Описание объекта закупки на выполнение комплекса услуг по реализации организационных мер защиты информации в Негосударственном учреждении здравоохранения «Отделенческая клиническая больница на станции Минеральные Воды открытого акционерного общества «Российские железные дороги»

1 Перечень принятых сокращений и обозначений

КИИ	Критическая информационная инфраструктура
АРМ	Автоматизированное рабочее место
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю (прежнее название – Гостехкомиссия России)
ФЗ	Федеральный закон
PDF	Portable Document Format

2 Правовые основания оказываемых услуг

Комплекс услуг по защите информации осуществляется во исполнение требований нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативно-правовой документации Российской Федерации в области защиты информации, в том числе Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.

3 Исходные данные об объектах информатизации Заказчика

Объекты информатизации Заказчика находятся по следующим адресам:

- 357207, Ставропольский край, г. Минеральные воды, ул. Советская,61;

Обособленные подразделения:

- 355008, Ставропольский край, г. Ставрополь, ул. Войтика,2а;
- 355118, Ставропольский край, г. Невинномысск, ул. Кооперативная,174.

4 Требования к оказанию услуг

4.1 Общие требования

Комплекс услуг должен выполняться в соответствии с требованиями Постановления Правительства РФ от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», а также требованиями нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативно-правовой документации Российской Федерации в области защиты информации.

4.1 Требования к реализации организационных мер защиты информации

4.1.1 Требования к составу организационных мер защиты информации

Состав организационных мер защиты информации должен включать в себя:

- сбор сведений об объекте критической информационной инфраструктуры;
- автоматизацию процессов управления информационной безопасностью;
- категорирование объекта критической информационной инфраструктуры.

4.1.2 Требования к сбору сведений об объекте критической информационной инфраструктуры

В процессе сбора сведений об объекте критической информационной инфраструктуры Исполнитель должен осуществить:

- определение процессов;
- выявление критических процессов;

– определение объектов критической информационной инфраструктуры;
– формирование перечня объектов критической информационной инфраструктуры;
– сбор исходных данных об объекте критической информационной инфраструктуры.

В рамках определения процессов Заказчик, совместно с Исполнителем, определяет управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры.

При выявлении критических процессов Исполнитель, на основании оценки данной Заказчиком, выявляет процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

После определения критических процессов Исполнитель должен определить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов и сформировать перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Сбор исходных данных об объекте критической информационной инфраструктуры должен включать в себя:

– сбор сведений об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

- сбор сведений о процессах, которые обеспечивают управленческие, технологические, производственные, финансово- экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры;
- состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;
- сбор сведений о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объектов критической информационной инфраструктуры от других таких объектов.

4.1.3 Требования к автоматизации процессов сопровождения и разработки документации, регламентирующей защиту информации

4.1.3.1 Общие сведения

Исполнитель должен организовать автоматизацию процессов управления информационной безопасностью, включающую в себя:

- самостоятельное сопровождение Заказчиком комплекта документации, регламентирующей защиту информации (корректировка разработанного комплекта документации при изменении условий обработки защищаемой информации или иных параметров, влияющих на содержание комплекта документации);
- самостоятельную разработку Заказчиком новых комплектов документации для вновь вводимых объектов защиты информации (ИСПДн, ГИС, СКЗИ);

– отслеживание изменений в нормативно-методической документации ФСТЭК России, ФСБ России, действующей нормативно-правовой документации Российской Федерации в области защиты информации и автоматическое изменение содержания документации, регламентирующей защиту информации;
– управление активами и мероприятиями информационной безопасности.

4.1.3.2 Требования к методам автоматизации

Автоматизация процессов управления информационной безопасностью, должна быть реализована посредством приложения, передаваемого Исполнителем Заказчику.

Исполнитель должен выполнить настройку и подготовить приложение к дальнейшему использованию Заказчиком, путем ввода данных, полученных в ходе сбора сведений о порядке обработки защищаемой информации и используемых при разработке комплекта документов.

4.1.3.3 Требования к сроку функционирования приложения

Передаваемое Исполнителем Заказчику приложение должно бесперебойно функционировать в течение двенадцати месяцев с момента заключения государственного контракта. Исполнителем должна быть предусмотрена возможность пролонгации использования приложения без потери имеющихся данных в течение двенадцати месяцев после завершения срока использования.

4.1.3.4 Требования к функциям приложения

Приложение должно выполнять следующие функции:
– разработка и сопровождение документации по информационной безопасности;
– учет активов информационной безопасности;

- управление мероприятиями по информационной безопасности;
- управление задачами по информационной безопасности;
- повышение осведомленности и контроль знаний сотрудников в области информационной безопасности;
- анализ показателей эффективности информационной безопасности;
- наличие календаря событий;
- управление инцидентами информационной безопасности;
- учет и сопровождение объектов критической информационной инфраструктуры;
- организация процесса технической поддержки Заказчика.

4.1.3.5 Требования к разработке и сопровождению документации по информационной безопасности

4.1.3.5.1 Требования к составу разрабатываемой документации по информационной безопасности

Приложение должно обеспечивать разработку и сопровождение документации по следующим направлениям:

- нормативно-распорядительная документация по обработке и защите персональных данных и государственных информационных систем;
- нормативно-распорядительная документация для средств криптографической защиты информации;
- модели угроз безопасности и модели нарушителя;
- политика конфиденциальности для веб-сайта Заказчика;
- управление информационной безопасностью;
- организационно-распорядительная документация объектов критической информационной инфраструктуры.

Приложение должно содержать видеоинструкцию и страницу руководства по работе с функционалом разработки и сопровождения документации в HTML-формате.

4.1.3.5.2 Общие требования к разработке документации по информационной безопасности

Приложение должно позволять осуществлять разработку и сопровождение документации по информационной безопасности, обеспечивающей выполнение комплекса требований нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативно-правовой документации Российской Федерации в области защиты информации, а также выполнять следующие функции:

- интеграция с пакетом офисных программ Microsoft Office в части загрузки массивов данных в приложение;
- отображение статуса готовности каждого документа и перечня данных, необходимых для окончательной подготовки документа;
- адаптация документов типа «Приказ», для печати на бланке Заказчика;
- настройка документов типа «Приказ»: указание автора, составителя и согласующих проект приказа лиц; замена предыдущего приказа новым;
- автоматический подбор падежей слов, вносимых сведений;
- выгрузка документов в формате приложения Microsoft Word;
- выгрузка пакета документов в формате приложения Microsoft Word в одном архиве.

