Приложение № 3 к Извещению

о проведении электронного аукциона

# Техническое задание

**на оказание комплекса услуг в области информационной безопасности**

# Используемые сокращения.

ИБ – информационная безопасность;

ИС – информационная система;

ИТ – информационные технологии;

ИСПДн – информационная система персональных данных;

КИИ – критическая информационная инфраструктура;

ПО – программное обеспечение;

Система – информационная система автоматизации процессов управления информационной безопасностью;

СЗИ – средство защиты информации;

СКЗИ – средство криптографической защиты информации;

ТС – техническое средство;

ФСБ России – Федеральная служба безопасности России;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю России

# Общие сведения.

**Заказчик:** Искательское муниципальное унитарное предприятие «Посжилкомсервис»

**Срок оказания услуг:** с момента заключения договора до «30» апреля 2024 года.

# Цель и правовые основания оказания услуг.

## Цель:

* автоматизация процессов исполнения организационных и технических мероприятий по защите информации в информационных системах Искательского муниципального унитарного предприятия «Посжилкомсервис»;
* приведение объекта информатизации Искательского муниципального унитарного предприятия «Посжилкомсервис» в соответствие требованиям действующей нормативно-правовой документации Российской Федерации в области защиты информации с поставкой, установкой и настройкой необходимых средств защиты информации.

## Правовые основания для оказания услуг:

* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление правительства РФ от 21 марта 2012 г. № 211 Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
* Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;
* Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* Национальный стандарт РФ ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* «Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных», утверждена 14.02.2008 заместителем директора ФСТЭК России;
* «Базовая модель угроз безопасности персональных данных при обработке в информационных системах персональных данных», утверждена 15.02.2008 заместителем директора ФСТЭК России.
* Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
* Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
* Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 центра ФСБ России 31 марта 2015 года № 149/7/2/6-432;

# Требования к Исполнителю.

Исполнитель должен иметь действующую лицензию государственного образца на следующие виды деятельности:

* Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации, а именно:
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

(в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» и Постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»);

Оказание услуг осуществляется Исполнителем непосредственно в соответствии с требованиями, изложенными в настоящем Техническом задании. Привлечение третьих лиц не допускается.

# Состав, описание и содержание услуг, требования к документированию.

4.1. Состав (перечень) оказываемых услуг

Оказание услуг по приведению объекта информатизации в соответствие требованиям действующего законодательства РФ в области защиты информации включает в себя следующие виды работ:

1. Автоматизации процессов управления информационной безопасностью.
2. Разработка организационно-распорядительной и технической документации для ИС.
3. Поставка сертификата экспертной поддержки.
4. Поставка, установка и настройка средств защиты информации;

4.2. Описание оказываемых услуг

Исполнитель обязан оказать услуги в порядке и объеме, представленном в таблице 1.

| **№ п/п** | **Наименование** | **Описание объема оказываемых услуг** |
| --- | --- | --- |
|  | Автоматизация процессов управления информационной безопасностью | * Возможность самостоятельной разработки новых комплектов документации для объектов защиты информации; * Возможность самостоятельного сопровождения комплекта документации, регламентирующей защиту информации (корректировка разработанного комплекта документации при изменении условий обработки защищаемой информации или иных параметров, влияющих на содержание комплекта документации) при ПО * Отслеживание изменений в нормативно-методической документации Роскомнадзора, 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. |
|  | Разработка организационно-распорядительной и технической документации | Исполнитель должен разработатьи передать заказчику проектыорганизационно-распорядительных документов в соответствии с требованиями законодательства РФ и нормативными документами регуляторов в области обеспечения информационной безопасности (для типовых сегментов информационных систем).  Модель угроз и нарушителя для ИСПДн:   * ПК«1С» (Бухгалтерия предприятия», Зарплата и управление персоналом», Формула ЖКХ»); * ПК «Спринтер».   Модель угроз и нарушителя для АСУ«Система мониторинга объектов теплоснабжения».  Частное техническое задание на подсистему информационной безопасности для ИСПДн:   * ПК «1С» (Бухгалтерия предприятия», Зарплата и управление персоналом», Формула ЖКХ»); * ПК «Спринтер».   Частное техническое задание на подсистему информационной безопасности для АСУ«Система мониторинга объектов теплоснабжения».  Технический паспорт (без инвентаризационных данных) для ИСПДн с описанием типового пользовательского и серверного сегмента:   * ПК «1С» (Бухгалтерия предприятия», Зарплата и управление персоналом», Формула ЖКХ»); * ПК «Спринтер».   Технический паспорт (без инвентаризационных данных)для АСУ «Система мониторинга объектов теплоснабжения»с описанием типового пользовательского и серверного сегмента: |
|  | Экспертная поддержка | Экспертная поддержка представляет собой документ, оформленный в виде бумажного и/или электронногосертификата, содержащий информацию о полном названии организации Заказчика, уникальном идентификационном номере сертификата экспертной поддержки, полном списке продуктов, на которые распространяется данный сертификат, и подтверждающий право Заказчика на получение технической поддержки в объеме до 10 обращений.  Приём обращений, работа над всеми проблемами и консультирование ведется с учетом режима рабочего времени: с 09:00 до 18:00 по московскому времени.  Приём обращений ведется:  - через web-портал;  - по электронной почте:  - по телефону:  При обращении Заказчик должен предоставить следующую информацию:  - номер сертификата на техническую поддержку;  - наименование компании Заказчика;  - описание возникшей ситуации.  **Экспертная информационная поддержка по вопросам информационной безопасности, экспертная поддержка при обращениях граждан по вопросам обработки персональных данных, по вопросам эксплуатации информационных систем, объектов критической информационной инфраструктуры (КИИ)**  Официальный ответ на обращение предоставляется на официальный запрос. Официальный запрос должен быть передан на электронную почту (скан) на официальном бланке организации, с указанием номера, даты и подписью ответственного должностного лица. В одном запросе может содержаться один или более вопросов. Заказчик указывает должностное лицо, которое имеет право подписывать официальные запросы от имени Заказчика.  Кол-во вопросов/ответов в месяц: **не более 5**. Неиспользованное кол-во вопросов не переходит на следующий месяц.  Срок ответа на официальный запрос: в течение 10 рабочих дней.  **Экспертная поддержка по согласованию Модели угроз с регуляторами**   1. Поставщик осуществляет логический контроль (проверка состава и наличия противоречий параметров друг другу) созданной Заказчиком модели угроз в сервисе. 2. Поставщик предоставляет рекомендации по оформлению модели угроз. 3. Поставщик предоставляет информацию о порядке отправки модели угроз регулятору, включая адрес отправки. 4. В случае получения замечаний регулятора к модели угроз, Поставщик вносит правки в модель угроз на основе замечаний регулятора и дополнительной информации от Заказчика. 5. Поставщик передает Заказчику откорректированную модель угроз в электронном виде.   Сроки выполнения пунктов 1-3 – 10 рабочих дней.  Сроки выполнения пунктов 4-5 – 20 рабочих дней.  **Экспертная поддержка по подготовке к проверкам регуляторов**  По запросу Заказчика Поставщик предоставляет чек-лист по подготовке к проверке. В зависимости от проверяющего регулятора (ФСБ, ФСТЭК, Роскомнадзор) предоставляется соответствующий чек-лист в электронном виде. Заказчик предоставляет Поставщику скан письма регулятора о предстоящей проверке.  **Сопровождение (удаленное) во время проверок регуляторов**  Поставщик осуществляет консультации по телефону и электронной почте в течение проводимой проверки. |
|  | Поставка, установка и настройка средств защиты информации | Исполнитель выполняет поставку средств защиты информации (далее – СЗИ) в соответствии с настоящим Техническим заданием. Перечень поставляемых Исполнителем средств защиты информации приведен в Приложении 1 к настоящему Техническому заданию.  Исполнитель проводит установку, настройку поставляемого СЗИ.  Поставляемые СЗИ должны удовлетворять требованиям, приведенным в Приложении 1 к настоящему Техническому заданию.  Поставляемые СЗИ должны быть ранее не эксплуатируемыми (новыми).  Поставляемые СЗИ должны реализовывать функции по обеспечению безопасности информации, в т.ч. персональных данных, в соответствии с требованиями действующего законодательства.  При оказании услуг должны соблюдаться все авторские и смежные с ними права разработчика средств защиты информации.  Установка и настройка СЗИ осуществляется Исполнителем в соответствии с требованиями нормативных документов ФСТЭК России и ФСБ России по защите информации, а также в соответствии с эксплуатационной документацией на СЗИ. |

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

## 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.

## 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.

## Требования к сроку функционирования приложения

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

## Требования к функциям приложения.

Приложение должно выполнять следующие функции:

* формирование документации по информационной безопасности на основании разработанных шаблонов, с учетом заполненных динамических параметров;
* возможность заполнения ответственных лиц;
* 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;
* календарь событий;
* управление инцидентами информационной безопасности;
* учет и актуализация объектов критической информационной инфраструктуры;
* автоматизированное формирование электронных журналов и ведение электронных журналов;
* организация процесса технической поддержки Заказчика.

## Требования к формированию комплекта документации по информационной безопасности

### Требования к составу формируемого комплекта документации по информационной безопасности

Приложение должно обеспечивать формирование комплекта 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;
* организационно-распорядительная документация объектов критической информационной инфраструктуры.

### Общие требования к формированию комплекта документации по информационной безопасности

Приложение должно позволять осуществлять разработку и сопровождение Приложение должно позволять осуществлять формирование комплекта 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 MS ОfficeExcel не ниже версии 2003, **OpenOffice, LibreOffice** в части загрузки массивов данных в приложение;
* загрузка в приложение данных в допустимых форматах (.jpg, .jpeg, .bmp, .png, .tiff, .pdf), конвертация файлов в формат pdf и их объединение;
* отображение статуса готовности документов, на основе заполнения его параметров;
* отображение перечня данных, необходимого для подготовки документа;
* отображение индикации заполненности параметров документа, необходимых для его готовности;
* адаптация документов типа «Приказ» для печати на бланке Заказчика;
* настройка документов типа «Приказ»: заполнение параметров «автор», «составитель» и «согласующие проект приказа лиц»;
* автоматический подбор падежей слов, вносимых сведений;
* выгрузка документов в форматах: docx, pdf, odt;
* выгрузка пакета документов в заданном формате (docx, pdf, odt) в одном архиве.

### Требования к формированию комплекта нормативно-распорядительной документации по обработке и защите персональных данных и государственных информационных систем.

Формируемый комплект нормативно-распорядительной документации по обработке и защите персональных данных должен включать в себя:

* Акт установления уровня защищённости персональных данных в информационной системе персональных данных;
* Заключение об оценке вреда субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
* План внутренних проверок состояния защиты персональных данных;
* План мероприятий по защите персональных данных;
* Политика обработки персональных данных;
* Приказ об ответственности за обработку, защиту и техническое обслуживание информационных систем с защищаемой информацией;
* Приказ об установлении границ контролируемой зоны объектов информатизации;
* Приказ об утверждении перечня лиц, имеющих право доступа в помещения с СКЗИ;
* Приказ об утверждении мест хранения материальных носителей, перечня лиц, ответственных за их сохранность и имеющих доступ к ним;
* Уведомление об обработке персональных данных или справка о причинах не уведомления в уполномоченный орган;
* Приказ о мерах, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством «О персональных данных», включающий в себя в качестве приложений:
* Правила обработки персональных данных субъектов персональных данных;
* Правила рассмотрения запросов субъектов персональных данных или их представителей;
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами;
* Перечень информационных систем персональных данных;
* Инструкцию пользователя, допущенного к обработке персональных данных в информационных системах;
* Типовое обязательство служащего/сотрудника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему, в связи с исполнением должностных обязанностей;
* Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;
* Порядок доступа служащих/сотрудников в помещения, в которых ведётся обработка персональных данных;
* Положение по работе с инцидентами информационной безопасности;
* Инструкцию по учёту, хранению и регистрации выдачи машинных носителей персональных данных;
* Форму журнала ознакомления служащих/сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) обучения указанных служащих/сотрудников.
* Приказ о назначении ответственного за организацию обработки персональных данных и других ответственных лиц, включающий в себя в качестве приложений:
  + Должностную инструкцию (регламент) ответственного за организацию обработки персональных данных;
  + Функциональные обязанности администратора информационной безопасности;
  + Функциональные обязанности администратора информационных систем;
  + Состав комиссии по установлению уровня защищённости персональных данных в информационных системах персональных данных;
  + Состав комиссии по классификации государственной и (или) муниципальной информационной системы по требованиям защиты информации (при наличии таких информационных систем);
  + Состав комиссии по работе с инцидентами информационной безопасности.

