рамках работ по анализу защищенности СЗИ, компонентов АСУ ТП и Промышленного Интернета (в рамках открытых соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации);

– наполнение Банка данных угроз и уязвимостей ФСТЭК России.

3.3 Требования к структуре и функционированию Киберполигона

3.3.1 Требования к технической инфраструктуре ИТ-полигона

3.3.1.1 Техническая инфраструктура ИТ-полигона должна состоять из трёх блоков:

– базовая инфраструктура для проведения кибер-учений и/или соревнований по информационной безопасности;

– инфраструктуры для проведения исследований защищенности;

– инфраструктура для тренировки специалистов по информационной безопасности.

3.3.1.2 Базовая инфраструктура для проведения кибер-учений и/или соревнований по кибербезопасности должна включать:

– не менее 2 инфраструктур, эмулирующих корпоративные сети организаций кредитно-финансовой сферы Российской Федерации, в составе не менее 50 виртуальных машин, эмулирующих серверное оборудование, не менее 100 рабочих станций, 10 инфраструктурных и 3 прикладных сервисов в каждой корпоративной инфраструктуре, в том числе, воспроизведения функций дистанционного банковского обслуживания;

– информационную систему, позволяющую проводить активные атакующие действия на инфраструктуры для эмуляции атаки и обеспечить удаленное подключение участников кибер-учений или соревнований;

– базовые типовые средства защиты информации для создаваемых элементов инфраструктур;

– базовые типовые средства мониторинга и управления инцидентами информационной безопасности в инфраструктурах;

– средства моделирования типовых пользовательских операций при работе в информационных системах (посещение веб-ресурсов, чтение и отправка почтовых сообщений, использование файловых хранилищ и т. д.);

– средства моделирования действий внешнего и внутреннего нарушителей, реализующие автоматические компьютерные атаки в зависимости от инфраструктуры компьютерной сети;

– средства визуализации текущего статуса при проведении кибер-учений и/или соревнований по кибербезопасности;

– средства контроля обучаемых при проведении кибер-учений и/или соревнований по кибербезопасности с возможностью выставления оценок.

3.3.1.3 При создании инфраструктуры для проведения кибер-учений должна быть проведена разработка и адаптация политик безопасности как на уровне инфраструктуры, так и на уровне средств защиты, в том числе, с

учётом требований Приказа ФСТЭК России от 25 декабря 2017 г. № 239, Приказа ФСТЭК России от 11 февраля 2013 г. № 17, Приказа ФСТЭК России от 18 февраля 2013 г. № 21.

3.3.1.4 При создании инфраструктуры для проведения кибер-учений должно отдаваться преимущество использованию программного обеспечения, включённого в состав Единого реестра российских программ для ЭВМ.

3.3.1.5 При создании инфраструктуры для проведения кибер-учений должна быть проведена разработка и адаптация политик безопасности как на уровне инфраструктуры, так и на уровне средств защиты, эмулирующих три сценария зрелости организации:

– низкий уровень зрелости – базовая настройка средств защиты, минимальный объем использования встроенных средств безопасности инфраструктуры;

– средний уровень зрелости – настройки, адаптированные под действия внешнего нарушителя с низким потенциалом;

– высокий уровень зрелости – настройки, адаптированные под действия внешнего нарушителя с высоким потенциалом.

3.3.1.6 Инфраструктура для тренировки специалистов по информационной безопасности должна обеспечивать возможность практической подготовки включая, но не ограничиваясь следующими областями:

– «Навыки информационной безопасности» – инфраструктура включает в себя платформу для тестирования и подготовки сотрудников практическим навыкам соблюдения правил информационной безопасности, включая имитацию фишинговых атак;

– «Защита от несанкционированного доступа» – инфраструктура включает в себя технологии и продукты не менее двух производителей средств разграничения доступа каждого типа: программных систем защиты информации для коммерческих операционных систем, аппаратно-

программных модулей доверенной загрузки (электронных замков), защищённых операционных систем отечественного (не менее двух разнотипных операционных систем) и иностранного производства, средств антивирусной защиты информации (не менее двух отечественных различных антивирусных средств защиты);