4.1.3.5.3 Требования к разработке и сопровождению нормативно-распорядительной документации по обработке и защите персональных данных и государственных информационных систем

Перечень разрабатываемой и сопровождаемой приложением нормативно-распорядительной документации по обработке и защите персональных данных должен включать в себя:

- Акт установления уровня защищенности информационных систем персональных данных;

- Журнал регистрации запросов граждан;
- Журнал регистрации обращений граждан;
- Заключение об оценке вреда субъектам персональных данных;
- Инструкция об осуществлении контроля;
- Инструкция по допуску лиц в помещения где ведется обработка персональных данных;
- Инструкция по учёту машинных носителей и регистрации их выдачи;
- Отзыв согласия субъекта персональных данных;
- Перечень информационных систем персональных данных;
- План внутренних проверок состояния защиты персональных данных;
- План мероприятий по защите персональных данных;
- Политика обработки персональных данных;
- Положение об ответственном за организацию обработки персональных данных;
- Положение о порядке обработки персональных данных;
- Положение по работе с инцидентами информационной безопасности;
- Приказ об ответственности за обработку и защиту персональных данных;
- Приказ об установлении границ контролируемой зоны;
- Приказ об утверждении мест хранения материальных носителей;
- Приказ об утверждении типового обязательства работника о неразглашении персональных данных субъектов персональных данных;
- Приказ об утверждении типовой формы поручения обработки персональных данных;

- Приказ об утверждении типовой формы разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
- Приказ об утверждении форм актов уничтожения персональных данных;
- Приказ об утверждении форм согласий;
- Приказ о допуске лиц в помещения с СКЗИ;
- Приказ о журнале ознакомления работников;
- Приказ о журнале регистрации инцидентов информационной безопасности;
- Приказ о назначении ответственного за организацию обработки персональных данных;
- Приказ о создании комиссии по работе с инцидентами информационной безопасности;
- Приказ о создании комиссии по установлению уровня защищенности персональных данных в информационных системах персональных данных;
- Уведомление об обработке персональных данных;
- Модель угроз и нарушителя.

Опционально должна быть предусмотрена возможность разработки следующих документов, в зависимости от условий обработки персональных данных:

- Акт классификации государственной информационной системы или муниципальной информационной системы;
- Приказ о журнале учёта проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля;
- Приказ о журнале учета посетителей.

К разрабатываемым и сопровождаемым приложением нормативно-распорядительным документам по обработке и защите персональных данных должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документа.

4.1.3.5.4 Требования к разработке и сопровождению нормативно-распорядительной документации для средств криптографической защиты информации

Приложение должно осуществлять разработку и сопровождение нормативно-распорядительной документации для средств криптографической защиты информации, обеспечивающей выполнение комплекса требований нормативно-методической документацией ФСБ России и действующей нормативной-правовой документации Российской Федерации в области эксплуатации средств криптографической защиты информации, а также выполнять следующие функции:

- проведение инструктажа пользователей о работе со средствами криптографической защиты информации;
- организация проведения тестирования пользователей по результатам инструктажа о работе со средствами криптографической защиты информации;
- проведение инструктажа и тестирования с использованием веб-браузера на личном автоматизированном рабочем месте пользователя;
- разработка заключений о возможности эксплуатации средств криптографической защиты информации и заключений о допуске пользователей средств криптографической защиты информации по результатам инструктажа и проведения зачетов.

Перечень разрабатываемой и сопровождаемой приложением нормативно-распорядительной документации для средств криптографической защиты информации должен включать в себя:

- Схема организации криптографической защиты конфиденциальной информации;
- Приказ о назначении ответственного пользователя СКЗИ;
- Приказ о допуске пользователей к работе со средствами криптографической защиты информации;
- Заключение о возможности эксплуатации средств криптографической защиты информации;
- Заключение о допуске пользователей средств криптографической защиты информации;
- Протокол зачета пользователей;
- План проведения проверок за соблюдением условий использования средств криптографической защиты информации;
- Правила доступа в помещения, в которых ведется эксплуатация средств криптографической защиты информации;
- Функциональные обязанности ответственного пользователя;
- Акт уничтожения ключевого документа;
- Журнал пользователей сети;
- Журнал поэкземплярного учёта средств криптографической защиты информации;
- Журнал учета опломбирования;
- Технический (аппаратный) журнал;
- Приказ о допуске лиц в помещения с СКЗИ;
- Годовой отчет в орган криптографической защиты об уничтоженной ключевой информации.

Опционально должна быть предусмотрена возможность разработки следующих документов, в зависимости от условий эксплуатации средств криптографической защиты информации:

- Журнал учета хранилищ средств криптографической защиты информации и ключей к ним;

- Журнал проверок исправности сигнализации;
- Лицевой счет.

Информация об эксплуатации средств криптографической защиты информации, необходимая для подготовки документов должна учитывать сведения о следующих активах информационной безопасности:

- средства криптографической защиты информации;
- сертификаты соответствия имеющихся средств криптографической защиты информации требованиям безопасности информации;
- технические средства на которых эксплуатируются средства криптографической защиты информации.

К разрабатываемым и сопровождаемым приложением нормативно-распорядительным документам для средств криптографической защиты информации должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документа.

4.1.3.5.5 Требования к разработке и корректировке моделей угроз безопасности и моделей нарушителя

Приложение должно осуществлять разработку и корректировку моделей угроз безопасности и моделей нарушителя, обеспечивающих выполнение комплекса требований нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативной-правовой документации Российской Федерации в области защиты информации, а также выполнять следующие функции:

- наличие перечня актуальных угроз безопасности, в том числе приведенных в банке данных угроз безопасности ФСТЭК России;
- определение уровня защищенности информационной системы персональных данных и класса защиты государственной информационной системы на основании данных имеющихся в приложении;

- оценка исходной защищенности и степени выполнения защитных мер;
- наличие технической анкеты для определения особенностей функционирования системы и исключения угроз безопасности, не имеющих предпосылки;
- выгрузка модели угроз в формате Microsoft Word, для каждой информационной системы;
- возможность создания единой модели угроз безопасности для всех информационных систем заказчика.