Опционально должна быть предусмотрена возможность формирования следующих документов на основании шаблонов:

* Акт классификации информационной (автоматизированной) системы;
* Поручение на обработку персональных данных;
* Приказ о ведении журнала учёта проверок, проводимых органами государственного (муниципального) контроля (надзора);
* Приказ о ведении журнала учёта посетителей.

Для каждого шаблона нормативно-распорядительного документа по обработке и защите персональных данных должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документа.

### Требования к формированию комплекта нормативно-распорядительной документации для средств криптографической защиты информации.

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

* возможность автоматизированного проведения инструктажа пользователей о работе со средствами криптографической защиты информации;
* возможность автоматизированного проведения тестирования пользователей по результатам инструктажа о работе со средствами криптографической защиты информации;
* прохождение инструктажа и тестирования с использованием веб-браузера на личном автоматизированном рабочем месте пользователя;
* формирование на основании шаблонов заключений о возможности эксплуатации средств криптографической защиты информации и заключений о допуске пользователей средств криптографической защиты информации по результатам инструктажа и проведения зачетов.

Формируемый приложением комплект нормативно-распорядительной документации для средств криптографической защиты информации должен включать в себя:

* Приказ об организации и обеспечении безопасности информации ограниченного доступа с использованием СКЗИ, включающий в себя в качестве приложений:
* Правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях, в которых ведётся эксплуатация СКЗИ;
* Инструкция о порядке оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене;
* Инструкция по подготовке, вводу, обработке, хранению и передаче, защищаемой с использованием СКЗИ конфиденциальной информации;
* Функциональные обязанности ответственного пользователя СКЗИ;
* Типовая форма лицевого счета пользователя СКЗИ;
* Типовая форма журнала поэкземплярного учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
* Типовая форма журнала учёта хранилищ ключевых документов, эксплуатационной и технической документации к СКЗИ и ключей к ним;
* Типовая форма журнала опломбирования аппаратных средств, с которыми осуществляется функционирование СКЗИ;
* Типовая форма журнала проверок исправности сигнализации в помещениях, где ведётся эксплуатация СКЗИ;
* Типовая форма технического (аппаратного) журнала;
* Типовая форма акта уничтожения ключевого документа;
* Типовая форма плана проведения проверок за соблюдением условий использования СКЗИ;
* Типовая форма журнала пользователей сети;
* Типовая форма годового отчёта в ОКЗИ об уничтоженных ключевых документах;
* Состав комиссии по уничтожению ключевых документов СКЗИ.
* Заключение о возможности допуска пользователей к самостоятельной работе с СКЗИ;
* Заключение о возможности эксплуатации СКЗИ на автоматизированных рабочих местах;
* Лицевой счёт пользователя СКЗИ;
* План проведения проверок за соблюдением условий использования СКЗИ;
* Приказ о допуске пользователей к работе с СКЗИ;
* Приказ об утверждении перечня лиц, имеющих право доступа в помещения с СКЗИ;
* Схема организации криптографической защиты конфиденциальной информации.

Информация об эксплуатации средств криптографической защиты информации, необходимая для формирования комплекта 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;
* эксплуатация СКЗИ;
* помещения с СКЗИ;
* готовность к эксплуатации СКЗИ;
* пользователи СКЗИ.

Для каждого шаблона нормативно-распорядительного документа средств криптографической защиты информации должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документа.

### Требования к формированию моделей угроз безопасности информации и моделей нарушителя безопасности информации.

Приложение должно осуществлять формирование моделей угроз безопасности информации и моделей нарушителя безопасности информации, обеспечивающих 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:

* наличие перечня актуальных угроз безопасности, в том числе приведенных в банке данных угроз безопасности ФСТЭК России;
* оценка исходной защищенности и степени выполнения защитных мер;

экспорт модели угроз и модели нарушителя, для каждой информационной системы.

### Требования к формированию политики конфиденциальности для веб-сайта Заказчика.

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

* общие сведения о веб-сайте:
* наименование веб-сайта;
* адрес веб-сайта;
* раздел сайта с контактной информацией;
* цели обработки данных Пользователя;
* группы обрабатываемой информации;
* сведения о публикации персональных данных;
* 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 сайте;

наличие/отсутствие оплаты услуг и сервисов.

### Требования к формированию комплекта организационно-распорядительной документации объекта критической информационной инфраструктуры

Формируемый приложением комплект организационно-распорядительной документации объекта критической информационной инфраструктуры должен включать в себя:

* Акт категорирования объектов КИИ;
* Заключение о формировании перечня объектов КИИ;
* Перечень объектов КИИ, подлежащих категорированию;
* Приказ о создании комиссии по категорированию объектов КИИ;
* Приказ об ответственности за обеспечение безопасности объектов КИИ;
* Уведомление ФСТЭК России о результатах категорирования объектов КИИ.
* Приказ об обеспечении безопасности ЗОКИИ;
* Приказ об установлении границ контролируемой зоны ЗОКИИ;
* Правила безопасной работы при эксплуатации ЗОКИИ;
* Концепция обеспечения безопасности ЗОКИИ;
* План мероприятий по обеспечению безопасности КИИ;
* Регламент обеспечения безопасности ЗОКИИ.

Опционально должна быть предусмотрена возможность формирования следующих документов на основании шаблонов:

* Приказ о ведении журнала учёта проверок, проводимых органами государственного (муниципального) контроля (надзора);
* Приказ о ведении журнала учёта посетителей.

Для каждого шаблона организационно-распорядительной документации объекта критической информационной инфраструктуры должны прилагаться справки, содержащие описание, порядок работы и необходимость применения документов.

## Требования к заполнению ответственных лиц.

* + 1. Требования к заполнению ответственных лиц в области ПДн.

Приложением должно обеспечиваться заполнение следующих ответственных лиц в области ПДн:

* Ответственные за ПДн:
* Ответственный за организацию обработки ПДн;
* Телефон ответственного за организацию обработки ПДн;
* Адрес электронной почты ответственного за организацию обработки ПДн;
* Ответственный за обеспечение безопасности ПДн в информационных системах;
* Ответственный за техническое обслуживание информационных систем;
* Ответственный за выявление угроз безопасности и разработки моделей угроз;
* Состав комиссии по установлению УЗ:
* Председатель комиссии по установлению уровня защищенности ПДн при их обработке в информационных системах;
* Члены комиссии по установлению уровня защищенности ПДн при их обработке в информационных системах.
* Состав комиссии по инцидентам ИБ:
* Председатель комиссии по инцидентам информационной безопасности;
* Члены комиссии по инцидентам информационной безопасности.
* Иные ответственные лица:
* Ответственный за проверку сведений и отправку уведомления в РКН;
* Телефон ответственного за проверку сведений и отправку уведомления в РКН;
* Адрес электронной почты ответственного за проверку сведений и отправку уведомления в РКН;
* Ответственный за документальное регламентирование работы с ПДн;
* Ответственный за заключение договора на проведение работ в области защиты ПДн;
* Ответственный за заключение договора с компанией – лицензиатом ФСТЭК (ФСБ) России на аутсорсинг технической защиты ПДн;
* Ответственный за разработку приказа о вводе в эксплуатацию информационных систем, обрабатывающих ПДн;
* Ответственный за пересмотр договоров с субъектами и контрагентами, в части обработки ПДн;
* Ответственный за повышение квалификации работников в области защиты ПДн;
* Ответственный за обучение работников, осуществляющих обработку ПДн;

Регулярность обучения ответственных лиц.

* + 1. Требования к заполнению ответственных лиц в области СКЗИ.

Приложением должно обеспечиваться заполнение следующих ответственных лиц в области СКЗИ:

* Ответственные за СКЗИ:
* Ответственный пользователь СКЗИ;
* Адрес электронной почты ответственного пользователя СКЗИ;
* Замещающий ответственного пользователя СКЗИ;
* Ответственные за организацию работ с СКЗИ.
* Состав комиссии:
* Председатель комиссии по уничтожению ключевых документов СКЗИ;
* Члены комиссии по уничтожению ключевых документов СКЗИ.
* Орган криптографической защиты информации (ОКЗИ):
* Название организации;
* Руководитель ОКЗИ;

Схема реализации криптографической защиты информации.

* + 1. Требования к заполнению ответственных лиц в области КИИ.

Приложением должно обеспечиваться заполнение следующих ответственных лиц в области КИИ:

* Ответственные за КИИ:
* Должностное лицо, на которое возложены функции обеспечения безопасности значимых объектов КИИ;
* Лицо, ответственное за взаимодействие с регулятором по вопросам категорирования объектов КИИ;
* Контактный телефон лица, ответственного за взаимодействие с регулятором по вопросам категорирования объектов КИИ;
* Адрес электронной почты лица, ответственного за взаимодействие с регулятором по вопросам категорирования объектов КИИ;
* Определение будет ли назначено отдельное подразделение, ответственное за обеспечение безопасности объектов КИИ (Да):
* Руководитель подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
* Контактный телефон руководителя подразделения, ответственного за обеспечение безопасности значимых объектов КИИ;
* Адрес электронной почты руководителя подразделения, ответственного за обеспечение безопасности значимых объектов КИИ.
* Определение будет ли назначено отдельное подразделение, ответственное за обеспечение безопасности объектов КИИ (Нет):
* Лица, ответственные за обеспечение безопасности значимых объектов КИИ;
* Контактный телефон группы лиц, ответственных за обеспечение безопасности значимых объектов КИИ;
* Адрес электронной почты группы работников, ответственных за обеспечение безопасности значимых объектов КИИ.
* Состав комиссии по категорированию объектов КИИ:
* Председатель комиссии по категорированию объектов КИИ;
* Члены комиссии по категорированию объектов КИИ.
* Состав комиссии по инцидентам ИБ:
* Председатель комиссии по инцидентам ИБ;
* Члены комиссии по инцидентам ИБ.
* Состав комиссии по внутреннему контролю:
* Председатель комиссии по проведению внутреннего контроля состояния безопасности ЗОКИИ;

Члены комиссии по проведению внутреннего контроля состояния безопасности ЗОКИИ.

* + 1. Требования к заполнению иных ответственных лиц.
* Ответственный за ведение журнала учёта посетителей;
* Ответственный за ведение и хранение журнала учёта проверок Организации.

## 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;
* объединение технических средств в логические группы;
* учет электронных носителей;
* учет помещений с СКЗИ;
* учет пользователей СКЗИ;
* учет критериев готовности к эксплуатации СКЗИ;
* 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 обеспечивать возможность импорта сведений о технических средствах из файла, сформированного внешним сервисом анализа защищенности RedCheck.

Приложение должно содержать 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;
* экспорт перечня сотрудников в файл;
* учет перечня сотрудников;
* быстрый поиск сотрудников 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).

## Требования к возможности управления 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 порядку обработки и защиты государственных информационных систем;
* 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 (список организаций), ответственном за выполнение мероприятия;
* статус;
* отчет о выполнении мероприятия;
* свидетельства выполнения мероприятия – прикрепленные файлы.