– «Сетевая безопасность» – инфраструктура включает технологии и продукты не менее двух производителей межсетевых экранов, не менее двух производителей системы обнаружения атак;

– «Защита веб-приложений» – инфраструктура включает технологии и продукты не менее двух производителей межсетевых экранов уровня веб-приложений;

– «Мониторинг и анализ инцидентов информационной безопасности» – инфраструктура включает технологии и продукты не менее двух производителей систем выявления и анализа инцидентов;

– «Реагирование на компьютерные инциденты и компьютерная форензика» – инфраструктура включает в себя не менее двух производителей средств поиска, восстановления и анализа цифровых доказательств, включая скрытую и технологическую системную информацию;

– «Организации работ по реагированию на инциденты информационной безопасности» – особые требования к инфраструктуре не предъявляются.

3.3.1.7 Инфраструктура для тренировки специалистов по информационной безопасности должна обеспечивать возможность одновременной подготовки не менее 100 специалистов.

3.3.1.8 При создании инфраструктуры для проведения кибер-учений должна быть обеспечена связность и взаимодействие между компонентами на уровне информационных систем и инфраструктур.

3.3.2 Требования к технической инфраструктуре Индустриального полигона

3.3.2.1 Техническая инфраструктура Индустриального полигона должна состоять из следующих блоков:

– инфраструктура стендов систем АСУ ТП и промышленного Интернета, эмулирующая функционирование объектов электросетевого комплекса;

– инфраструктуры для проведения исследований защищенности;

– инфраструктуры для организации и проведения работ сторонних исследователей в рамках открытых соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации;

– инфраструктура для проведения киберучений и соревнований в составе не менее 21 виртуальных машин, эмулирующих серверное оборудование, не менее 19 рабочих станций, 5 инфраструктурных сервисов.

3.3.2.2 Техническая инфраструктура Индустриального полигона должна быть выполнена в соответствии с пятиуровневой моделью университета Пердью, в частности, должны быть реализованы следующие уровни:

– уровень 0 – датчики и исполнительный устройства;

– уровень 1 – базовые системы контроля;

– уровень 2 – системы диспетчерского управления и сбора данных.

3.3.2.3 Для организации уровня 0 технической инфраструктуры Индустриального полигона должны применяться имитирующие устройств, комплексы для моделирования или реальные компоненты систем промышленной автоматизации.

3.3.2.4 Для организации уровня 1 технической инфраструктуры Индустриального полигона должны применяться как реальные компоненты систем промышленной автоматизации, так и моделируемые.

3.3.2.5 Для организации уровня 2 технической инфраструктуры Индустриального полигона должны применяться реальные компоненты систем промышленной автоматизации.

3.3.2.6 Технологической основой Индустриального полигона должен являться комплекс систем промышленной автоматизации (АСУ), входящих в состав автоматизированных и цифровых подстанций, центров управления сетями.

3.3.2.7 В состав технической инфраструктуры Индустриального полигона должны входить:

– инфраструктура лабораторного комплекса полунатурного моделирования объектов электросетевого комплекса (подстанции, АСТУ) в составе:

а) система математического моделирования энергосистем;

б) система релейной защиты и автоматики;

в) система информационно-телекоммуникационной инфраструктуры;

г) система мониторинга переходных режимов;

д) автоматизированная система управления технологическим процессом;

е) система диспетчерского управления;

ж) система единого точного времени;

з) система коммерческого учета электроэнергии;

и) система контроля и управления доступом;

– программные и программно-аппаратные технические средства позволяющее проводить кибер-учения, обучения и соревнования очно и удаленно (онлайн);

– программные и программно-аппаратные технические средства для проведения работ сторонних исследователей в рамках анализа защищенности СЗИ, компонентов АСУ ТП и Промышленного Интернета (в рамках открытых соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации);

– программные и программно-аппаратные технические средства для проведения работ по исследованию СЗИ, компонентов АСУ ТП и Промышленного Интернета;

– система защиты информации, в том числе средства защиты удаленного доступа.

3.3.2.8 При реализации технической инфраструктуры может применяться оборудование как отечественного, так и зарубежного производства.

3.3.2.9 Техническая инфраструктура лабораторного комплекса полунатурного моделирования объекта электросетевого комплекса должна позволять имитировать работу энергосистемы в высоким уровнем симуляции.