4.1.3.5.6 Требования к разработке и корректировке политики конфиденциальности для веб-сайта Заказчика

Приложение должно осуществлять разработку и корректировку политики конфиденциальности для веб-сайта Заказчика. При подготовке документа должна учитываться следующая информация:

- общие сведения о веб-сайте:
  - наименование;
  - адрес;
  - раздел с контактной информацией;
- цели обработки данных пользователя веб-сайта;
- группы обрабатываемой информации;
- сведения о публикации персональных данных на веб-сайте;
- сведения о передаче информации третьим лицам:
  - наименование третьего лица;
  - описание случая передачи информации;
  - отметка об осуществлении трансграничной передачи информации;
- сведения о сроке хранения данных;
- сведения о месте размещения серверов веб-сайта;
- принимаемые меры защиты данных на веб-сайте;
- наличие/отсутствие оплаты услуг и сервисов веб-сайта.

4.1.3.5.7 Требования к разработке организационно-распорядительной документации объекта критической информационной инфраструктуры

Перечень разрабатываемой и сопровождаемой приложением организационно-распорядительной документации объекта критической информационной инфраструктуры должен включать в себя:

- Приказ о создании комиссии по категорированию объектов критической информационной инфраструктуры;
- Заключение о формировании перечня объектов КИИ;
- Перечень объектов критической информационной инфраструктуры;
- Акт категорирования объектов критической информационной инфраструктуры;
- Уведомление ФСТЭК России о результатах категорирования объектов критической информационной инфраструктуры;
- Приказ об ответственности за обеспечение безопасности объектов критической информационной инфраструктуры.

К разрабатываемой и сопровождаемой приложением организационно-распорядительной документации объекта критической информационной инфраструктуры должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документов.

4.1.3.6 Требования к учету активов информационной безопасности

Приложением должны обеспечиваться следующие функции по учету активов:

- учет информационных систем персональных данных;
- учет государственных информационных систем;
- учет аттестатов соответствия информационных систем требованиям безопасности информации;

- учет средств защиты информации с указанием реализуемых подсистем информационной безопасности;
- учет знаков и сертификатов соответствия имеющихся средств защиты информации требованиям безопасности информации;
- учет действующих лицензий на право использования средств защиты информации;
- учет технических средств с указанием принадлежности к информационным системам;
- объединение технических средств в логические группы;
- учет лиц, ответственных за эксплуатацию технических средств;
- учет лиц, ответственных за информационную безопасность;
- учет сведений об обучении и стаже в области информационной безопасности ответственных лиц.

Приложение должно содержать видеоинструкцию и страницу руководства по работе с функционалом учета активов в HTML-формате.

Приложением должен обеспечиваться функционал по управлению информацией о сотрудниках, включающей в себя:

- учет перечня должностей сотрудников;
- импорт перечня сотрудников из файла;
- учет перечня сотрудников;
- быстрый выбор сотрудников из перечня при назначении лиц, ответственных за мероприятия по информационной безопасности или при допуске сотрудников к защищаемой информации, хранилищам и помещениям;
- просмотр истории инструктажей и тестировании по вопросам информационной безопасности пройденных сотрудником;
- просмотр информации об обучении сотрудника по вопросам информационной безопасности и стаже в области информационной безопасности.

Приложение должно обеспечивать возможность указать следующую информацию о сотруднике:

- должность;
- подразделение;
- фамилию, имя и отчество;
- контактную информацию (адрес электронной почты).

Приложение должно содержать видеоинструкцию страницу руководства по работе с функционалом управления информацией о сотрудниках в HTML-формате.

4.1.3.7 Требования к управлению мероприятиями по информационной безопасности

Приложением должны обеспечиваться автоматическая загрузка базы возможных мероприятий по информационной безопасности из предустановленного в приложении набора, включающего в себя:

- мероприятия по общей информационной безопасности;
- мероприятия по порядку обработки и защиты персональных данных;
- мероприятия по порядку эксплуатации средств криптографической защиты информации;
- мероприятия по организации обеспечения безопасности объектов КИИ.

Информация о мероприятиях по информационной безопасности должна включать:

- наименование мероприятия;
- описание мероприятия;
- плановый срок выполнения мероприятия;
- информация об обязательности мероприятия (рекомендуемые мероприятия);
- пояснение по выполнению мероприятия;

– тема мероприятия;
– группы мероприятия;
– информацию о лице, ответственном за выполнение мероприятия;
– статус;
– отчет о выполнении мероприятия;
– свидетельства выполнения мероприятия – прикрепленные файлы.

Список доступных мероприятий должен поддерживать фильтрацию полям: «группы мероприятия», «тема мероприятия», «эталонность мероприятия» и «вес мероприятия».

Приложение должно содержать видеоинструкцию и страницу руководства по работе с функционалом управления мероприятиями по информационной безопасности в HTML-формате.

4.1.3.8 Требования к управлению задачами по информационной безопасности

Приложением должны обеспечиваться следующие возможности управлению задачами по информационной безопасности:

– назначение задач сотрудникам из числа указанных в приложении;
– назначение задач группам сотрудников из числа указанных в приложении;
– отправка сотрудникам уведомлений о назначении задачи;
– фильтрация задач по категории, статусу и приоритету;
– поиск задач по теме;
– изменение свойств задач и добавление отчётов.

Назначаемые сотрудникам задачи должны включать в себя следующую информацию:

– тема;
– дата завершения;
– исполнитель или группа исполнителей;

– статус;
– приоритет;
– описание задачи;
– отчёт о выполнении задачи.

В приложении для назначенных задач должна обеспечиваться возможность установления связи с зарегистрированными инцидентами информационной безопасности.

В приложении для назначенных задач должна обеспечиваться возможность добавлять вложения в виде одного или нескольких файлов.

4.1.3.9 Требования к повышению осведомленности и контролю знаний сотрудников в области информационной безопасности

Приложением должны обеспечиваться следующие возможности по повышению осведомленности по вопросам информационной безопасности:

– назначение сотрудникам онлайн-инструктажей из числа доступных в приложении;
– тестирование сотрудника по результатам прохождения онлайн-инструктажа;
– назначение сотрудникам отдельных тестов из числа доступных в приложении;
– уведомление сотрудников, контактные адреса которых указаны в справочнике, о необходимости прохождения онлайн-инструктажа или теста;
– генерация уникальных ссылок на онлайн-инструктажи или тесты для отдельных сотрудников;
– электронный журнал проведенных онлайн-инструктажей и тестов сотрудников.

Результаты тестирования должны определяться автоматически для тестов, снабженных критериями оценки. Для тестов без установленных

критериев оценки должна быть предусмотрена возможность ручного определения результатов тестирования автором теста.