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

## Требования к возможности управления задачами по информационной безопасности

Приложением должны обеспечиваться следующие возможности управления задачами по информационной безопасности:

* назначение задач сотрудникам из числа указанных в приложении;
* назначение задач группам сотрудников из числа указанных в приложении;
* фильтрация задач по статусу и приоритету;
* поиск задач по теме;
* изменение свойств задач и добавление отчётов;
* добавление комментариев к задаче;
* отправка сотрудникам уведомлений о назначении задачи, изменении ее свойств и добавлении комментариев.

Назначаемые сотрудникам задачи должны включать в себя следующую информацию:

* тема;
* дата завершения;
* исполнитель или группа исполнителей;
* статус;
* приоритет;
* описание задачи;
* отчёт о выполнении задачи или основание для отклонения.

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.

Для назначенных задач должна обеспечиваться возможность просматривать информацию по задаче и добавлять комментарии без авторизации в приложении.

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

Приложением должны обеспечиваться следующие возможности по повышению осведомленности сотрудников 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;
* протоколы 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.

## 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.

## 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.

## Требования к возможности управления 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;
* отчет о выполнении мер;
* 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;
* информационные системы;
* 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.

## Требования к учету и актуализации объектов критической информационной инфраструктуры

### 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;

### Требования к учету и актуализации процессов КИИ

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 КИИ с указанием наименований и выбора параметра, указывающего на принадлежность процесса к сфере критической информационной инфраструктуры.

Для каждого процесса КИИ, входящего в сферу КИИ, должна быть доступна оценка критичности, разделенная на пять логических блоков:

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

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

### Требования учету информационных систем в КИИ

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

* основные данные об информационной системе в разрезе следующих атрибутов:
* наименование информационной системы;
* тип системы;
* используемые технологии;
* назначение информационной системы;
* 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;
* отметка об осуществлении взаимодействия ИС с сетями электросвязи;
* используемые сети связи;
* технические средства;
* адрес и состав размещения ЦОД (при наличии):
* адрес размещения ЦОД;
* используемые ОС;
* используемое прикладное ПО;
* отметка об осуществлении взаимодействия ИС с сетями электросвязи;
* используемые сети связи;
* технические средства;
* сторонние организации в ОКИИ (при наличии):
* сторонняя организация, эксплуатирующая объект КИИ;
* тип технического средства;
* 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);
* отметка о возможности возникновения компьютерных инцидентов в результате реализации угроз;
* возможные типы компьютерных инцидентов (при их наличии);
* обоснование отсутствия возможности компьютерных инцидентов (при их отсутствии);
* защитные меры:
* принятые организационные меры или обоснование их отсутствия;
* принятые меры защиты информации или обоснование их отсутствия;
* отметка применяются ли СЗИ в ИС (на объекте КИИ);
* используемые СЗИ;
* КИИ:
* сфера деятельности;
* планируемая дата завершения категорирования;
* критические процессы, обеспечиваемые системой;
* итоговая категория значимости;
* обоснования значений показателей критериев значимости или их неприменимости;

значения показателей значимости объекта критической информационной инфраструктуры.

### Требования учету 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.

### Требования к автоматизированному формированию электронных журналов и ведению электронных журналов

Приложение должно обеспечивать возможность автоматизированного формирования и ведения следующих журналов:

* журнал учета СКЗИ;
* журнал учета носителей персональных данных;
* журнал ознакомления работников с положениями по ПДн;
* журнал учета носителей информации для объектов КИИ;
* журнал ознакомления работников с положениями о безопасности КИИ.

Приложением должны быть обеспечены следующие функции по работе с журналами, включающие в себя:

* установку даты начала и окончания ведения журнала;
* назначение работников, имеющих право работать с журналом;
* сортировку и поиск по записям журнала;
* импорт данных из файла;
* экспорт журнала или отдельных записей в файл;

удаление импортированных записей из журнала.

## Требования к организации процесса технической поддержки

### Общие сведения

Техническая поддержка осуществляется в будние дни с 09:00 до 18:00 по Московскому времени и включает в себя консультирования пользователей по вопросам, связанным с функционалом работы сервиса, включающим:

* регистрация учетных записей пользователей;
* продление тарифа пользователей;
* консультирование по вопросам функционального использования приложения (очередность выполнения мероприятий, внесение корректных данных для формирования документации и т.п.);
* консультирование по порядку формирования и выгрузки документации;
* экспертные консультации в области документального обеспечения деятельности по информационной безопасности (не более 3 консультации в период действия лицензии).

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

Функционал приложения должен позволять пользователям создавать обращения в техническую поддержку и отслеживать ход их исполнения. Должна быть возможность добавлять к обращению файлы в форматах: .doc, .docx, .xls, .xlsx, .jpg, .jpeg, .png, .pdf.

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.

Приложение должно иметь руководство по работе с функционалом приложения в HTML-формате.

### Технические характеристики приложения

Приложение должно иметь клиент-серверную архитектуру, не требовать установки на АРМ и сервера Заказчика и функционировать в современном веб-браузере (GoogleChrome, Yandex, MozillaFirefox 3.0 и выше). Приложениедолжно быть доступно Заказчику по предоставленному Исполнителем веб-адресу 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 или посредством информационного сообщения в приложении.

Гарантийная поддержка должна осуществляться Исполнителем в течение срока действия лицензии Приложения.

Гарантийная поддержка должна распространяться на все функциональные компоненты Приложения и обеспечивать исправление ошибок в Приложении и документации, влияющих на выполнение условий настоящего технического задания.

Таблица 2. Состав и содержание поставляемого приложения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование  товара | Наименование показателя, технического, функционального параметра, характеристики и т.п. | Описание,  значение | Ед. изм. | Кол-во |
| Приложение по автоматизации процессов сопровождения и разработки документации, регламентирующей защиту информации. | 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 | Шт. | 1 |
| Возможность самостоятельного формирования в приложении Заказчиком комплектов документации по шаблонам, с учетом заполнения необходимых динамических параметров в приложении для вновь вводимых объектов защиты информации (ИСПДн, ГИС, СКЗИ) | Наличие функции |
| 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 Оffice, Excel не ниже версии 2003, **OpenOffice, LibreOffice,** в части загрузки массивов данных в приложение | Наличие функции |
| Загрузка в приложение данных в допустимых форматах (.jpg, .jpeg, .bmp, .png, .tiff, .pdf), конвертация файлов в формат pdf, и их объединение | Наличие функции |
| Функционал «Работа с документами»  Отображение статуса готовности документов, на основе заполнения его параметров | Наличие функции |
| Отображение перечня данных, необходимого для подготовки документа | Наличие функции |
| Отображение индикации заполненности параметров документа, необходимых для его готовности | Наличие функции |
| Адаптация документов типа «Приказ», для печати на бланке Заказчика | Наличие функции |
| Настройка документов типа «Приказ»: заполнение параметров «автор», «составитель» и «согласующие проект приказа лиц» | Наличие функции |
| Автоматический подбор падежей слов, вносимых сведениях | Наличие функции |
| Выгрузка документов в форматах: docx, pdf, odt | Наличие функции |
| Выгрузка пакета документов в заданном формате (docx, pdf, odt) в одном архиве | Наличие функции |
| Формирование комплекта нормативно-распорядительной документации по обработке и защите персональных данных и государственных информационных систем | Наличие функции |
| Количество формируемых документов, штук | Не менее 16 |
| Наличие справок, содержащих описание, порядок работы и необходимость применения документов формируемые приложением по обработке и защите персональных данных | Наличие функции |
| Формирование комплекта нормативно-распорядительной документации для средств криптографической защиты информации | Наличие функции |
| Количество формируемых документов, штук | Не менее 8 |
| Наличие справок, содержащих описание, порядок работы и необходимость применения документов формируемые приложением для средств криптографической защиты информации | Наличие функции |
| Возможность загрузки в базу данных файлов с иной организационно-распорядительной документацией Заказчика | Наличие функции |
| Формирование пакета организационно-распорядительной документации объектов критической информационной инфраструктуры | Наличие функции |
| Количество формируемых документов, штук | Не менее 14 |
| Наличие справок, содержащих описание, порядок работы и необходимость применения документов, формируемых приложением для объектов критической информационной инфраструктуры | Наличие функции |
| Функционал «Ответственность»  Возможность заполнения ответственных лиц в области ПДн:   * Ответственные за ПДн; * Состав комиссии по установлению УЗ; * Состав комиссии по инцидентам ИБ; * Иные ответственные лица. | Наличие функции |
| Возможность заполнения ответственных лиц в области СКЗИ:   * Ответственные за СКЗИ; * Состав комиссии по уничтожению ключевых документов СКЗИ; * Ответственный ОКЗИ. | Наличие функции |
| Возможность заполнения ответственных лиц по классификации ГИС | Наличие функции |
| Возможность назначения ответственных лиц в области КИИ:   * Ответственныеза КИИ; * Состав комиссии по категорированию объектов; * Состав комиссии по инцидентам ИБ; * Состав комиссии по внутреннему контролю. | Наличие функции |
| Возможность назначения иных лиц | Наличие функции |
| Функционал «Инвентаризация»  Учет сведений о следующих активах информационной 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; * пользователи СКЗИ; * помещения СКЗИ; * критерии готовности к эксплуатации СКЗИ. | Наличие функции |
| Функционал «Обучение и тесты»  Проведение инструктажа пользователей работе со средствами криптографической защиты информации | Наличие функции |
| Возможность 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 |
| Формирование 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 |
| Просмотр истории инструктажей и тестировании по вопросам информационной безопасности пройденных сотрудником | Наличие функции |
| Просмотр информации об обучении сотрудника по вопросам информационной безопасности и стаже в области информационной безопасности | 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 |
| Протоколы 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; * фишинг и другие актуальные угрозы ИБ для пользователей. | Наличие функции |
| Возможность создания инструктажей, оформленных во встроенным редактором, в том числе содержащих:   * тексты; * рисунки;   видеоматериалы. | Наличие функции |
| 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. | Наличие функции |
| Функционал «Модель угроз»  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 |
| Оценка исходной защищенности и степени выполнения защитных мер | Наличие функции |
| Выгрузка модели угроз и модели нарушителя, для каждой информационной системы | Наличие функции |
| Функционал «Инвентаризация»  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 реализуемых подсистем информационной безопасности | Наличие функции |
| 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 | Наличие функции |
| Объединение технических средств в логические группы | Наличие функции |
| Учет электронных носителей | 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 безопасности ответственных лиц | Наличие функции |
| Функционал «Сведения об организации»  Управление информацией о сотрудниках | Наличие функции |
| Импорт перечня сотрудников из файла | Наличие функции |
| Экспорт перечня сотрудников из файла | Наличие функции |
| Учет перечня сотрудников | Наличие функции |
| Быстрый поиск сотрудников при назначении лиц, ответственных за мероприятия по информационной безопасности или при допуске сотрудников к защищаемой информации, хранилищам и помещениям | Наличие функции |
| Возможность указания следующей информации о сотруднике:   * фамилию, имя и отчество; * подразделение; * должность; * контактную информацию (адрес электронной почты). | Наличие функции |
| Функционал «Работа с журналами»  Автоматизированное ведение электронного журнала учета СКЗИ | Наличие функции |
| Автоматизированное ведение электронного журнала учета носителей персональных данных | Наличие функции |
| Ведение электронного журнала ознакомления работников с положениями по ПДн | Наличие функции |
| Автоматизированное ведение электронного журнала учета носителей информации для объектов КИИ | Наличие функции |
| Ведение электронного журнала ознакомления работников с положениями о безопасности КИИ | Наличие функции |
| Функционал «Мероприятия»  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 порядку обработки и защиты государственных информационных систем; * мероприятия по организации обеспечения безопасности объектов КИИ. | Наличие функции |
| Информация о мероприятиях по информационной безопасности, включающая в себя:   * 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 (список организаций), ответственном за выполнение мероприятия; * отметку о выполнении мероприятия; * статус; * отчет о выполнении мероприятия; * свидетельства выполнения мероприятия – прикрепленные файлы. | Наличие функции |
| Поддержка фильтрации по следующим полям «группы мероприятия», «тема мероприятия», «эталонность мероприятия», «состояние мероприятия» и «вес мероприятия» в списке мероприятий | Наличие функции |
| Функционал «Задачи»  Назначение задач сотрудникам из числа указанных в приложении | Наличие функции |
| Назначение задач группам сотрудников из числа указанных в приложении | 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 |
| Добавление комментариев к задаче | Наличие функции |
| Отправка сотрудникам уведомлений о назначении задачи, изменении ее свойств и добавлении комментариев | Наличие функции |
| Назначаемые сотрудникам задачи, включающие в себя следующую информацию:   * тема; * дата завершения; * исполнитель или группа исполнителей; * статус; * приоритет; * описание задачи; * отчёт о выполнении задачи или основание для отклонения. | Наличие функции |
| 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 |
| Обеспечение возможности просматривать информацию по задаче и добавлять комментарии без авторизации в приложении | Наличие функции |
| Функционал «Контроль и отчетность»  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; * дата последнего входа пользователей в приложение. | Наличие функции |
| 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 каждого назначенного мероприятия | Наличие функции |
| Функционал «Календарь»  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 |
| Функционал «Инциденты»  Возможность регистрации и управление инцидентами 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; * 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. | Наличие функции |
| Хранение описания инцидента, включающего:   * 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; * отчет о выполнении мер. | Наличие функции |
| Хранение связей с активами информационной безопасности, включающими:   * технические средства; * группы ТС; * информационные системы; * СЗИ; * работники; * связь с другими инцидентами. | Наличие функции |
| Функционал «КИИ». Учет и актуализация 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 |
| Оценка критичности | Наличие функции |
| 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; * тип системы; * используемые технологии; * назначение информационной системы; * отметка об использовании стороннего центра обработки данных (ЦОД) (при наличии);   отметка о наличии сторонних организаций, эксплуатирующих объект КИИ (при наличии). | Наличие функции |
| Учет адреса и состава размещения объекта в составе:   * наименование и адрес организации / филиала; * используемые ОС; * используемое прикладное ПО; * отметка об осуществлении взаимодействия ИС с сетями электросвязи; * используемые сети связи;   технические средства. | Наличие функции |
| Учет адреса и состава размещения ЦОД (при наличии) в составе:   * адрес размещения ЦОД; * используемые ОС; * используемое прикладное ПО; * отметка об осуществлении взаимодействия ИС с сетями электросвязи; * используемые сети связи;   технические средства. | Наличие функции |
| Учет сторонних организацией в ОКИИ (при наличии) в составе:   * сторонняя организация, эксплуатирующая объект КИИ;   тип технического средства. | Наличие функции |
| Учет архитектуры системы | Наличие функции |
| Учет нарушителей и угроз в КИИ в составе:   * 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); * отметка о возможности возникновения компьютерных инцидентов в результате реализации угроз; * возможные типы компьютерных инцидентов (при их наличии);   обоснование отсутствия возможности компьютерных инцидентов (при их отсутствии). | Наличие функции |
| Учет защитных мер в составе:   * принятые организационные меры или обоснование их отсутствия; * принятые меры защиты информации или обоснование их отсутствия; * отметка применяются ли СЗИ в ИС (на объекте КИИ);   используемые СЗИ. | Наличие функции |
| Учет критической информационной инфраструктуры в составе:   * сфера деятельности; * планируемая дата завершения категорирования; * критические процессы, обеспечиваемые системой; * итоговая категория значимости; * обоснования значений показателей критериев значимости или их неприменимости;   значения показателей значимости объекта критической информационной инфраструктуры. | Наличие функции |
| 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 |
| Функционал «Техническая поддержка»  Техническая поддержка в будние дни с 09:00 до 18:00 по Московскому времени | Наличие функции |
| Консультирование пользователей по вопросам, связанным с функционалом работы сервиса, включающим:   * регистрация учетных записей пользователей; * продление тарифа пользователей; * консультирование по вопросам функционального использования приложения (очередность выполнения мероприятий, внесение корректных данных для формирования документации и т.п.); * консультирование по порядку формирования и выгрузки документации. | Наличие функции |
| Техническая поддержка по телефону горячей линии, электронной почте, а также с помощью встроенного функционала по приему обращений в приложении. | Наличие функции |
| Создание обращений в техническую поддержку и отслеживание хода их исполнения с помощью функционала сервиса и возможность добавлять к обращению файлы в форматах: .doc, .docx, .xls, .xlsx, .jpg, .jpeg, .png, .pdf. | Наличие функции |
| Онлайн обмен сообщениями между специалистами Заказчика и Исполнителя по вопросам технической и консультационной поддержки при использовании приложения | Наличие функции |
| Оценка исполнения заявки в техническую поддержку | Наличие функции |
| Руководство по работе с функционалом приложения в HTML-формате | 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 |
| Гарантийная поддержка приложения в течение срока действия лицензии | Наличие функции |
| Исправление ошибок в приложении и документации в рамках гарантийной поддержки | Наличие функции |
| Возможность пролонгации использования приложения без потери имеющихся данных, после завершения срока использования, месяцев | Не менее 12 |
| Бесперебойное функционирование приложения, месяцев | Не менее 12 |