3.3.2.10 В технической инфраструктуре лабораторного комплекса полунатурного моделирования объекта электросетевого комплекса должны применяться следующие промышленные протоколы:

– IEC 60870-6 ICCP;
– IEC 60870-5-104;
– IEC 61850 MMS;
– GOOSE;
– GSSE;
– SMV;
– PTP (МЭК 61850-9-3, IEEE Std 1588-2008, профиль Power Profile);
– NTP (SNTP).

3.3.2.11 Техническая инфраструктура Индустриального полигона должна позволять проводить исследования СЗИ, компонентов АСУ ТП и Промышленного Интернета преимущественно отечественного производства и в интересах российских организаций и должна состоять из трех рабочих мест исследователей и общего оборудования для всех исследователей.

3.3.2.12 Общее оборудование:

– инфракрасная паяльная станция для монтажа/демонтажа модулей памяти и других микросхем.

3.3.2.13 Каждое рабочее место исследователя должно включать в себя следующий список ПО и оборудования:

– дисассемблеры, декомпиляторы бинарных файлов для реверс-инжиниринга;

– комплексные инструменты для разнообразного тестирования web-сервисов;

– перехватчиками и анализаторами сетевых пакетов;

– программно-аппаратный комплекс для моделирования, записи и воспроизведения разнообразных сетевых атак, флудов, штормов и т. д.;

– инструментарием для фаззинга различных компонентов ПО;

– универсальные сканеры известных уязвимостей;

– анализаторы WiFi сетей;

– устройства для тестирования JTAG интерфейса;

– аппаратные сниферы (перехватчики): различных протоколов, включая Ethernet, I2C, SPI, UART, CAN, а также других специализированных протоколов, применяемых во встраиваемых устройствах;

– аппаратные платформы для анализа RFID/NFC;

– многофункциональные.

3.3.2.14 Техническая инфраструктура Индустриального полигона должна включать систему, позволяющую организовать работу сторонних исследователей в рамках работ по анализу защищенности СЗИ, компонентов АСУ ТП и промышленного Интернета (в рамках открытых соревнований по

поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации).

3.3.3 Требования к порядку наполнения банка данных угроз безопасности информации ФСТЭК России

3.3.3.1 Наполнение банка данных угроз безопасности информации сведениями об уязвимостях программного обеспечения, выявленных по результатам работы Киберполигона, должно осуществляться Исполнителем с учётом Регламента включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

3.3.3.2 Способы и механизмы взаимодействия Киберполигона и Банка данных угроз безопасности информации ФСТЭК России должны быть выработаны Исполнителем и согласованы с Заказчиком на этапе проектирования.

3.3.4 Требования к учебно-практическим центрам Киберполигона

3.3.4.1 Исполнитель должен обеспечить создание учебно-практических центров по техническому тестированию программного и аппаратного обеспечения, в том числе средств обеспечения безопасности информации, позволяющих компаниям получить доступ к аналитической информации и результатам независимого тестирования предлагаемых на рынке решений.

3.3.4.2 Создаваемые отраслевые Киберполигоны должны быть построены на основе общей централизованной инфраструктуры Киберполигона (ИТ-киберполигона, Индустриального киберполигона) в соответствии с п. 3.1.1-3.1.2 Технического задания.

3.3.4.3 Исполнитель должен обеспечить создание условий по использованию Киберполигона для отработки практических навыков специалистов, экспертов и руководителей по обеспечению информационной безопасности на территории учебно-практических центров, а именно:

– обеспечить удалённый доступ к инфраструктуре и функциональным возможностям Киберполигона для участия в киберучениях и тестирования программного обеспечения;

– оснастить площадки учебно-практических центров Киберполигона типовыми рабочими местами (не менее 12 типовых рабочих мест) и средствами коллективной визуализации, обеспечить наличие сетевой и вычислительной инфраструктуры для организации взаимодействия с основной инфраструктурой Киберполигона.