Приложением должны предоставляться онлайн инструктажи и тесты по следующим темам:

- персональные данные;
- эксплуатация средств криптографической защиты информации (СКЗИ);
- фишинг и другие актуальные угрозы ИБ для пользователей.

Приложением должна обеспечиваться возможность создания инструктажей, оформленных во встроенном редакторе, в том числе содержащих:

- тексты;
- рисунки;
- видеоматериалы.

Приложением должна обеспечиваться возможность создания тестов, содержащих следующую информацию:

- название теста;
- тема;
- общее количество вопросов;
- количество задаваемых вопросов;
- процент правильных ответов для успешного прохождения;
- пояснение к тесту, отображаемое работнику;
- вопросы теста;
- варианты ответов на вопросы теста.

Приложение должно содержать видеоинструкцию и страницу руководства по работе с функционалом повышения осведомленности и контроля знаний сотрудников в области информационной безопасности в HTML-формате.

4.1.3.10 Требования к анализу показателей эффективности информационной безопасности

Приложением должна быть обеспечена возможность представления информации о состоянии информационной безопасности в организации, а также об эффективности использования приложения.

В качестве критериев эффективности использования приложения должны выступать:

- сводный показатель эффективности работы;
- дата последнего входа пользователей в приложение;
- дата последнего изменения параметров документов.

Приложением должна быть обеспечена возможность представления информации о степени соответствия организации информационной безопасности требованиям законодательства РФ в интерфейсе приложения с учетом критериев оценки.

В качестве критериев оценки степени соответствия организации информационной безопасности требованиям законодательства РФ должны выступать:

- степень готовности документов;
- степень актуальности документов (готовность документов с учетом срока их актуальности);
- степень выполнения мероприятий по информационной безопасности в организации.

Приложение должно обеспечить отображение состояния каждого критерия с помощью цветовой индикации, а также текстовой и/или табличной информации.

Приложение должно обеспечить отображение подробного отчета, содержащего информацию о готовности каждого отдельного документа или выполнении каждого назначенного мероприятия.

4.1.3.11 Требования к календарю событий

Приложением должны обеспечиваться следующие возможности календаря событий, связанных с информационной безопасностью:

- просмотр календаря за день, неделю, месяц;
- добавление новых событий с указанием наименования, даты начала, даты окончания и даты уведомления.

4.1.3.12 Требования к управлению инцидентами информационной безопасности

Приложением должны обеспечиваться следующие возможности по управлению инцидентами информационной безопасности:

- регистрация инцидента пользователем Приложения с составлением описания инцидента;
- возможность прикладывать файлы, содержащие свидетельства инцидента, размером не более 25 Мегабайт;
- организация реагирования на инциденты с помощью назначения задач сотрудникам и группам сотрудников;
- установление связи с активами информационной безопасности;
- указание внешних источников инцидентов при их наличии;
- указание заключения по инциденту;
- просмотр журнала инцидента;
- просмотр текущей информации по инциденту;
- скачивание паспорта инцидента;
- просмотр сводной информации по инцидентам.

Информация об инцидентах информационной безопасности должна включать:

- описание инцидента со следующими данными:
  - номер инцидента (идентификатор);

- заголовок инцидента;
- теги инцидента;
- тип инцидента;
- организация, в которой произошел инцидент;
- описание;
- дата, когда произошел инцидент;
- плановая дата реагирования на инцидент;
- группа информирования;
- информация об основном ответственном лице или группе исполнителей;
- уровень критичности инцидента;
- уровень конфиденциальности;
- источник;
- ранее принятые меры оперативного реагирования на инцидент;
- описание иных объектов;
- меры по недопущению подобных инцидентов;

- свидетельства инцидента в виде файлов вложений;
- задачи сотрудникам или группам сотрудников, связанные с реагированием на инциденты с возможностью их поиска по теме и исполнителю;
- связи с активами информационной безопасности, включающими:
  - технические средства;
  - группы ТС;
  - ГИС;
  - ИСПДн;
  - СЗИ;
  - работники;
  - связь с другими инцидентами;

- внешние источники инцидента со следующими данными:
  - IP;
  - URL;
  - описание;
- заключение по инциденту со следующими данными:
  - статус (отклонен, ложное срабатывание, подтвержден);
  - ущерб от подтвержденного инцидента;
- события в журнале инцидента, связанные с его изменениями.

4.1.3.13 Требования к учету и сопровождению объектов критической информационной инфраструктуры

4.1.3.13.1 Общие сведения

Приложением должен быть обеспечен учет и сопровождение объектов критической информационной инфраструктуры в соответствии с требованиями Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ и определен Постановлением Правительства РФ от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Целью учета и сопровождения объектов критической информационной инфраструктуры является категорирование и поддержание в актуальном состоянии сведений об объектах критической информационной инфраструктуры.

Учет и сопровождение объектов критической информационной инфраструктуры должен охватывать следующие сущности:

- управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций

(полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

- объекты критической информационной инфраструктуры;
- сети связи, используемые организацией;
- ответственные лица.

Приложение должно содержать видеоинструкцию и страницу руководства по работе с функционалом учета и сопровождения объектов критической информационной инфраструктуры в HTML-формате.

4.1.3.13.2 Требования к учету и сопровождению процессов

Приложением должен быть обеспечен учет управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры.

Приложением должна быть обеспечена возможность создания процессов с указанием наименований и выбора параметра, указывающего на принадлежность процесса к сфере критической информационной инфраструктуры.

Для каждого процесса должен быть доступен модуль оценки возможного ущерба, включающий двадцать один критерий, разделенный на пять логических блоков:

- социальная значимость;
- политическая значимость;
- экономическая значимость;
- экологическая значимость;
- значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Каждый критерий должен включать четыре варианта значений, отражающих категорию значимости, доступных для выбора пользователем.

Приложением должно обеспечиваться автоматическое определение критического процесса в соответствии с проводимой оценкой возможного ущерба.