# Требования к разработке организационно-распорядительной и технической документации

Исполнитель обязан оказать услуги по разработке документов в составе и объеме, указанном в Таблице 3.

Таблица 3. Наименование, состав и отчетная документация к оказываемым услугам

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование услуг** | **Отчетная документация** |
| 1 | Разработка организационно-распорядительной и технической документации | Список документов, выгружаемых из приложения автоматизации процессов управления информационной безопасностью:   |  |  | | --- | --- | | 1. | Акт классификации государственной или муниципальной информационной системы *(только для государственных информационных систем)* | | 2. | Акт установления уровня защищённости персональных данных в информационной системе персональных данных*(только для информационных систем с обработкой персональных данных)* | | 3. | Заключение о возможности допуска пользователей к самостоятельной работе с СКЗИ | | 4. | Заключение о возможности эксплуатации СКЗИ на автоматизированных рабочих местах | | 5. | Заключение об оценке вреда субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» | | 6. | Лицевой счёт пользователя СКЗИ | | 7. | План внутренних проверок состояния защиты персональных данных | | 8. | План мероприятий по защите персональных данных | | 9. | План проведения проверок за соблюдением условий использования СКЗИ | | 10. | Политика конфиденциальности для сайта *(если информационная система является веб-сайтом)* | | 11. | Политика обработки персональных данных | | 12. | Приказ о ведении журнала учёта посетителей | | 13. | Приказ о ведении журнала учёта проверок ЮЛ, ИП, проводимых органами государственного контроля (надзора), органами муниципального контроля | | 14. | Приказ о допуске пользователей к работе с СКЗИ | | 15. | Приказ о мерах, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством «О персональных данных» | | 16. | Приказ об организации и обеспечении безопасности информации ограниченного доступа с использованием СКЗИ | | 17. | Приказ об ответственности за обработку, защиту и техническое обслуживание информационных систем с защищаемой информацией | | 18. | Приказ об установлении границ контролируемой зоны объектов информатизации | | 19. | Приказ об утверждении мест хранения материальных носителей, перечня лиц, ответственных за их сохранность и имеющих доступ к ним | | 20. | Приказ об утверждении перечня лиц, имеющих право доступа в помещения с СКЗИ | | 21. | Схема организации криптографической защиты конфиденциальной информации | | 22. | Уведомление об обработке персональных данных или справка о причинах не уведомления в уполномоченный орган | |
| 2 | Разработка и передача Заказчику проектов документов Разработка Модели угроз и нарушителя для ИС (без согласования с ФСТЭК) | Проект документа «Модель угроз и нарушителя информационной безопасности ИС». |
| 3 | Разработка и передача Заказчику проектов документов «Частное техническое задание на подсистему обеспечения информационной безопасности» | Проект документа «Частное техническое задание на подсистему обеспечения информационной безопасности ИС» |
| 4 | Разработка и передача Заказчику проектов документов Технический паспорт (без инвентаризационных данных) | Проект технического паспорта (без инвентаризационных данных) |
| 5 | Сертификат экспертной поддержки | Сертификат экспертной поддержки |
| 6 | Поставка, установка и настройка средств защиты информации | Акт приема-передачи СЗИ |

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС Заказчика (в том числе уязвимостей программного обеспечения, используемого для обеспечения работы ИС Заказчика), возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение, которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (далее - банк данных угроз безопасности информации ФСТЭК России), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИС Заказчика, включающие структуру и состав ИС Заказчика, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС Заказчика, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в ИС и в ее отдельных сегментах, а также иные характеристики ИС Заказчика, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИС Заказчика, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации и нарушителя должна содержать описание ИСЗаказчика и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСЗаказчика, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Потенциал нарушителей определяется в ходе оценки их возможностей, проводимой при определении угроз безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации и нарушителя применяются методические документы, разработанные и утвержденные ФСБ России и ФСТЭК России.

Требования к системе защиты информации ИС Заказчика определяются Исполнителем в зависимости от уровня защищенности ПДн в ИС Заказчика и угроз безопасности информации, включенных в модель угроз безопасности информации.

В рамках оказания услуг Исполнитель разрабатывает «Частное техническое задание на подсистему обеспечения информационной безопасности ИС (далее – частное техническое задание) Заказчика.

Требования к системе защиты информации ИСЗаказчика включаются в частное техническое задание и должны в том числе содержать:

* цель и задачи обеспечения защиты информации в ИС;
* уровень защищенности ИС Заказчика;
* перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС Заказчика;
* перечень объектов защиты ИС Заказчика;
* требования к мерам и средствам защиты информации, применяемым в ИС;
* стадии (этапы работ) создания системы защиты ИС Заказчика;
* требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
* функции заказчика и оператора по обеспечению защиты информации в ИС;
* требования к защите средств и систем, обеспечивающих функционирование ИС (обеспечивающей инфраструктуре);
* требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При определении требований к системе защиты информации ИСЗаказчика учитываются положения политик обеспечения информационной безопасности обладателя информации (Заказчика), а также политик обеспечения информационной безопасности оператора и уполномоченного лица в части, не противоречащей политикам обладателя информации (Заказчика).

Организационные меры и средства защиты информации, применяемые в ИС, должны обеспечивать защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом, определенным по результатам экспертного аудита.

Технические меры защиты информации должны реализовываться посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом должны применяться средства защиты информации и средства вычислительной техники, удовлетворяющие требованиям, предъявляемым к средствам защиты информации и средствам вычислительной техники, применяемым в ИС соответствующего уровня защищенности ПДн.

# Требования к патентной чистоте.

При оказании услуг должны соблюдаться положения законодательства Российской Федерации по соблюдению авторских прав и защите специальных знаков.

# Требования по обеспечению режима конфиденциальности при оказании услуг

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, перечень которой определен внутренним распорядительным документом Заказчика, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с Законодательством Российской Федерации.