3.4 Требования к численности и квалификации персонала Киберполигона и режиму его работы

3.4.1.1 В рамках создания Киберполигона должны быть разработаны и реализованы предложения по организационной структуре, необходимой для реализации деятельности Полигона в соответствии с его функциями, включая:

– описание ролей персонала Киберполигона;

– перечень их функциональных обязанностей и зон ответственности;

– требования к необходимой квалификации сотрудников;

– методические рекомендации по подтверждению квалификации.

3.4.1.2 Численность персонала Киберполигонов должна быть установлена из расчета обеспечения ее работоспособности во всех требуемых режимах функционирования.

3.4.1.3 Киберполигон должен обеспечивать доступность инфраструктуры не менее 5 дней в неделю 8 часов в сутки с 10:00 до 18:00 с момента ввода в промышленную эксплуатацию.

3.4.1.4 Допустимое время простоя Киберполигона в год – не более 40 часов с момента ввода в промышленную эксплуатацию.

3.5 Требования к надежности

3.5.1 Надежность программно-технических средств Киберполигона должна обеспечиваться за счет:

– периодического резервного копирования информации на резервные машинные носители информации;

– возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала.

3.6 Требования безопасности

3.6.1 Защита информации при создании и функционировании Киберполигона должна осуществляться с учётом требований действующего законодательства и нормативных правовых актов Российской Федерации, в том числе, Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

3.6.1.1 Исполнителю рекомендуется использовать решения по обеспечению защиты информации в рамках Киберполигона с учётом требований, применяемых к значимым объектам критической информационной инфраструктуры не ниже третей категории значимости.

3.6.1.2 Исполнителю рекомендуется обеспечить выполнение требований, предъявляемых Приказом ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60)».

3.6.2 Состав и содержание мер обеспечения информационной безопасности должны быть выработаны Исполнителем на этапе

проектирования, в том числе, должна быть обеспечена защита инфраструктуры Киберполигона от несанкционированного доступа, вредоносного программного обеспечения.

3.6.3 Киберполигон не должен быть предназначен для обработки информации, составляющей государственную тайну.

3.6.4 В процессе монтажа, наладки, эксплуатации, обслуживания и ремонта технических средств Киберполигона должны соблюдаться нормы электрической и противопожарной безопасности, установленные на объекте проведения работ.

3.6.5 Система электропитания Киберполигона должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

3.6.6 Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов Киберполигона, не должны превышать действующих норм (СанПиН 2.2.2/2.4.1340-03 от 03.06.2003).

3.7 Требования к эргономике и технической эстетике

3.7.1 Компоненты технической части Киберполигона должны иметь возможность установки в монтажные стойки (шкафы) в имеющихся серверных помещениях или на имеющихся виртуальных мощностях Исполнителя.

3.7.2 В рамках технической инфраструктуры Киберполигона должны быть организованы унифицированные автоматизированные рабочие места для проведения обучений и тренировок в размере не менее 20 шт. с возможностью дальнейшего увеличения.

3.7.2.1 Техническое обеспечение унифицированных рабочих мест должно предоставлять возможность использования инфраструктуры Киберполигона для участия в киберучениях и проведения тестирования программного обеспечения.

3.7.2.2 Организационное обеспечение унифицированных рабочих мест должно осуществляться с использованием регламентов использования Киберполигона и содержать порядок использования и доступа к инфраструктуре Киберполигона.

3.7.2.3 Методическое обеспечение унифицированных рабочих мест должно осуществляться с использованием системы дистанционного обучения и содержать материалы, инструкции, сценарии для прохождения подготовки к участию в киберучениях, соревнованиях по информационной безопасности, проведения тестирования программного обеспечения.

3.7.3 Техническая инфраструктура Киберполигона должна обеспечивать возможность подключения удаленных слушателей с использованием системы дистанционного обучения. Требования к системе дистанционного обучения должны быть выработаны Исполнителем на этапе технического проектирования.

3.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Киберполигона

3.8.1 Исполнитель должен обеспечить эксплуатацию и функционирование Киберполигона и его компонентов.

3.8.2 Технические средства Киберполигона должны выбираться с учетом их непрерывного функционирования.

3.8.3 Эксплуатация программно-технических средств Киберполигона должна предусматривать следующие виды технического обслуживания:

- оперативное обслуживание;
- профилактические работы.

3.8.4 Оперативное обслуживание должно осуществляться в виде ежедневного контроля функционирования программно-технических средств Киберполигона.