4.1.3.13.3 Требования учету и сопровождению информационных систем

Приложением должен быть обеспечен учет объектов критической информационной инфраструктуры (далее – информационная система), включающий возможность хранения и редактирования следующих данных:

- основные данные об информационной системе:
  - наименование информационной системы;
  - назначение информационной системы;
  - принадлежность к объекту критической информационной инфраструктуры;
  - отметка об использовании стороннего центра обработки данных (ЦОД);
  - отметка о наличии сторонних организаций, эксплуатирующих объект КИИ;
- адреса и состав размещения объекта:
  - наименование и адрес организации / филиала;
  - используемые ОС;
  - используемое прикладное ПО;
  - используемые сети связи;
  - технические средства;
- адрес и состав размещения ЦОД (при наличии):
  - адрес размещения ЦОД;
  - используемые ОС;
  - используемые сети связи;
  - технические средства;

- сторонние организации в ОКИИ:
  - сторонняя организация, эксплуатирующая объект КИИ;
  - тип технического средства;
- структурно-функциональные характеристики:
  - тип системы;
  - архитектура системы;
- нарушители и угрозы в КИИ:
  - отметка о наличии нарушителей, являющихся источником компьютерных атак на данную систему;
  - нарушители безопасности информации (при их наличии);
  - обоснование отсутствия нарушителя безопасности (при его отсутствии);
  - отметка о наличии актуальных угроз компьютерных атак на данную систему;
  - основные угрозы безопасности информации (при их наличии);
  - обоснование отсутствия актуальных угроз (при их отсутствии);
  - возможные типы компьютерных инцидентов (при их наличии);
  - обоснование отсутствия возможности компьютерных инцидентов (при их отсутствии);
  - степень возможного ущерба;
- защитные меры:
  - принятые организационные мероприятия;
  - принятые меры защиты информации;
  - используемые СЗИ;
- КИИ:
  - сфера деятельности;
  - планируемый срок категорирования;
  - критические процессы, обеспечиваемые системой;

- итоговая категория значимости;
- обоснования значений показателей критериев значимости или их неприменимости;
- значения показателей значимости объекта критической информационной инфраструктуры;
- обоснования значений показателей критериев значимости или их неприменимости.

4.1.3.13.4 Требования учету и сопровождению сетей связи организации

Приложением должен быть обеспечен учет сетей связи, используемых при взаимодействии объектов критической информационной инфраструктуры, включающий возможность хранения и редактирования следующих данных:

- наименование сети связи;
- категория сети связи;
- наименование оператора сети;
- цель взаимодействия информационных систем с сетью;
- тип взаимодействия;
- используемые технологии и протоколы.

4.1.3.13.5 Требования к управлению ответственностью в области обеспечения безопасности критической информационной инфраструктуры

Приложением должна быть обеспечена возможность определения и учета ответственных лиц, принимающих участие в процессе категорирования и обеспечения безопасности объектов критической информационной инфраструктуры, включающая возможность хранения и редактирования данных о следующих ответственных лицах:

– лицо уполномоченное на организацию безопасности объектов критической информационной инфраструктуры;
– члены комиссии по категорированию объектов критической информационной инфраструктуры;
– лицо ответственное за взаимодействие с государственными регуляторами по вопросам категорирования объектов критической информационной инфраструктуры.

Сведения об ответственных лицах должны включать:

– фамилию, имя, отчество;
– структурное подразделение организации;
– должность.

Функционал Приложения должен обеспечить возможность назначения ответственности за организацию безопасности объектов критической информационной инфраструктуры, как на отдельных сотрудников, так и структурное подразделение.

4.1.3.14 Требования к организации процесса технической поддержки

4.1.3.14.1 Общие сведения

Техническая поддержка приложения должна включать в себя:

– консультирование по вопросам входа в сервис, смены пароля;
– консультирование по вопросам использования сервиса (очередность выполнения мероприятий, внесение корректных данных для подготовки документации и т.п.);
– предоставление информационных материалов по работе с системой;
– обеспечение стабильной работы сервиса;
– устранение технических ошибок в работе сервиса;
– предоставление обновлений шаблонов документов в соответствии с изменениями законодательства РФ и требований регуляторов по ИБ.

Техническая поддержка должна оказываться по телефону, электронной почте, а также с помощью встроенного функционала по приему обращений.

Функционал приложения должен позволять пользователям создавать обращения в техническую поддержку и отслеживать ход их исполнения. Должна быть возможность добавлять к обращению снимки экрана в форматах файлов .jpg, .jpeg, .png.

Приложение должно позволять организовывать онлайн обмен сообщениями между специалистами Заказчика и Исполнителя по вопросам технической и консультационной поддержки при использовании приложения.

Приложение должно позволять проводить оценку исполнения заявки в техническую поддержку.

4.1.3.15 Технические характеристики приложения

Приложение должно иметь клиент-серверную архитектуру, не требовать установки на АРМ и сервера Заказчика и функционировать в любом современном веб-браузере. Серверная часть должна располагаться на мощностях Исполнителя и функционировать не менее 24 часов, 7 дней в неделю. Время отклика приложения должно составлять не более 3 секунд, а время простоя в случае форс-мажорных обстоятельств не должно превышать 60 минут. При возникновении форс-мажорных обстоятельств Заказчик должен быть уведомлен о недоступности приложения по электронной почте.

Исполнитель должен принимать перечень организационных и технических мер в соответствии с требованиями нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативно-правовой документации Российской Федерации в области защиты информации для обеспечения безопасности хранимой информации о Заказчике.

Исполнитель должен подтвердить выполнение перечня организационных и технических мер в соответствии с требованиями нормативно-методической документации ФСТЭК России, ФСБ России и

действующей нормативно-правовой документации Российской Федерации в области защиты информации действующим аттестатом соответствия, выданным организацией, имеющей лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации (аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации).

4.1.4 Требования к категорированию объектов критической информационной инфраструктуры

В процессе категорирования объектов критической информационной инфраструктуры Исполнитель должен осуществить:

- анализ угроз;
- оценка значимости объектов критической информационной инфраструктуры;
- присвоение категории значимости объектов критической информационной инфраструктуры;
- подготовку сведений о категорировании объектов критической информационной инфраструктуры.

При анализе угроз Исполнитель должен:

- выявить группы угроз безопасности информации в отношении объекта критической информационной инфраструктуры, а также запросить имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа;
- рассмотреть возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

– проанализировать угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры.

В рамках оценки значимости объектов критической информационной инфраструктуры Исполнитель должен провести оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры.

Исполнитель, по согласованию с Заказчиком должен осуществить присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости, либо обосновать принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

После присвоения категории значимости объектов критической информационной инфраструктуры Исполнитель осуществляет подготовку документа «Сведения о категорировании объектов критической информационной инфраструктуры» в соответствии с требованиями Приказа ФСТЭК России 236 от 22.12.2017 «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».