**Приложение № 1**

**Перечень средств защиты информации, необходимых к поставке**

| **№№ п/п** | **Наименование средств защиты информации** | **Функциональные характеристики средств защиты информации** | **Кол-во,**  **шт.** |
| --- | --- | --- | --- |
|  | Программно-аппаратный комплекс, реализующий функции криптографического шлюза КС3 | **Общие требования**  Оборудование должно быть новым.  Гарантийный срок на поставляемое оборудование не менее срока действия гарантии производителя.  Количество туннелируемых адресов – неограниченное количество.  ПАК должен выполнять следующие функции криптографического шлюза:  1. Сервер IP-адресов. Функция, которая позволяет обеспечить взаимодействие VPN- узлов. Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.  2. Маршрутизатор VPN-пакетов. Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через криптошлюз на другие защищенные узлы.  3. Сервер соединений. Функция, которая обеспечивает соединение клиентов и других криптошлюзов друг с другом кратчайшим путем.  4. VPN-шлюз. Функция, которая позволяет организовать защищенные соединения между узлами локальных сетей и между сегментами сетей с помощью защищенных каналов (туннелей).  5. Транспортный сервер. Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программного комплекса (далее – ПК) управления VPN-сетью, а также обмен прикладными транспортными конвертами между узлами.  6. Межсетевой экран. Функция, которая позволяет обеспечить фильтрацию IP-трафика. Одновременно криптошлюз может выполнять функции трансляции адресов для проходящего через него открытого трафика.  7. Сервер открытого Интернета. Функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной VPN сети.  **Технические характеристики**  **Требования к аппаратному обеспечению:**  ПАК должен удовлетворять следующим техническим требованиям:  - пропускная способность L3 VPN – до 75 Мбит/с;  - форм-фактор должен быть выполнен MiniPC;  - количество сетевых интерфейсов Ethernet RJ45 10/100/1000 Мбит/с – не менее 3 (трех).  **Требования к совместимости**  ПАК должен быть совместим (по ключевой системе и средствам управления сети) с программным обеспечением, реализующим функции управления защищенной сетью, использующемся в центральном узле системы:  - обновление программного обеспечения,  -обновление справочно-ключевой информацией,  - управление политиками безопасности.  **Требования по сертификации**  1. Должен быть сертифицирован на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3.  2. Должен быть сертифицирован на соответствие требованиям ФСБ России устройствам типа межсетевые экраны 4 класса  Должен быть сертифицирован на соответствие требованиям ФСТЭК России по безопасности информации, установленным в документах:   1. «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 4 уровню доверия, 2. «Требования к межсетевым экранам» (ФСТЭК России, 2016),   3.«Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016). | 9 |
|  | Сертификат активации сервиса совместной технической поддержкина срок 1 год, уровень – Расширенный. | Сертификат активации сервиса совместной технической поддержки представляет собой документ, оформленный в бумажном и/или электронном виде, содержащий информацию о полном названии организации Заказчика, уникальном идентификационном номере сертификата активации технической поддержки, полном списке продуктов, на которые распространяется данный сертификат, и подтверждающий право Заказчика на получение технической поддержки на 9 программно-аппаратных комплексов, реализующих функции криптографического шлюза КС3.  Приём обращений, работа над всеми проблемами и консультирование ведется Поставщиком с учетом режима рабочего времени: с 09:00 до 18:00 по московскому времени.  Приём обращений ведется Поставщиком:  - через web-портал;  - по электронной почте:  - по телефону:  При обращении Заказчик должен предоставить следующую информацию:  - номер сертификата на техническую поддержку;  - наименование компании Заказчика;  - описание возникшей ситуации.  Консультирование Поставщиком при установке Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса установки;  - ответы на вопросы, возникающие при установке.  Консультирование Поставщиком при эксплуатации Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса эксплуатации;  - ответы на вопросы по Продуктам, возникающие в процессе эксплуатации;  - расшифровка кодов ошибок Продуктов;  - оказание консультаций при настройке дополнительного функционала Продуктов;  - разрешение возникших проблем.  Заказчик обязан предоставить Поставщику информацию, достаточную для того, чтобы воспроизвести данную проблему на основании копии Продуктов, и включающую в себя подробное описание проблемы: регистрационные файлы, дампы оперативной памяти, лог-файлы, файлы настроек и пр. Полный список дополнительной информации, необходимой для воспроизведения и анализа проблемы, уточняется при обращении в Службу технической поддержки Поставщика.  Поставщик предоставляет обновление (программные коррекции), а также все изменения, производимые в рамках текущей версии базового программного продукта.  Поставщик предоставляет новые версии базового программного продукта без взимания дополнительной платы.  Новые версии передаются посредством:  - ftp и www серверов заказчика;  - записи экземпляров Продукции на диске и последующей пересылке их Заказчику (не более одного экземпляра на диске каждого Продукта).  Доставка экземпляров ПО осуществляется за счёт Поставщика. | 1 |
|  | Программно-аппаратный комплекс, реализующий функции криптографического шлюза КС3 | **Общие требования**  Оборудование должно быть новым.  Гарантийный срок на поставляемое оборудование не менее срока действия гарантии производителя.  Количество туннелируемых адресов – неограниченное количество.  ПАК должен выполнять следующие функции криптографического шлюза:  Сервер IP-адресов. Функция, которая позволяет обеспечить взаимодействие VPN- узлов. Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.  Маршрутизатор VPN-пакетов. Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через криптошлюз на другие защищенные узлы.  Сервер соединений. Функция, которая обеспечивает соединение клиентов и других криптошлюзов друг с другом кратчайшим путем.  VPN-шлюз. Функция, которая позволяет организовать защищенные соединения между узлами локальных сетей и между сегментами сетей с помощью защищенных каналов (туннелей).  Транспортный сервер. Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений справочников, ключей и программного обеспечения из программного комплекса (далее – ПК)  управления VPN-сетью, а также обмен прикладными транспортными конвертами между узлами.  Межсетевой экран. Функция, которая позволяет обеспечить фильтрацию IP-трафика. Одновременно криптошлюз может выполнять функции трансляции адресов для проходящего через него открытого трафика.  Сервер открытого Интернета. Функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной VPN сети.  **Функциональные требования**  Криптошлюз должен позволять:  Обеспечивать функции прозрачного шифратора протокола IP.  Обеспечивать защиту соединения между удаленными сегментами сети на сетевом и канальном уровне модели OSI.  Выполнять шифрование и имитозащиту сетевого трафика в соответствии с ГОСТ 28147-89.  Шифровать каждый IP-пакет на уникальных симметричных ключах связи с другими VPN-узлами.  Должны поддерживать технологию виртуальных IP-адресов с целью обеспечения связи между защищаемыми сетями с пересекающейся IP адресацией.  Обеспечивать функцию сокрытия сетевой структуры VPN сети, которая обеспечивает работу защищенных компьютеров локальной сети (сегмента сети) в VPN от имени одного адреса;  Поддерживать прозрачную работу через различные NAT-устройства.  Обеспечивать возможность подключения VPN клиентов по протоколам UDP и TCP.  Обеспечивать функции сервера IP-адресов для VPN-узлов для регистрации и предоставления информации о текущих IP-адресах и способах подключения VPN-узлов к VPN-сети.  Выполнять обработку прикладных протоколов (FTP, DNS, H.323, SCCP (Ciscoskinny), SIP) на защищенных узлах, которым назначены виртуальные IP-адреса или для которых выполняется трансляция адресов.  Обеспечивать замкнутость среды функционирования криптосредства.  Выполнять межсетевое экранирование расшифрованного IP-трафика и IP-трафика, подлежащего шифрованию.  Выполнять перехват всего IP-трафика на сетевом уровне модели OSI и блокировать все протоколы, кроме IP.  Обеспечивать межсетевое экранирование по совокупности сетевых параметров (сетевой узел, IP, порт, протокол).  Фиксировать все события, связанные с фильтрацией IP-трафика, в электронном журнале регистрации IP-пакетов.  Принимать централизованные политики безопасности с сервера управления.  Выполнять функции DHСP-сервера и агента DHCP-relay.  Выполнять функцию DNS-сервера.  Выполнять функцию NTP-сервера.  Выполнять функцию HTTP-прокси сервера (HTTP, HTTPS).  Использовать справочную и ключевую информацию, созданную в ПК управления сетью.  Поддерживать работу с виртуальными локальными сетями (VLAN), соответствующими стандарту IEEE 802.1Q.  Обеспечивать возможность агрегации сетевых интерфейсов ПАК – механизм bonding с поддержкой протокола LACP (802.3ad)  Обеспечивать политику качества обслуживания (QoS) приоритетной обработки средствами сервиса дифференцированного обслуживания (DiffServ).  Поддерживать протокол динамической маршрутизации OSPF.  Обеспечивать взаимодействие с источником бесперебойного питания (наличие UPS-службы).  Должен поддерживать мониторинг по протоколу SNMP (включая асинхронный режим работы SNMP Traps).  Поддерживать удаленное администрирование с помощью графического WEB-интерфейса и протокола SSH.  Поддерживать ролевую аутентификацию пользователя и администратора.  Обеспечивать контроль целостности ПО, программных модулей и данных, осуществляемый путем вычисления контрольных значений;  Обеспечивать автоматический прием и обновления справочной и ключевой информации, а также программного обеспечения.  **Требования к аппаратному обеспечению**  - форм-фактор должен быть выполнен в виде MiniPC.  - количество сетевых интерфейсов Ethernet RJ45 10/100/1000 Мбит/с не менее 4 (четырех)  **Требования к сертификации**  Должен быть сертифицирован на соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3.  Должен быть сертифицирован на соответствие требованиям ФСБ России устройствам типа межсетевые экраны 4 класса.  Должен быть сертифицирован на соответствие требованиям ФСТЭК России к устройствам типа межсетевые экраны 3 класса | 1 |
|  | Сертификат активации сервиса совместной технической поддержкина срок 1 год, уровень – Расширенный. | Сертификат активации сервиса совместной технической поддержки представляет собой документ, оформленный в бумажном и/или электронном виде, содержащий информацию о полном названии организации Заказчика, уникальном идентификационном номере сертификата активации технической поддержки, полном списке продуктов, на которые распространяется данный сертификат, и подтверждающий право Заказчика на получение технической поддержки программно-аппаратного комплекса, реализующего функцию криптографического шлюза КС3.  Приём обращений, работа над всеми проблемами и консультирование ведется Поставщиком с учетом режима рабочего времени: с 09:00 до 18:00 по московскому времени.  Приём обращений ведется Поставщиком:  - через web-портал;  - по электронной почте:  - по телефону:  При обращении Заказчик должен предоставить следующую информацию:  - номер сертификата на техническую поддержку;  - наименование компании Заказчика;  - описание возникшей ситуации.  Консультирование Поставщиком при установке Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса установки;  - ответы на вопросы, возникающие при установке.  Консультирование Поставщиком при эксплуатации Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса эксплуатации;  - ответы на вопросы по Продуктам, возникающие в процессе эксплуатации;  - расшифровка кодов ошибок Продуктов;  - оказание консультаций при настройке дополнительного функционала Продуктов;  - разрешение возникших проблем.  Заказчик обязан предоставить Поставщику информацию, достаточную для того, чтобы воспроизвести данную проблему на основании копии Продуктов, и включающую в себя подробное описание проблемы: регистрационные файлы, дампы оперативной памяти, лог-файлы, файлы настроек и пр. Полный список дополнительной информации, необходимой для воспроизведения и анализа проблемы, уточняется при обращении в Службу технической поддержки Поставщика.  Поставщик предоставляет обновление (программные коррекции), а также все изменения, производимые в рамках текущей версии базового программного продукта.  Поставщик предоставляет новые версии базового программного продукта без взимания дополнительной платы.  Новые версии передаются посредством:  - ftp и www серверов заказчика;  - записи экземпляров Продукции на диски и последующей пересылке их Заказчику (не более одного экземпляра на диске каждого Продукта).  Доставка экземпляров ПО осуществляется за счёт Поставщика. | 1 |