3.8.5 Оперативное обслуживание не должно нарушать выполнения функций Киберполигона в целом.

3.8.6 Профилактические работы должны включать периодическую проверку и обслуживание программно-технических средств Киберполигона, для которых такие процедуры предусмотрены эксплуатационной документацией компании-производителя средств.

3.8.7 Объем и порядок выполнения технического обслуживания технических и программных средств Киберполигона должны определяться эксплуатационной документацией.

3.8.8 Все пользователи Киберполигона должны соблюдать правила эксплуатации электроустановок.

3.9 Требования по сохранности информации при авариях

3.9.1 При авариях должна быть обеспечена сохранность следующей информации:

– параметры конфигурационных настроек систем Киберполигона;

– параметры настроек средств идентификации, аутентификации и авторизации систем Киберполигона;

– данные журналов событий.

3.9.2 Сохранность информации должна обеспечиваться при следующих аварийных ситуациях:

– нарушение электропитания;

– сбой общего или специального программного обеспечения компонентов Киберполигона;

– проведение внутренних и внешних атак на инфраструктуру Киберполигона.

3.9.3 Должна быть предусмотрена возможность восстановления работоспособности и параметров настройки технических средств Киберполигона, в том числе с помощью резервных копий и (или) дистрибутивов.

3.10 Требования к защите от влияния внешних воздействий

3.10.1Программно-технические и технические средства Киберполигона должны быть установлены в специально оборудованных помещениях, в которых обеспечивается необходимая степень климатической защиты от воздействия внешней среды.

3.10.2Помещения, в которых размещаются программные и технические средства Киберполигона, должны быть оборудованы средствами контроля и управления доступом, пожарной безопасности, вентиляции и кондиционирования.

3.10.3Помещения и оборудование Киберполигона должны исключать возможность бесконтрольного доступа посторонних лиц.

3.11 Требования к патентной чистоте

3.11.1Применяемые решения в рамках Киберполигона должны отвечать требованиям по патентной чистоте в соответствии с действующим законодательством Российской Федерации.

3.12 Требования по стандартизации и унификации

3.12.1Все технические решения в рамках создания Киберполигона должны основываться на использовании типовых решений и максимальной унификации технического и программного обеспечения.

3.12.2В составе Киберполигона возможно применение как серийно выпускаемых программных, технических и программно-аппаратных средств, так и специально разработанных средств.

3.12.3Не допускается формальная декларация соответствия специально разработанных программных, технических и программно-аппаратных средств в случае, если это недопустимо в соответствии с законодательством Российской Федерации.

3.13 Требования к развитию и модернизации Киберполигона

3.13.1Организационная, техническая и методическая инфраструктура Киберполигона должна обеспечивать возможность развития и модернизации путем добавления новых и расширения указанных в рамках настоящего ТЗ инфраструктур, систем, отраслей, в частности, должны быть выработаны предложения по запуску организации тестирования программного обеспечения организаций в сфере связи на базе Киберполигона («Телеком-киберполигон») в целях импортозамещения, проведения киберучений и практической подготовки сотрудников информационной безопасности компаний в сфере связи, тестирования программного обеспечения на безопасность и отсутствие недекларированных возможностей.

3.13.2Организационная, техническая и методическая инфраструктура Киберполигона должна обеспечивать возможность обеспечения взаимоувязанных отраслевых Киберполигонов и межотраслевых киберучений.

3.13.3Организационная, техническая и методическая инфраструктура Киберполигона должна предусматривать возможность масштабирования по производительности путем модернизации используемых аппаратных или выделяемых виртуальных платформ. Используемое программное обеспечение также должно поддерживать возможности по масштабированию, в том числе, с использованием облачных технологий.

3.13.4В рамках проведения работ необходимо обеспечить проведение исследований для определения перечня внешних систем, с которыми должно быть организовано межсистемное взаимодействие в рамках задач, выполняемых Киберполигоном, в том числе, с Банком данных угроз безопасности информации ФСТЭК России.

4 Показатели результативности, состав и содержание работ по созданию и функционированию Киберполигона

4.1 Показатели результативности, наименование этапов и сроки выполнения работ с момента заключения Соглашения о предоставлении субсидии представлены в таблице 1.