4.1.5 Требования к документации

В результате выполнения комплекса услуг Исполнитель должен предоставить Заказчику для каждого объекта информатизации следующие документы:

– Приказ о создании комиссии по категорированию объектов критической информационной инфраструктуры;

- Заключение комиссии по категорированию объектов критической информационной инфраструктуры;
- Перечень объектов критической информационной инфраструктуры;
- Акт категорирования объектов критической информационной инфраструктуры;
- Уведомление ФСТЭК России о результатах категорирования объектов критической информационной инфраструктуры;
- Приказ об ответственности за обеспечение безопасности объектов критической информационной инфраструктуры;
- Модель угроз безопасности значимого объекта критической информационной инфраструктуры.

5 Состав и содержание поставляемого товара

№ п/п	Наименование товара	Код по ОКПД 2*	Наименование показателя, технического, функционального параметра, характеристики и т.п.	Описание, значение	Ед. изм.	Кол-во
1	Приложение по автоматизации процессов сопровождения и разработки документации, регламентирующей защиту информации	62.01.29.000	Возможность самостоятельного сопровождения Заказчиком комплекта документации, регламентирующей защиту информации (корректировка разработанного комплекта документации при изменении условий обработки защищаемой информации или иных параметров, влияющих на содержание комплекта документации)	Наличие функции	Лиц.	1
			Возможность самостоятельной разработки Заказчиком новых комплектов документации для вновь вводимых объектов защиты	Наличие функции		

			информации (ИСПДн, ГИС, СКЗИ)			
			Отслеживание изменений в нормативно-методической документации ФСТЭК России, ФСБ России, действующей нормативно-правовой документации Российской Федерации в области защиты информации и автоматическое изменение содержания документации, регламентирующей защиту информации	Наличие функции		
			Интеграция с пакетом офисных программ в части загрузки массивов данных в приложение	Наличие функции		
			Отображение статуса готовности каждого документа и перечня данных, необходимых для окончательной подготовки документа	Наличие функции		
			Адаптация документов типа «Приказ», для печати на бланке Заказчика	Наличие функции		

			Настройка документов типа «Приказ»: указание автора, составителя и согласующих проект приказа лиц; замена предыдущего приказа новым	Наличие функции		
			Автоматический подбор падежей слов, вносимых сведениях	Наличие функции		
			Выгрузка документов в формате приложения Microsoft Word	Наличие функции		
			Выгрузка пакета документов в формате приложения Microsoft Word в одном архиве	Наличие функции		
			Разработка нормативно-распорядительной документации по обработке и защите персональных данных и государственных информационных систем	Наличие функции		
			Количество разрабатываемых документов, штук	Не менее 31		
			Наличие справок, содержащих описание, порядок работы и необходимость применения	Наличие функции		

			документа для разрабатываемых приложением нормативно-распорядительным документам по обработке и защите персональных данных			
			Разработка нормативно-распорядительной документации для средств криптографической защиты информации	Наличие функции		
			Количество разрабатываемых документов, штук	Не менее 16		
			Наличие справок, содержащих описание, порядок работы и необходимость применения документа для разрабатываемых приложением нормативно-распорядительным документам для средств криптографической защиты информации	Наличие функции		
			Учет сведений о следующих активах информационной	Наличие функции		

			безопасности при разработке комплекта документов для средств криптографической защиты информации: – средства криптографической защиты информации; – сертификаты соответствия имеющихся средств криптографической защиты информации требованиям безопасности информации; технические средства на которых эксплуатируются средства криптографической защиты информации			
			Проведение инструктажа пользователей работе со средствами криптографической защиты информации	Наличие функции		
			Организация проведения тестирования пользователей по результатам инструктажа о работе со средствами криптографической защиты информации	Наличие функции		

			Проведение инструктажа и тестирования с использованием веб-браузера на личном автоматизированном рабочем месте	Наличие функции		
			Разработка заключений о возможности эксплуатации средств криптографической защиты информации и заключений о допуске пользователей средств криптографической защиты информации по результатам инструктажа и проведения зачетов	Наличие функции		
			Разработка организационно-распорядительной документации объектов критической информационной инфраструктуры	Наличие функции		
			Количество разрабатываемых документов, штук	Не менее 6		
			Разработка моделей угроз и моделей нарушителя	Наличие функции		

			Наличие перечня актуальных угроз безопасности в том числе приведенных в банке данных угроз безопасности ФСТЭК России	Наличие функции		
			Определение уровня защищенности информационной системы персональных данных и класса защиты государственной информационной системы на основании данных имеющихся в приложении	Наличие функции		
			Оценка исходной защищенности и степени выполнения защитных мер	Наличие функции		
			Наличие технической анкеты для определения особенностей функционирования системы и исключения угроз безопасности, не имеющих предпосылки	Наличие функции		
			Выгрузка модели угроз в формате Microsoft Word, для	Наличие функции		

			каждой информационной системы			
			Возможность создания единой модели угроз безопасности для всех информационных систем заказчика	Наличие функции		
			Видеоинструкция по работе с функционалом разработки и сопровождения документации	Наличие		
			Страница руководства по работе с функционалом разработки и сопровождения документации в HTML-формате	Наличие		
			Учет информационных систем персональных данных	Наличие функции		
			Учет государственных информационных систем	Наличие функции		
			Учет аттестатов соответствия информационных систем требованиям безопасности информации	Наличие функции		
			Учет средств защиты информации с указанием	Наличие функции		

			реализуемых подсистем информационной безопасности			
			Учет знаков и сертификатов соответствия имеющихся средств защиты информации требованиям безопасности информации	Наличие функции		
			Учет действующих лицензий на право использования средств защиты информации	Наличие функции		
			Учет технических средств с указанием принадлежности к информационным системам	Наличие функции		
			Объединение технических средств в логические группы	Наличие функции		
			Учет лиц, ответственных за эксплуатацию технических средств	Наличие функции		
			Учет лиц, ответственных за информационную безопасность	Наличие функции		
			Учет сведений об обучении и стаже в области информационной	Наличие функции		

			безопасности ответственных лиц			
			Управление информацией о сотрудниках	Наличие функции		
			Импорт перечня сотрудников из файла	Наличие функции		
			Видеоинструкция по работе с функционалом учета активов	Наличие		
			Страница руководства по работе с функционалом учета активов в HTML-формате	Наличие		
			Учет перечня сотрудников	Наличие функции		
			Быстрый выбор сотрудников из перечня при назначении лиц, ответственных за мероприятия по информационной безопасности или при допуске сотрудников к защищаемой информации, хранилищам и помещениям	Наличие функции		
			Просмотр истории инструктажей и тестировании по вопросам информационной	Наличие функции		