|  | Комплекс, реализующий функции межсетевого экрана | **Общие требования**  Оборудование должно быть новым.  Гарантийный срок на поставляемое оборудование не менее срока действия гарантии производителя.  **Технические характеристики**  1.Совместимость (по средствам управления сети) с имеющимся программным обеспечением, реализующим функции управления защищённой сетью ViPNetAdministrator.  2. Встроенная операционная система - адаптированная ОС Linux.  3. Встроенный жёсткий диск.  4. Не менее 4 сетевых интерфейсов 4 x RJ45 1 Гбит/с и 1 x SFP+ 1 Гбит/с.  5. Порты ввода/вывода – VGA – не менее 1; USB – не менее 2.  6.Количество одновременно обслуживаемых соединений – не менее 148 500.  7. Форм-фактор MiniPC.  8. Обеспечение отказоустойчивости путём организации кластера на безе 2-х одинаковых ПАК в конфигурации «активный –пассивный».  9. Обеспечение фильтрации IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам, портам и приложениям в соответствии с настроенными сетевыми фильтрами.  10. Осуществление трансляции сетевых адресов (NAT) для проходящего через устройство трафика.  11. Защита от атак Antispoofing.  12. Обеспечение выполнения функций прокси-сервера для узлов сети, включая:   * поддержку протоколов HTTP и FTP; * проверку и фильтрацию трафика по типу файлов, исполняемых на стороне компьютера клиента; * проверку трафика сторонним антивирусом по протоколу ICAP.   13. Обеспечение фильтрации трафика по следующим параметрам (с помощью технологии DPI):   * по источнику; * по назначению; * по сетевому интерфейсу; * по сетевому протоколу; * по типу приложения; * по типу прикладного протокола; * по методам протокола HTTP/1.1; * по MIME-типу файла;   по пользователю (при настроенном подключении к серверу ActiveDirectory или Captiveportal).  14. Выявление и блокировка прикладных протоколов и приложений среди которых игры, социальные сети, сервисы мгновенных сообщений, видео трансляции, сервисы P2P, torrent, хостинг файлов, туннелирование, VPN, удаленное управление, промышленные протоколы – не менее 2000.  15. Обеспечение поддержки протокола классификации сетевого трафика по приоритетам.  16. Поддержка VLAN (dot1q).  17. Агрегирование каналов связи (bonding (LACP), EtherChannel).  18. Поддержка QoS, ToS, DiffServ.  19. Поддержка серверных функций – DNS-сервер, NTP-сервер, DHCP-сервер, DHCP –Relay.  20. Обеспечение возможности удаленного управления и мониторинга настройками межсетевого экрана.  21. Наличие сертификата соответствия ФСТЭК России, удостоверяющего, что программно-аппаратный комплекс соответствует требования ФСТЭК России к межсетевым экранам типа А 4 класса и межсетевым экранам типа Б 4 класса | 1 |
|  | Сертификат активации сервиса совместной технической поддержки на срок 1 год, уровень – Расширенный. | Сертификат активации сервиса совместной технической поддержки представляет собой документ, оформленный в бумажном и/или электронном виде, содержащий информацию о полном названии организации Заказчика, уникальном идентификационном номере сертификата активации технической поддержки, полном списке продуктов, на которые распространяется данный сертификат, и подтверждающий право Заказчика на получение технической поддержки комплекса, реализующего функции межсетевого экрана.  Приём обращений, работа над всеми проблемами и консультирование ведется Поставщиком с учетом режима рабочего времени: с 09:00 до 18:00 по московскому времени.  Приём обращений ведется Поставщиком:  - через web-портал;  - по электронной почте:  - по телефону:  При обращении Заказчик должен предоставить следующую информацию:  - номер сертификата на техническую поддержку;  - наименование компании Заказчика;  - описание возникшей ситуации.  Консультирование Поставщиком при установке Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса установки;  - ответы на вопросы, возникающие при установке.  Консультирование Поставщиком при эксплуатации Продуктов включает себя:  - предоставление инструкций (документаций) Заказчику относительно процесса эксплуатации;  - ответы на вопросы по Продуктам, возникающие в процессе эксплуатации;  - расшифровка кодов ошибок Продуктов;  - оказание консультаций при настройке дополнительного функционала Продуктов;  - разрешение возникших проблем.  Заказчик обязан предоставить Поставщику информацию, достаточную для того, чтобы воспроизвести данную проблему на основании копии Продуктов, и включающую в себя подробное описание проблемы: регистрационные файлы, дампы оперативной памяти, лог-файлы, файлы настроек и пр. Полный список дополнительной информации, необходимой для воспроизведения и анализа проблемы, уточняется при обращении в Службу технической поддержки Поставщика.  Поставщик предоставляет обновление (программные коррекции), а также все изменения, производимые в рамках текущей версии базового программного продукта.  Поставщик предоставляет новые версии базового программного продукта без взимания дополнительной платы.  Новые версии передаются посредством:  - ftp и www серверов заказчика;  - записи экземпляров Продукции надиски и последующей пересылке их Заказчику (не более одного экземпляра на диске каждого Продукта).  Доставка экземпляров ПО осуществляется за счёт Поставщика. | 1 |
|  | Программный клиент, реализующий функции криптографического шлюза КС2 forWindows | Технические характеристики:   1. Совместимость с программным обеспечением, реализующим функции управления защищенной сетью: обновление программного обеспечения, обновление справочно-ключевой информацией, управление политиками безопасности; 2. Совместимость с комплексом, реализующим функции криптографического шлюза зашифрование/расшифрование направляемого/принимаемого IP-трафика; 3. Реализация криптографических алгоритмов, соответствующих ГОСТ 28147-89; 4. Поддержка операционных систем, используемых заказчиком: MicrosoftWindows 8.1, 10; 5. Функция клиента службы обмена файлами и сообщениями; 6. Функция защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами; 7. Функция контроля запускаемых в операционной системе приложений; 8. Функция контентной фильтрации прикладных протоколов http, ftp; 9. Программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищенной сетью; 10. Взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза); 11. Возможность использования при создании информационных систем персональных данных до 1 класса включительно; 12. Сертификат ФСБ России на СКЗИ по требованиям к СКЗИ класса КС2; 13. Возможность использования в автоматизированных системах не ниже класса 1Г.   Все средства защиты и информации, планируемые к поставке, должны быть сертифицированы как средства защиты информации, что подтверждается сертификатом ФСТЭК/ФСБ. | 3 |
|  | Сертификат активации сервиса совместной технической поддержки программного клиента, реализующий функции криптографического шлюза КС2 forWindows на срок 1 год, уровень – Расширенный | Набор услуг, предоставляемых по сертификату технической поддержки:  - Приём обращений и консультирование по электронной почте с 9:00 до 18:00;  - Приём обращений и консультирование по телефону горячей линии с 9:00 до 18:00;  - Рекомендации по процессу установки продукта в объеме эксплуатационной документации;  - Рекомендации по настройке продукта в объеме эксплуатационной документации;  - Предоставление обновлений (hotfix), устраняющих дефекты, выявленные в продукте;  - Предоставление обновление (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии ПРОДУКТА (servicepack);  - Предоставление новых версий (изменение мажорной (MAJOR) версии, поколения) продукта без взимания дополнительной платы. | 3 |
|  | Дистрибутив программного клиента, реализующего функции криптографического шлюза КС2 forWindows | Диск с дистрибутивом и пользовательской документацией, формуляр и копия сертификата ФСТЭК/ФСБ | 1 |
|  | Комплексное программное средство защиты информации для конечных точек (СЗИ) | ***Должно осуществлять:***   * защиту серверов и рабочих станций от НСД; * контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; * разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации; * разграничение доступа пользователей к информации; * регистрацию событий безопасности и аудит; * паспортизацию используемого программного обеспечения.   ***Требования к сертификации и применению в информационных системах:***  СЗИ должно соответствовать требованиям документов:   * «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» по 4 уровню доверия (ФСТЭК России, 2020); * «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности; * «Требования к средствам контроля съемных машинных носителей информации» не ниже 4 класса защиты (ФСТЭК России, 2014); * «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014).   СЗИ должно допускать использование в следующих информационных системах:   * автоматизированные системы - до класса 1Г (включительно); * государственные информационные системы – до 1 класса защищенности (включительно); * информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); * автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно); * значимые объекты КИИ до 1 категории значимости (включительно).   СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин.  ***Требования к операционной платформе и аппаратной части:***   * СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):   + Windows 11;   + Windows 10;   + Windows 8.1;   + Windows 7 SP1 (при наличии купленной поддержки производителя);   + Windows Server 2022;   + Windows Server 2019;   + Windows Server 2016;   + Windows Server 2012/2012 R2;   + WindowsServer 2008 R2 SP1 (при наличии купленной поддержки производителя). * Должна быть возможность установки СЗИ по произвольному пути. * Должна быть возможность централизованного развертывания СЗИ с использованием SystemCenterConfigurationManager. * СЗИ должно быть подписано WHQL-сертификатом Microsoft. * СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix. * СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMwareESX(i) и MicrosoftHyper-V. * СЗИ должно поддерживать работу с технологией PersonalvDiskCitrixXenDesktop. * СЗИ с централизованным управлением должно функционировать совместно с MicrosoftActiveDirectory. * СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. * СЗИ не должно требовать при развертывании модификации топологии локальной вычислительной сети. * СЗИ должно иметь в составе дистрибутива драйвера для поддержки аппаратных идентификаторов. * В случае совместного применения аппаратных средств доверенной загрузки – должно быть обеспечено наличие свободного разъема системной шины стандарта PCI/PCI Express/Mini PCI Express[[1]](#footnote-2).   ***Требования к функциональности СЗИ:***  СЗИ должно выполнять следующие функции по защите информации:   * Контроль входа пользователей в систему и работа пользователей в системе:   + проверка пароля пользователя при входе в систему;   + поддержка аппаратных средств аутентификации:   - идентификаторы iButton (типы DS1990 — DS1996);  - USB-ключи eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta PKI/BIO, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta PKI/ГОСТ/BIO, JaCarta ГОСТ Flash, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 PKI/ГОСТ/BIO, JaCartaSF/ГОСТ, JaCartaPRO, JaCarta-2 PRO/ГОСТ, JaCartaWebPass, JaCarta-2 SE, JaCartaU2F, JaCartaLT, РутокенS, Рутокен ЭЦП, Рутокен ЭЦП PKI, Рутокен ЭЦП 2.0 Flash, Рутокен ЭЦП 2.0 Touch, Рутокен ЭЦП 2.0 FlashTouch, Рутокен ЭЦП 2.0, Рутокен ЭЦП Bluetooth, РутокенLite, Рутокен 2151, ESMARTToken, ESMARTToken ГОСТ, ESMARTTokenD, Guardant ID, Guardant ID 2.0, R301 Foros, vdToken, Uruguayan ID, с любыми совместимыми USB-считывателями;  - смарт-карты eTokenPRO, eTokenPRO (Java), JaCartaPKI, JaCarta PKI/BIO, JaCarta ГОСТ, JaCarta PKI/ГОСТ/BIO, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 PKI/ГОСТ/BIO, JaCartaPRO, JaCarta-2 PRO/ГОСТ, Рутокен ЭЦП SC, Rutoken ЭЦП 2.0, RutokenLite, Рутокен 2151, ESMARTToken, ESMARTToken ГОСТ, ESMARTTokenD, c любыми совместимыми SC-считывателями;   * + возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;   + возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);   + однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);   + возможность блокирования входа в систему локальных пользователей;   + возможность блокирования операций вторичного входа в систему в процессе работы пользователей;   + возможность блокировки сеанса работы пользователя по истечении интервала неактивности;   + возможность задания временного интервала блокировки компьютера (в минутах) в случае достижения установленного максимального количества попыток ввода неправильного пароля;   + возможность управления политикой сложности паролей;   + поддержка возможности входа в систему по графическому паролю;   + поддержка возможности входа в систему по WindowsLiveID;   + поддержка возможности входа в систему по сертификатам;   + возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей;   + возможность оповещения пользователя о последнем успешном входе в систему;   + возможность выдачи пользователю предупреждения в виде сообщения о том, что в информационной системе реализованы меры защиты информации.   + возможность защиты от локального администратора, обеспечивающая разграничение прав и привилегий между администратором безопасности и администратором IT на управление СЗИ. * Избирательное (дискреционное) управление доступом:   + возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;   + возможность наследования прав доступа для файлов, каталогов и устройств;   + возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту. * Полномочное (мандатное) управление доступом:   + возможность заведения в системе не менее 10 уровней конфиденциальности;   + возможность выбора уровня конфиденциальности сессии для пользователя;   + возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;   + возможность изменения количества мандатных меток в системе и их названий;   + контроль потоков конфиденциальной информации в системе;   + возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP.   + возможность сокрытия файлов (в том числе их названий), имеющих метку конфиденциальности выше, чем уровень допуска пользователя и/или текущий уровень сессии пользователя. * Контроль вывода конфиденциальных данных на печать:   + возможность ограничить перечень мандатных меток информации для печати на заданном принтере;   + теневое копирование информации, выводимой на печать:     - должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;     - должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом WindowsSearch.   + автоматическая маркировка документов, выводимых на печать;   + управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать:     - отдельный вид грифа для каждой мандатной метки;     - отдельный вид маркировки для первой страницы документа;     - отдельный вид маркировки для последней страницы документа;     - вид маркировки для оборота последнего листа;   + поддержка функции печати в файл;   + поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях. * Контроль аппаратной конфигурации компьютера и подключаемых устройств:   + Должны контролироваться следующие устройства:     - последовательные и параллельные порты;     - локальные устройства;     - сменные, физические и оптические диски;     - программно реализованные диски;     - USB-устройства;     - PCMCIA-устройства;     - IEEE1394 (FireWire)- устройства;     - устройства, подключаемые по шине SecureDigital.   + Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.   + Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации.   + Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться.   + Должна быть возможность группового добавления устройств в подсистему контроля устройств без подключения устройства к компьютеру.   + Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации:     - должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;     - должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом WindowsSearch.   + В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя.   + При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств. * Контроль сетевых интерфейсов:   + Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).   + Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя. * Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии ActiveScripts.   + Список модулей, разрешенных для запуска, должен строиться:     - с помощью явного указания модулей;     - по информации об установленных на компьютере программах;     - по зависимостям исполняемых модулей;     - по ярлыкам в главном меню;     - по событиям журнала безопасности. * Контроль целостности файлов, каталогов, элементов системного реестра:   + Должна быть возможность проведения контроля целостности до загрузки операционной системы (при применении с аппаратными средствами доверенной загрузки)[[2]](#footnote-3), в процессе загрузки ОС, в фоновом режиме при работе пользователя.   + Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.   + Должна быть возможность восстановления исходного состояния контролируемого объекта.   + Должна быть возможность расчета контрольных сумм по алгоритму ГОСТ Р 34.11-2012.   + Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.   + При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. * Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей. * Должна быть обеспечена возможность проверки подозрительного ПО с помощью механизмов песочницы. * Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации. * Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации. * Затирание информации на локальных и сменных дисках по команде пользователя. * Возможность настройки количества проходов затирания информации отдельно для локальных дисков, съемных носителей, оперативной памяти. * Затирание данных и имен файлов, каталогов при удалении информации. * Возможность добавления объектов файловой системы в исключения подсистемы затирания данных. * Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. * Функциональный контроль ключевых компонентов системы. * Регистрация событий безопасности в журнале.   + Должна быть возможность формирования отчетов по результатам аудита.   + Должна быть возможность поиска и фильтрации при работе с данными аудита.   + Должна быть возможность аудита изменения политик.   + Должна быть возможность аудита идентификации действий администратора в системе.   + Должна быть возможность аудита отключения защитных подсистем.   СЗИдолжно иметь возможность функционирования совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей[[3]](#footnote-4).  ***Требования к централизованному управлению в доменной сети:***  СЗИ должно предоставлять следующие возможности по управлению системой:   * Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров. * Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты. * Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности. * Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров. * Возможность настройки отображения диаграмм (детализации, цветовой гаммы), добавления, удаления, перемещения диаграмм на панели мониторинга. * Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер). * Выполнение команд, специфичных для защитных подсистем – удаленный запуск антивирусной проверки и обновления базы данных признаков компьютерных вирусов, включение и отключение режима обучения сетевой фильтрации и т.д. * Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера. * Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров. * Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования. * Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз. * Возможность инвентаризации объектов файловой системы компьютера с последующим сохранением отчета в виде эталонного паспорта. Возможность сравнения нового паспорта с эталонным, возможность переопределения эталона. Возможность экспорта данных инвентаризации файловой системы в csv-файл. * Возможность использования механизмов усиленной аутентификации через сервер аутентификации при функционировании СЗИ в сетевом режиме. * Возможность создания отчетов о настройках системы, установленных программах, зарегистрированных аппаратных средствах аутентификации. * Возможность централизованного управления лицензиями СЗИ через сервер безопасности; * Возможность поддержки использования кумулятивных патчей. * Возможность пакетного применения патчей (обычных и кумулятивных). * Возможность создания шаблонов политик:   + возможность создания шаблона по настроенным политикам СЗИ на компьютере;   + возможность проверки соответствия настроенных политик СЗИ на компьютере с выбранным шаблоном;   + возможность распространения (применения) шаблонов политик на компьютер или группу компьютеров. * Централизованное управление в сложной доменной сети (domaintree) должно функционировать по иерархическому принципу, при этом система должна позволять:   + распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов);   + посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов);   + создавать иерархию серверов безопасности с не менее чем 3 уровнями вложенности. * Возможность управление лицензированием продуктов для Windows и Linux систем. * Возможность экспорта и импорта списка рабочих станций с целью подчинения серверу безопасности и для добавления агентов оперативного управления. * Возможность управления сессиями рабочих станций средствами центра управления. * Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности). * Возможность организации иерархической структуры лесов доменов безопасности, в которую можно добавлять леса доменов безопасности на основе несвязанных лесов доменов WindowsAD. | 17 |
|  | Ключ активации сервиса совместной технической поддержки уровня «Расширенный» на 17средств защиты информации для конечных точек на 1год | Обращения Заказчика: самостоятельная регистрация и контроль обращений через web-портал; электронная почта, посредством телефонной связи. Удаленное подключение Исполнителем к Заказчику для помощи в решении обращений.  Доступ к пакетам обновлений в рамках основной версии продукта.  Предоставлять информацию о ходе решения зарегистрированных обращений.  Предоставлять ответы по обращению Заказчика, а именно: готовое решение или рекомендации для решения проблемы.  Информирование о доступных обновлениях продукта по запросу Работа над инцидентами в режиме 8х5 (рабочие дни МСК 10:00-18:00) | 1 |
|  | Средство анализа защищенности на 50 IP-адресов на 1 год | Требования к средству анализа защищенности (САЗ):Требования к основным параметрам и характеристикам  * + 1. Продукт должен функционировать под управлением операционных систем: * Microsoft Windows 7 / 8 / 8.1 / 10;   - Astra Linux Special Edition / Воронеж   * Microsoft Windows Server 2012 R2 / 2016 / 2019;   - Astra Linux Special Edition / Воронеждлясервера.   * + 1. Управление Продуктом должно осуществляться с помощью графической консоли, установленной на сервере Продукта.     2. Лицензия на Продукт должна иметь ограничение согласно лицензии на одновременно добавленные в Продукт элементы ИТ-инфраструктуры, для возможности сканирования, просмотра результатов и контроля. Пользователь должен иметь возможность в пределах имеющейся у него лицензии изменять, добавлять, удалятьсканируемые элементы ИТ-инфраструктуры (IP-адреса, FQDN) без изменения имеющегося у него лицензионного ключа.     3. Продукт должен реализовывать хранение решающих правил (сигнатур), сканируемых объектов ИТ-инфраструктуры, настроек подключения и Продукта с использованием системы управления реляционными базами данных MicrosoftSQLServer.     4. Продукт должен реализовывать обновление базы решающих правил (сигнатур) с использованием репозитория обновлений базы решающих правил Производителя в сети Интернет, защищенных SSL-сертификатом.     5. Продукт должен реализовывать определение перечня сканируемых узлов на основе ключевого атрибута – FQDN (полное доменное имя), IP-адрес элемента ИТ-инфраструктуры:  1. вводом данных о сканируемых узлах в ручном режиме на основании ключевого атрибута; 2. интеграцией с единым каталогом домена MicrosoftActiveDirectory для импорта списка узлов из базы данных домена с сохранением иерархии контейнеров элементов ИТ-инфраструктуры; 3. импортом данных из CSV-файла, содержащем ключевые атрибуты. 4. импортом результатов с обнаруженными узлами сети с помощью сетевого сканирования Nmap.    * 1. Продукт должен поддерживать и иметь возможность проверки сетевого туннеля в агентном режиме системного сканирования, с использованием специального агентского программного обеспечения, устанавливаемого на сканируемый узел.      2. Продукт должен поддерживать и иметь возможность проверки сетевого туннеля в безагентном режиме системного сканирования, с использованием привилегированных учетных записей и соответствующих стандартизованных протоколов.      3. Продукт должен реализовывать аудит в режиме «Пентест» в рамках сетевого сканирования: 5. Продукт должен обеспечивать сканирование портов заданной группы сетевых узлов с возможностью выбора режима профиля, диапазона и типов портов TCP или UDP, с результатом идентификации открытых портов и сервисов в графическом окне Продукта; 6. Продукт должен обеспечивать поиск уязвимостей с возможностью выбора точностисканирования; 7. Продукт должен обеспечивать подбор паролей в виде пары «логин-пароль» для локальных учетных данных к опубликованным сетевым службам методом полного перебора с возможностью использования внешних словарей, результаты которого должны отображаться в графическом окне Продукта.    * 1. Результаты сетевого аудита в режиме «Пентест» в рамках поиска уязвимостей должны отображаться в графическом окне Продукта и содержать: 8. идентификатор уязвимости; 9. определение применимости уязвимости CPE; 10. векторы уязвимости CVSSv2, CVSSv3, CWE; 11. уровень риска обнаруженной уязвимости; 12. описание уязвимости; 13. рекомендуемые меры по устранению уязвимости, ссылки на БДУ УБИ и ресурсы-источники, в которых содержатся сведения об обнаруженных уязвимостях; 14. детализация порта и программного обеспечения обнаруженной уязвимости; 15. уровень точности, используемый при сканировании.     * 1. Продукт должен реализовывать системный аудит уязвимостей системного и прикладного программного обеспечения: 16. Продукт должен обеспечивать сигнатурный анализ данных, собранных при системном сканировании сетевого узла и предоставлять информацию об обнаруженных уязвимостях; 17. Продукт должен обеспечивать сканирование группы сетевых узлов; 18. Продукт должен обеспечивать сканирование следующих платформ:  * Microsoft Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019; * Microsoft Windows XP SP3 / Vista / 7 / 8 / 8.1 / 10; * ALT Linux 6; * ALT Linux SPT 6 / 7 / 8; * Amazon Linux AMI; * Astra Linux; * CentOS Linux 5 / 6 / 7; * Debian 6 / 7 / 8 / 9; * Debian GNU / Linux 2.2 /3.0 /3.1 / 4 / 5 / 6 / 7; * OpenSUSE 11.4 / 12.1 / 12.2 / 12.3 / 13.1 / 13.2; * OpenSUSE Evergreen 11.4; * OpenSUSE Leap 42.1 / 42.2 / 42.3; * Oracle Linux 5 / 6 / 7; * Red Hat Enterprise Linux 5 / 6 / 7; * ROSA DX COBALT 1.0; * ROSA SX COBALT 1.0; * SUSE Linux Enterprise Desktop 10 / 10 SP4 / 11 / 11 SP1 / 11 SP2 / 11 SP3 / 11 SP4 / 12; * SUSE Linux Enterprise Server 10 / 10 SP2 / 10 SP3 / 10 SP4 / 11 / 11 SP1 / 11 SP2 / 11 SP3 / 11 SP4 / 12; * Ubuntu 4.10 / 5.04 / 5.10 / 6.06 / 6.10 / 7.04 / 7.10 / 8.04 / 8.10 / 9.04 / 9.10 / 10.04 / 10.10 / 11.04 / 11.10 / 12.04 / 12.10 / 13.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 18.10; * Photon 1 / 2; * Mageia 4 / 5 / 6 / 7; * Solaris 10 / 11; * FreeBSD 6 / 7; * Cisco IOS; * Huawei VRP; * S-Terra IOS; * CheckPointGAiA; * VMware ESXi Server 5.1 / 5.5 /6.0 / 6.5 / 6.7; * VMware vCenter Server 5.1 / 5.5 / 6.0 / 6.5 / 6.7; * Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017; * MySQL Server 5.5 / 5.6 / 5.7; * Oracle Database Server 11 / 12; * PostgreSQL 8 / 9 / 10 / 11; * IBM DB2.   + 1. Результаты аудита уязвимостей должны отображаться в графическом окне Продукта и содержать:  1. название уязвимости; 2. идентификатор уязвимости; 3. векторы уязвимости CVSSv2, CVSSv3, CWE; 4. уровень опасности обнаруженной уязвимости; 5. описание уязвимости; 6. рекомендуемые меры по устранению уязвимости; 7. наименование ПО, подверженного уязвимости; 8. детализация пути расположения уязвимого ПО;   ссылки на БДУ УБИ и ресурсы-источники, в которых содержатся сведения об обнаруженных   1. уязвимостях.    * 1. Продукт должен реализовывать системный аудит обновлений безопасности, результаты которого должны отображаться в графическом окне Продукта и для каждого узла содержать: 2. наименование обновления; 3. сведения о рисках, связанных с отсутствием недостающего обновления на узле; 4. ссылку на производителя, заявившего о выходе обновления; 5. ссылку на доступное для загрузки обновление в репозитории производителя или аналогичном доверенном хранилище.    * 1. Продукт должен реализовывать системный аудит конфигураций безопасности, выполняя проверку соответствия настроек параметров безопасности системного и прикладного ПО, включая СУБД, по заданному конфигурационному профилю. Результаты аудита должны отображаться в графическом окне Продукта и содержать информацию о степени соответствия сканируемого узла выбранному профилю безопасности:  * MicrosoftWindowsServer 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 (включая роли серверов); * Microsoft Windows XP SP3 / Vista / 7 / 8 / 8.1 / 10; * Astra Linux Special Edition / Воронеж; * CentOS Linux 5 / 6 / 7; * Debian 6 / 7 / 8 / 9; * OpenSUSE 13.1 / 13.2; * OpenSUSE Leap 42.1; * Oracle Linux 5 / 6 / 7; * Red Hat Enterprise Linux 5 / 6 / 7; * SUSE Linux Enterprise Desktop 10 / 11 / 12; * SUSE Linux Enterprise Server 10 / 11 / 12; * Ubuntu 12.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 18.10; * Cisco IOS; * Huawei VRP; * CheckPointGAiA; * VMware vCenter 5.1 / 5.5 / 6.0 / 6.5 / 6.7; * VMware ESXi 5.1 / 5.5 / 6.0 / 6.5 / 6.7; * Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017; * MySQL Server 5.5 / 5.6 / 5.7; * Oracle Database Server 11 / 12; * PostgreSQL 8 / 9 / 10 / 11; * IBM DB2; * Apache HTTP Server; * Apache Tomcat 6 / 7 / 8; * Веб-сервер Nginx; * Компонент PHP; * Microsoft IIS и .Net; * Microsoft Office 2010 / 2013; * Microsoft Internet Explorer 8 / 9 / 10 / 11; * Стандарт PCI DSS 3.2.1; * Конфигурация ГИС. Класс 3 / 4; * Средства защиты информации SecretNet 7, DallasLock 8, КриптоПРОCSP, Континент-АП.   + 1. Продукт должен обладать инструментами по модификации состава и значений параметров профилей аудита и создания собственных конфигураций на основе существующих.     2. Продукт должен реализовывать фиксацию и контроль целостности каталогов и файлов по выбранной маске наименования методом контрольного суммирования (MD5, SHA1, SHA256, SHA512, ГОСТ Р 34.11-2012).     3. Продукт должен реализовывать инвентаризацию программного и аппаратного обеспечения, результаты которой должны отображаться в графическом окне Продукта и для каждого узла содержать:  1. для сканируемых узлов с операционной системой MicrosoftWindows:   Аппаратное обеспечение:   * Список CPU; * Материнская плата; * BIOS; * Слоты памяти; * Видео контроллеры; * Сетевые адаптеры; * Физические диски; * Логические диски; * Приводы чтения лазерных дисков; * USB-устройства.   Программное обеспечение:   * Операционная система; * Службы; * Установленное ПО; * Переменные среды; * Локальные группы; * Локальные пользователи; * Общие папки.   для сканируемых узлов с операционной   1. системой семейства Linux:   Аппаратное обеспечение:   * Список CPU; * Материнская плата; * BIOS; * Слоты памяти; * Сетевые параметры:   + Адаптеры;   + Шлюз;   + DNS-сервер;   Программное обеспечение:   * Операционная система; * Переменные среды; * Локальные пользователи; * Локальные группы; * Установленные пакеты.  1. для сканируемых узлов с платформой VMwareESXiServer:   Аппаратное обеспечение:   * Список CPU; * Материнская плата; * BIOS; * Количество оперативной памяти; * Видео контроллеры; * Сетевые параметры:   + Адаптеры;   + Mac-адрес;   + IP-адрес; * Хранилища данных.   Программное обеспечение:   * Версия ESXi; * Параметры сетевого экрана; * Перечень и статус служб; * Перечень пакетов; * Установленные конфигурационные значения; * Перечень и параметры виртуальных машин.  1. для сканируемых узлов с платформой VMwarevCenterServer:   Программное обеспечение:   * Версия vCenter; * Тип ОС; * Установленные конфигурационные значения; * Перечень и параметры узлов виртуализации, включая аппаратное и программное обеспечение каждого узла.  1. для сканируемых узлов с платформой Cisco IOS, S-Terra IOS:   Аппаратное обеспечение:   * Модель; * Список CPU; * Количество оперативной памяти; * Устройство хранения данных и объем; * Серийные номера узла.   Программное обеспечение:   * Версия Cisco IOS; * Семейство; * Имя узла; * Домен узла; * Значение конфигурационного регистра; * Файловая система; * Конфигурационные файлы; * Службы; * Локальный пользователи; * Списки доступа; * ARP-таблица; * Терминальные линии; * SNMP-строки; * Служба регистрации событий; * Сетевые интерфейсы, включая Mac-адрес, IP-адреса и списки доступа.  1. для сканируемых узлов с платформой CheckPointGAiA:   Аппаратное обеспечение:   * Устройство; * Платформа; * Модель; * Серийный номер; * Список CPU; * Объем оперативной памяти; * Физический накопитель и объем; * Сетевые адаптеры.   Программное обеспечение:   * Версия GAiA; * Параметры сетевых интерфейсов; * Перечень исправлений; * Перечень продуктов с исправлениями.   + 1. Продукт должен реализовывать установку выполненных заданий аудита уязвимостей, аудита конфигураций, инвентаризации и фиксации на контроль для дальнейшего их сравнения с контролируемыми текущими значениями. Результаты должны отображаться в графическом окне Продукта и содержать: * Номер контроля; * Ключевой атрибут сетевого узла; * Статус контроля; * Наименование задания сканирования; * Номер задания сканирования; * Тип задания сканирования; * Дата создания контроля; * Дата завершения задания сканирования; * Детализация соответствия контроля в части добавления, удаления и изменения контролируемых объектов.   + 1. Продукт должен обеспечивать создание заданий по сканированию узлов с параметрами, определяющими время запуска: * выполнение задания сканирования сразу после создания; * разовое выполнение задания сканирования в назначенное время; * выполнение задания сканирования по расписанию с заданной периодичностью.   + 1. Продукт должен иметь возможность автоматического создания именований объектов заданий по заданному шаблону.     2. Продукт должен реализовывать формирование отчетов по результатам сканирования в форматах PDF, XML, HTML: * отчет по выбранному диапазону элементов ИТ-инфраструктуры, по последним результатам сканирования; * отчет по выбранному заданию сканирования; * дифференциальный отчет, сравнивающий два результата сканирования одной задачи за разные промежутки времени.   + 1. Сформированный отчет по результатам сканирования должен содержать следующие разделы: * статистические данные аудита в виде диаграммы или таблицы; * сводную информацию о результатах аудита; * детализированную информацию о данных аудита, сгруппированную по сканируемым элементам ИТ-инфраструктуры.   + 1. Сформированный отчет по результатам аудита конфигураций безопасности должен содержать: * иерархию проверяемых параметров, сгруппированных по классификационному признаку; * сводные данные по количеству параметров с различными состояниями (соответствует эталонному значению/ не соответствует эталонному значению/ не проверено); * ссылку на классификатор CCE; * описание настройки проверяемого параметра; * эталонное (рекомендованное) значение параметра; * текущее значение проверяемого параметра; * описание варианта конфигурации параметра для соответствия рекомендованным значениям.   + 1. Продукт должен обеспечивать отправку отчетов по результатам сканирования заданному списку получателей на электронный почтовый ящик, сетевой каталог.     2. Продукт должен обеспечивать контроль целостности собственных исполняемых файлов, отвечающих за реализацию механизмов безопасности, с использованием метода контрольного суммирования.     3. Продукт должен иметь возможность диагностики собственных служб в графическом окне Продукта, включая проверку работоспособности базы данных, службы синхронизации, службы сканирования и состояния лицензии на Продукт.     4. Производитель Продукта должен предоставить доступ к описаниям уязвимостей, хранящимся на специализированном портале, доступном в сети Интернет:  1. На специализированном портале Производителя по описанию уязвимостей должны содержаться способы (сигнатуры) обнаружения уязвимостей; 2. Описания баз уязвимостей, используемых Продуктом, должны быть выполнены в соответствии с требованиями:  * ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»; * ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;  1. В качества языка описания уязвимостей должен использоваться стандартизованный язык OVAL; 2. Классификаторы уязвимостей, перечни идентифицируемых продуктов, степень опасности, критерии опасности и другая информация о выявленных проблемах безопасности должны быть стандартизованы и выполнены с поддержкойпротокола SCAP (SecurityContentAutomationProtocol).    * 1. Продукт должен иметь возможность импорта и использования сторонних OVAL-определений, предоставляемых Производителем продукта или другими авторитетными источниками.      2. Продукт должен обеспечивать разграничение прав доступа пользователей на основе групп безопасности единого каталога домена MicrosoftActiveDirectory, локальных групп безопасности на сервере Продукта:  * Администратор Продукта с полными правами; * Администратор безопасности; * Пользователь Продукта;   - Администратор обслуживания Продукта, для выполнения обновлений, обслуживания учетных записей сканирования и сканируемых сетевых узлов, диагностики и устранения проблем. | 1 |
|  | Медиа-комплект для сертифицированной версии средства анализа защищенности | Верифицированный дистрибутив с программой на диске;руководства по установке, настройке и работе с Продуктом;формуляр на сертифицированный Продукт, промаркированный голографическим знаком соответствия ФСТЭК России;копия сертификата ФСТЭК России на сертифицированный Продукт, заверенный производителем. | 1 |
|  | Kaspersky Стандартный Certified media Pack Russian Edition. media Pack –Установочныйкомплект | Верифицированный дистрибутив с программой на диске;руководства по установке, настройке и работе с Продуктом;формуляр на сертифицированный Продукт, промаркированный голографическим знаком соответствия ФСТЭК России;копия сертификата ФСТЭК России на сертифицированный Продукт, заверенный производителем. *Эквивалент недопустим т.к. на объекте информатизации Заказчика уже используется ПО KasperskyEndpointSecurity.* | 1 |

Подготовил

Системный администратор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Рачков

1. [↑](#footnote-ref-2)
2. [↑](#footnote-ref-3)
3. [↑](#footnote-ref-4)