Таблица 1 – Показатели результативности, состав и содержание работ по созданию и функционированию Киберполигона

№	Наименование этапов работ	Результат	Срок
1	Создан 1 (один) киберполигон для не менее 2 (двух) ИТ-инфраструктур, эмулирующих корпоративные сети организаций кредитно-финансовой сферы Российской Федерации («ИТ-киберполигон»)	ИТ-киберполигон создан и функционирует, Отчёт	24 мес.
1.1	Разработано частное техническое задание	Отчёт	2 мес.
1.2	Разработан эскизный проект	Отчёт	4 мес.
1.3	ИТ-киберполигон введён в опытную эксплуатацию	Акт о вводе в опытную эксплуатацию	11 мес.
1.4	ИТ-киберполигон введён в промышленную эксплуатацию	Акт о вводе в промышленную эксплуатацию	24 мес.
2	Проведена тренировка не менее 30 (тридцати) учащихся, специалистов, экспертов и руководителей современным практикам обеспечения информационной безопасности, за исключением сотрудников Получателя субсидии	Отчёт	12 мес.
3	Проведено не менее 1 (одного) кибер-учения или соревнования по информационной безопасности	Отчёт	12 мес.
4	Разработан план мероприятий (дорожная карта) по развитию Киберполигона на 2020-2024 гг.	План мероприятий (дорожная карта), Отчёт	6 мес.
5	Разработана методическая и методологическая основа для функционирования Киберполигона	Комплект методической документации, Отчёт	8 мес.
6	Создан 1 (один) киберполигон для не менее 1 индустриальной инфраструктуры (АСУ ТП или систем Промышленного интернета) электроэнергетического	Индустриальный киберполигон создан и	24 мес.

№	Наименование этапов работ	Результат	Срок
	сектора («Индустриальный киберполигон»)	функционирует, Отчёт	
6.1	Разработано частное техническое задание	Отчёт	4 мес.
6.2	Разработан эскизный проект	Отчёт	6 мес.
6.3	Индустриальный киберполигон введён в опытную эксплуатацию	Акт о вводе в опытную эксплуатацию	12 мес.
6.4	Индустриальный киберполигон введён в промышленную эксплуатацию	Акт о вводе в промышленную эксплуатацию	24 мес.
7	Проведена тренировка не менее 150 (ста пятидесяти) учащихся, специалистов, экспертов и руководителей современным практикам обеспечения информационной безопасности и противодействия компьютерным атакам, за исключением сотрудников Получателя субсидии	Отчёт	12 мес.
8	Проведено не менее 6 (шести) кибер-учений или соревнований по информационной безопасности	Отчёт	12 мес.
9	Создано не менее 2 (двух) Центров Киберполигона в партнёрстве с организациями высшего профессионального образования Российской Федерации, в том числе, 1 (один) центр на базе Центра Цифрового Развития Дальневосточного федерального университета	Отчёт	12 мес.
10	Проведено не менее 3 (трёх) соревнований по поиску уязвимостей и тестированию программного обеспечения на защищённость по инициативе правообладателя в Российской Федерации	Отчёт	12 мес.
11	Проведена тренировка не менее 150 (ста пятидесяти) учащихся, специалистов, экспертов и руководителей современным практикам обеспечения информационной безопасности и противодействия компьютерным атакам, за исключением сотрудников Получателя субсидии	Отчёт	24 мес.
12	Проведено не менее 12 (двенадцати) кибер-учений или соревнований по информационной безопасности (накопительно)	Отчёт	24 мес.
13	Создано не менее 4 (четырёх) Центров Киберполигона в партнёрстве с организациями высшего профессионального образования Российской Федерации (накопительно)	Отчёт	24 мес.
14	Проведено не менее 12 (двенадцати) соревнований по поиску уязвимостей и тестированию программного	Отчёт	24 мес.