			безопасности пройденных сотрудником			
			Просмотр информации об обучении сотрудника по вопросам информационной безопасности и стаже в области информационной безопасности	Наличие функции		
			Возможность указания следующей информации о сотруднике: – фамилию, имя и отчество; – подразделение; – должность; контактную информацию (адрес электронной почты).	Наличие функции		
			Видеоинструкция по работе с функционалом управления информацией о сотрудниках	Наличие		
			Страница руководства по работе с функционалом управления информацией о сотрудниках в HTML-формате	Наличие		
			Автоматическая загрузка базы возможных мероприятий по информационной	Наличие функции		

			безопасности из предустановленного в приложении набора, включающего в себя: – мероприятия по общей информационной безопасности; – мероприятия по порядку обработки и защиты персональных данных; – мероприятия по порядку эксплуатации средств криптографической защиты информации; мероприятия по организации обеспечения безопасности объектов КИИ.			
			Информация о мероприятиях по информационной безопасности, включающая в себя: – наименование мероприятия; – описание мероприятия; – плановый срок выполнения мероприятия;	Наличие функции		

			– информация об обязательности мероприятия (рекомендуемые мероприятия); – пояснение по выполнению мероприятия; – тема мероприятия; – группы мероприятия; – информацию о лице, ответственном за выполнение мероприятия; – отметку о выполнении мероприятия; – статус; – отчет о выполнении мероприятия; свидетельства выполнения мероприятия – прикрепленные файлы.			
			Поддержка поиска по ролям «группы мероприятия» и «тема мероприятия» в списке мероприятий	Наличие функции		
			Видеоинструкция по работе с функционалом управления мероприятиями по	Наличие		

			информационной безопасности			
			Страница руководства по работе с функционалом управления мероприятиями по информационной безопасности в HTML-формате	Наличие		
			Назначение задач сотрудникам из числа указанных в приложении	Наличие функции		
			Назначение задач группам сотрудников из числа указанных в приложении	Наличие функции		
			Отправка сотрудникам уведомлений о назначении задачи	Наличие функции		
			Фильтрация задач по категории, статусу и приоритету	Наличие функции		
			Поиск задач по теме	Наличие функции		
			Изменение свойств задач и добавление отчётов	Наличие функции		
			Назначаемые сотрудникам задачи, включающие в себя следующую информацию: – тема; – теги;	Наличие функции		

			– дата завершения; – исполнитель или группа исполнителей; – статус; – приоритет; – описание задачи; отчёт о выполнении задачи.			
			Возможность установления связи с зарегистрированными инцидентами информационной безопасности.	Наличие функции		
			Обеспечение возможности добавления вложений в виде одного или нескольких файлов для назначенных задач	Наличие функции		
			Назначение сотрудникам онлайн-инструктажей из числа доступных в приложении	Наличие функции		
			Тестирование сотрудника по результатам прохождения онлайн-инструктажа	Наличие функции		
			Назначение сотрудникам отдельных тестов из числа доступных в приложении	Наличие функции		

			Уведомление сотрудников, контактные адреса которых указаны в справочнике, о необходимости прохождения онлайн-инструктажа или теста	Наличие функции		
			Генерация уникальных ссылок на онлайн-инструктажи или тесты для отдельных сотрудников	Наличие функции		
			Электронный журнал проведенных онлайн-инструктажей и тестов сотрудников	Наличие функции		
			Автоматическое определение результатов тестирования для тестов, снабженных критериями оценки	Наличие функции		
			Ручное определение результатов тестирования автором теста	Наличие функции		
			Онлайн инструктажи и тесты по следующим темам: – персональные данные; – эксплуатация средств криптографической защиты информации;	Наличие функции		

			фишинг и другие актуальные угрозы ИБ для пользователей.			
			Создания инструктажей, оформленных во встроенным редактором, в том числе содержащих: – тексты; – рисунки; видеоматериалы.	Наличие функции		
			Создание тестов, содержащих следующую информацию: – название теста; – тема; – общее количество вопросов; – количество задаваемых вопросов; – процент правильных ответов для успешного прохождения; – пояснение к тесту, отображаемое работнику; – вопросы теста; варианты ответов на вопросы теста.	Наличие функции		

			Видеоинструкция по работе с функционалом повышения осведомленности и контроля знаний сотрудников в области информационной безопасности	Наличие		
			Страница руководства по работе с функционалом повышения осведомленности и контроля знаний сотрудников в области информационной безопасности в HTML-формате	Наличие		
			Представление информации о степени соответствия организации информационной безопасности требованиям законодательства РФ в интерфейсе приложения с учетом критериев оценки	Наличие функции		
			Критерии эффективности использования приложения, включающие: – сводный показатель эффективности работы;	Наличие функции		

			– дата последнего входа пользователей в приложение; дата последнего изменения параметров документов.			
			Наличие критериев оценки, включающих: – степень готовности документов; – степень актуальности документов (готовность документов с учетом срока их актуальности); степень выполнения мероприятий по информационной безопасности в организации	Наличие функции		
			Отображение состояния каждого критерия с помощью цветовой индикации, а также текстовой и табличной информации	Наличие функции		
			Отображение подробного отчета, содержащего информацию о готовности каждого отдельного документа или выполнении	Наличие функции		

			каждого назначенного мероприятия			
			Календарь событий	Наличие функции		
			Просмотр календаря за день, неделю, месяц	Наличие функции		
			Добавление новых событий с указанием наименования, даты начала, даты окончания и даты уведомления	Наличие функции		
			Регистрация инцидента пользователем Приложения с составлением описания инцидента	Наличие функции		
			Возможность прикладывать файлы, содержащие свидетельства инцидента, размером не более 25 Мегабайт	Наличие функции		
			Организация реагирования на инциденты с помощью назначения задач сотрудникам и группам сотрудников	Наличие функции		
			Установление связи с активами информационной безопасности	Наличие функции		

			Указание внешних источников инцидентов при их наличии	Наличие функции		
			Указание заключения по инциденту	Наличие функции		
			Просмотр журнала инцидента	Наличие функции		
			Просмотр текущей информации по инциденту	Наличие функции		
			Скачивание паспорта инцидента	Наличие функции		
			Просмотр сводной информации по инцидентам	Наличие функции		
			Хранение информации об инцидентах информационной безопасности, включающей: – описание инцидента; – свидетельства инцидента в виде файлов вложений; – задачи сотрудникам или группам сотрудников, связанные с реагированием на инциденты с возможностью их поиска по теме и исполнителю;	Наличие функции		