№	Наименование этапов работ	Результат	Срок
	обеспечения на защищённость по инициативе правообладателя на площадке Киберполигона в Российской Федерации (накопительно)		

4.2 В ходе создания Киберполигона должны осуществляется следующие работы:

– эскизное и/или техническое проектирование;

– проведение закупки программного и аппаратного обеспечения, в том числе, в сервисной модели;

– проведение ремонтных, монтажных и пусконаладочных работ:

а) создание необходимых подразделений и рабочих мест;

б) подготовка площадки внедрения к развертыванию технической инфраструктуры Киберполигона;

в) проверка комплектности программно-технических компонентов Киберполигона;

г) монтаж и установка технической инфраструктуры Киберполигона;

д) настройка технической инфраструктуры Киберполигона для обеспечения выполнения предъявляемых к ней требований и функций.

4.3 В ходе эскизного проектирования должны быть разработаны следующие документы:

– эскизный проект.

4.4 В ходе технического проектирования должны быть разработаны следующие документы:

– ведомость технического проекта;

– пояснительная записка;

– схема структурная комплекса технических средств;

– руководство пользователя;

– инструкция по эксплуатации.

4.5 В ходе разработки методической и методологической основы для функционирования Киберполигона должны быть разработаны:

– методические материалы, принципы и порядок организации и проведения, сценарии, оценки эффективности практической подготовки при проведении киберучений и соревнований по информационной безопасности;

– методические материалы, принципы и порядок использования пользователями инфраструктуры Киберполигона в целях тестирования программного обеспечения и элементов информационных систем;

– проекты правовых и распорядительных документов по организации и проведению мероприятий, в том числе, проведению киберучений, практических соревнований, практической подготовке слушателей Киберполигона, тестированию программного обеспечения с учётом отраслевой специфики;

– формы отчётных документов по результатам проведенных мероприятий, в том числе, проведению киберучений, практических соревнований, практической подготовке слушателей Киберполигона, тестированию программного обеспечения, продвижению Киберполигона.

4.6 В ходе разработки плана мероприятий (дорожной карты) по развитию Киберполигона на 2020-2024 гг. должны быть разработаны:

– предложения и мероприятия по развитию отраслевых центров Киберполигона, поддержке типовых инфраструктур предприятий различных отраслей экономики Российской Федерации;

– предложения и мероприятия по развитию функциональных возможностей Киберполигона;

– предложения и мероприятия по обеспечению взаимодействия отраслевых Киберполигонов и проведению межотраслевых киберучений.

4.7 В ходе создания и функционирования Киберполигона в 2019-2021 гг. должно быть обеспечено продвижение Киберполигона, в том

числе, посредством участия Исполнителя в отраслевых мероприятиях и конференциях по информационной безопасности.

5 Порядок контроля и приемки Киберполигона

5.1 В приемке работ участвуют Заказчик и Исполнитель.

5.2 Приемка работ осуществляется поэтапно в сроки и объёме, указанных в 4.1.

5.3 Предоставление результатов работ при создании и обеспечении функционирования Киберполигона осуществляется в соответствии с Правилами предоставления субсидии.

6 Требования к составу и содержанию работ по подготовке Киберполигона к вводу системы в действие

6.1 Исполнитель должен разработать перечень основных мероприятий и их исполнителей, которые следует выполнить при подготовке и вводу Киберполигона в действие, в том числе, в части продвижения Киберполигона на рынке РФ.

6.2 В перечень основных мероприятий должны быть включены:

– создание условий функционирования Киберполигона, при которых гарантируется соответствие Киберполигона требованиям ТЗ;

– создание необходимых для функционирования Киберполигона подразделений и служб;

– сроки и порядок комплектования штатов и обучения персонала Киберполигона.

Перечень принятых сокращений

АСТУ	–	Автоматизированные системы технологического управления
АСУ ТП	–	Автоматизированная система управления технологическим процессом
ИБ	–	Информационная безопасность
ИТ	–	Информационные технологии
КИИ	–	Критическая информационная инфраструктура
РФ	–	Российская Федерация
СЗИ	–	Средство защиты информации
ТЗ	–	Техническое задание
ФЗ	–	Федеральный закон
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭВМ	–	Электронно-вычислительная машина

Перечень принятых терминов

Киберучения	–	процесс практической подготовки и освоения навыков у учащихся, специалистов, экспертов и руководителей по обеспечению информационной безопасности путем моделирования компьютерных атак и отработки реакций на них
Киберполигон	–	инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них