			– связи с активами информационной безопасности; – внешние источники инцидента со следующими данными: IP, URL, описание; – заключение по инциденту со следующими данными: статус, ущерб от подтвержденного инцидента; события в журнале инцидента, связанные с его изменениями.			
			Хранение описания инцидента, включающего: – номер инцидента (идентификатор); – заголовок инцидента; – теги инцидента; – организация, в которой произошел инцидент; – описание; – дата, когда произошел инцидент; – плановая дата реагирования на инцидент;	Наличие функции		

			– группа информирования; – информация об основном ответственном лице или группе исполнителей; – уровень критичности инцидента; – уровень конфиденциальности; – источник; – ранее принятые меры оперативного реагирования на инцидент; – описание иных объектов; меры по недопущению подобных инцидентов.			
			Хранение связей с активами информационной безопасности, включающими: – технические средства; – группы ТС; – ГИС; – ИСПДн; – СЗИ; – работники; связь с другими инцидентами	Наличие функции		

			Учет и сопровождение объектов критической информационной инфраструктуры	Наличие функции		
			Учет управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры	Наличие функции		
			Создание процессов с указанием наименований и выбора параметра, указывающего на принадлежность процесса к сфере критической информационной инфраструктуры	Наличие функции		
			Модуль оценки возможного ущерба	Наличие функции		
			Критерии оценки ущерба, штук	Не менее18		

			Значения критериев оценки ущерба, штук	Не менее 4		
			Автоматическое определение критического процесса в соответствии с проводимой оценкой возможного ущерба	Наличие функции		
			Учет объектов критической инфраструктуры (информационных систем)	Наличие функции		
			Учет основных данных об информационных системах в составе: – наименование информационной системы; – назначение информационной системы; принадлежность к объекту критической информационной инфраструктуры.	Наличие функции		
			Учет структурно-функциональных характеристик информационных систем в составе: – тип информационной системы;	Наличие функции		

			архитектура информационной системы.			
			Учет состава объектов информационных в составе: – используемые сети связи; – технические средства; – используемые операционные системы; используемое прикладное программное обеспечение.	Наличие функции		
			Учет нарушителей и угроз, определенных в рамках категорирования объектов критической информационной инфраструктуры в составе: – нарушители безопасности информации; – обоснование отсутствия нарушителя безопасности; – основные угрозы безопасности информации; – обоснование отсутствия актуальных угроз; – возможные типы компьютерных инцидентов;	Наличие функции		

			– обоснование отсутствия возможности компьютерных инцидентов; – степень возможного ущерба; перечень показателей критериев значимости.			
			Определение категории в составе: – сфера деятельности; – планируемый срок категорирования; – критические процессы, обеспечиваемые системой; – значения показателей значимости объекта критической информационной инфраструктуры; итоговая категория значимости.	Наличие функции		
			Учет защитных мер в составе: – принятые организационные мероприятия; – принятые меры защиты;	Наличие функции		

			используемые средства защиты информации.			
			Учет сетей связи, используемых при взаимодействии объектов критической информационной инфраструктуры, включающий возможность хранения и редактирования следующих данных: – наименование сети связи; – категория сети связи; – наименование оператора сети; – цель взаимодействия информационных систем с сетью; – тип взаимодействия; используемые технологии и протоколы.	Наличие функции		
			Определение и учет ответственных лиц, принимающих участие в процессе категорирования и обеспечения безопасности объектов критической информационной	Наличие функции		

			инфраструктуры, включающий возможность хранения и редактирования данных.			
			Сведения об ответственных лицах, включающие: – фамилию, имя, отчество; – структурное подразделение организации; должность.	Наличие функции		
			Возможность назначения ответственности за организацию безопасности объектов критической информационной инфраструктуры, как на отдельных сотрудников, так и структурное подразделение	Наличие функции		
			Видеоинструкция по работе с функционалом учета и сопровождения объектов критической информационной инфраструктуры	Наличие		
			Страница руководства по работе с функционалом учета и сопровождения	Наличие		

			объектов критической информационной инфраструктуры в HTML-формате			
			Техническая поддержка приложения	Наличие функции		
			Консультирование по вопросам входа в сервис, смены пароля	Наличие функции		
			Консультирование по вопросам использования сервиса (очередность выполнения мероприятий, внесение корректных данных для подготовки документации и т.п.)	Наличие функции		
			Предоставление информационных материалов по работе с системой	Наличие функции		
			Обеспечение стабильной работы сервиса	Наличие функции		
			Устранение технических ошибок в работе сервиса	Наличие функции		
			Предоставление обновлений шаблонов документов в соответствии с изменениями законодательства РФ и	Наличие функции		

			требований регуляторов по ИБ			
			Обеспечение технической поддержки по телефону, электронной почте, а также с помощью встроенного функционала по приему обращений	Наличие функции		
			Создание пользователями обращения в техническую поддержку и отслеживание хода их исполнения	Наличие функции		
			Возможность добавлять к обращению снимки экрана в форматах файлов .jpg, .jpeg, .png	Наличие функции		
			Оценка исполнения заявки в техническую поддержку	Наличие функции		
			Клиент-серверная архитектура приложения	Наличие функции		
			Отсутствие необходимости установки приложения на АРМ Заказчика	Наличие функции		
			Доступность серверной части приложения, часов/ дней в неделю	Не менее 24/7		

			Максимальное время простоя при сбоях приложения, минут	Не более 60		
			Допустимое время отклика, секунд	Не более 3		
			Уведомление о недоступности приложения по электронной почте	Наличие функции		
			Наличие аттестата соответствия, подтверждающего выполнение перечня организационных и технических мер по защите приложения в соответствии с требованиями нормативно-методической документации ФСТЭК России, ФСБ России и действующей нормативно-правовой документации Российской Федерации в области защиты информации	Наличие функции		
			Онлайн обмен сообщениями между специалистами Заказчика и Исполнителя по вопросам технической и консультационной	Наличие функции		

			поддержки при использовании приложения			
			Возможность пролонгации использования приложения без потери имеющихся данных, после завершения срока использования, месяцев	Не менее 12		
			Бесперебойное функционирование приложения, месяцев	Не менее 12		

*Общероссийский классификатор продукции по видам экономической деятельности ОК 034-2014.

Инженер ХО

_____Цой Е.В.