ПРИЛОЖЕНИЕ №1 К ДОКУМЕНТАЦИИ

**ВЫПОЛНЕНИЕ КОМПЛЕКСА РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ПУБЛИЧНОГО АКЦИОНЕРНОГО ОБЩЕСТВА «КАЛУЖСКАЯ СБЫТОВАЯ КОМПАНИЯ»**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

ОГЛАВЛЕНИЕ

[1. ОБЩИЕ СВЕДЕНИЯ 4](#_Toc207745952)

[**1.1.** **Заказчик** 4](#_Toc207745953)

[**1.2.** **Исполнитель** 4](#_Toc207745954)

[**1.3.** **Место выполнения работ** 4](#_Toc207745955)

[**1.4.** **Цели и задачи выполнения работ** 5](#_Toc207745956)

[**1.5.** **Состав работ и срок выполнения работ** 5](#_Toc207745957)

[**1.6.** **Нормативно-технические документы, методические материалы, регламентирующие выполнение работ** 5](#_Toc207745958)

[**1.7.** **Перечень сокращений** 6](#_Toc207745959)

[2. ХАРАКТЕРИСТИКИ ОБЪЕКТА ЗАЩИТЫ 7](#_Toc207745960)

[**2.1.** **Характеристики ИСПДн «Свет и тепло»** 7](#_Toc207745961)

[**2.2.** **Характеристики ИСПДн «Документооборот»** 8](#_Toc207745962)

[**2.3.** **Характеристики ИСПДн «Бухгалтерия и кадры»** 8](#_Toc207745963)

[3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ 9](#_Toc207745964)

[4. ТРЕБОВАНИЯ К ПОСТАВЛЯЕМОМУ ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ 10](#_Toc207745965)

[**4.1.** **Общие требования к оборудованию и программному обеспечению ИСПДн ПАО «КСК»** 10](#_Toc207745966)

[**4.1.1.** **Требования к качеству** 10](#_Toc207745967)

[**4.1.2.** **Требования к надежности** 10](#_Toc207745968)

[**4.1.3.** **Требования к гарантийным обязательствам** 10](#_Toc207745969)

[**4.1.4.** **Требования к эргономичности исполнения** 10](#_Toc207745970)

[**4.1.5.** **Требования по безопасности исполнения** 10](#_Toc207745971)

[**4.1.6.** **Требования к эксплуатации и техническому обслуживанию** 10](#_Toc207745972)

[5. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ 11](#_Toc207745973)

[**5.1.** **Требования к выполнению работ по поставке оборудования и программного обеспечения** 11](#_Toc207745974)

[**5.2.** **Требования к выполнению работ по защите информации** 11](#_Toc207745975)

[**5.2.1.** **Требования к работам по обследованию и разработке СЗПДн ИСПДн ПАО «КСК»** 11](#_Toc207745976)

[**5.2.1.1.** **Требования к работам по обследованию ИСПДн ПАО «КСК»** 11](#_Toc207745977)

[**5.2.1.2.** **Требования к формированию требований к СЗПДн ИСПДн ПАО «КСК»** 12](#_Toc207745978)

[**5.2.2.** **Требования к выполнению работ по внедрению СЗПДн ИСПДн ПАО «КСК»** 13](#_Toc207745979)

[**5.2.2.1.** **Требования к установке и настройке оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК»** 13](#_Toc207745980)

[**5.2.2.2.** **Требования к разработке и оформлению Технического паспорта ИСПДн ПАО «КСК»** 13](#_Toc207745981)

[**5.2.2.3.** **Требования к разработке проектов организационно-распорядительных документов** 13](#_Toc207745982)

[**5.2.3.** **Требования к выполнению работ по аттестации ИСПДн ПАО «КСК» на соответствие требованиям по защите информации** 14](#_Toc207745983)

[**5.2.3.1.** **Требования к разработке программы и методик аттестационных испытаний ИСПДн ПАО «КСК»** 14](#_Toc207745984)

[**5.2.3.2.** **Требования к аттестационным испытаниям ИСПДн ПАО «КСК»** 14](#_Toc207745985)

[**5.3.** **Общие требования к документированию** 14](#_Toc207745986)

[**5.4.** **Требования к гарантийным обязательствам на результаты выполненных работ** 14](#_Toc207745987)

[**5.5.** **Общие требования к безопасности работ** 15](#_Toc207745988)

[**5.6.** **Требования к Исполнителю** 15](#_Toc207745989)

[6. ТРЕБОВАНИЯ ПО СДАЧЕ РАБОТ 17](#_Toc207745990)

[**6.1.** **Состав и содержание работ** 17](#_Toc207745991)

[ПРИЛОЖЕНИЕ № 1 Требования к поставляемым товарам и программному обеспечению СЗПДн ИСПДн ПАО «КСК» 19](#_Toc207745992)

1. **ОБЩИЕ СВЕДЕНИЯ**

В соответствии с настоящим Техническим заданием Исполнитель должен выполнить комплекс работ в целях обеспечения защиты персональных данных при их обработке в информационных системах персональных данных Публичного акционерного общества «Калужская сбытовая компания» в соответствии с требованиями законодательства РФ, предъявляемыми к защите персональных данных.

Объектом защиты являются информационные системы персональных данных ПАО «Калужская сбытовая компания», указанные в Таблице № 1.

Таблица № 1

|  |  |
| --- | --- |
| **№ п/п** | **Наименование информационной системы персональных данных** |
|  | Свет и тепло |
|  | Документооборот |
|  | Бухгалтерия и кадры |

Результатом выполнения работ по настоящему Техническому заданию являются системы защиты персональных данных информационных систем персональных данных ПАО «Калужская сбытовая компания», смонтированные и настроенные по адресам, указанным в п. 1.3, обеспечивающие в полном объеме реализацию требований, установленных законодательством в области защиты персональных данных.

* 1. **Заказчик**

Наименование: Публичное акционерное общество «Калужская сбытовая компания» (далее – ПАО «КСК»).

ИНН/КПП: 4029030252 / 402801001.

Юридический адрес: 248001, г. Калуга, пер. Суворова, д. 8.

* 1. **Исполнитель**

Исполнитель определяется по результатам проведения аукциона.

* 1. **Место выполнения работ**

Работы должны быть выполнены по месту размещения технических средств информационных систем персональных данных ПАО «КСК», перечисленных в Таблице № 1, по адресам:

* 248000, Калужская область, г. Калуга, пер. Суворова д.8
* 248000, Калужская область, г. Калуга, улица Циолковского, 4
* 248001, Калужская область, г. Калуга, ул. Ленина, 82
* 248033, Калужская область, г. Калуга, ул. Генерала Попова, 13
* 248000, Калужская область, г. Калуга, ул. Баумана д.3
* 8249039, Калужская область, г. Обнинск, проспект Маркса, 126
* 249210, Калужская область, п. Бабынино, ул. Ленина, д.10
* 249650, Калужская область, п. Барятино, ул. 1 мая, д.6
* 249000, Калужская область, Боровский район, г. Балабаново, ул. Боровская, д.5
* 249300, Калужская область, п. Думиничи, ул. Ленина, д.12
* 249340, Калужская область, г. Жиздра, ул. Луначарского, д.2
* 249192, Калужская область, г. Жуков, ул. Ленина, д.34А
* 249880, Калужская область, с. Износки, ул. Ленина, д. 6а, пом. 2
* 249440, Калужская область, г. Киров, ул. Мира, 23 б
* 249720, Калужская область, г. Козельск, ул. Чкалова, д. 69
* 249832, Калужская область, Дзержинский район, г. Кондрово, пл. Центральная, д. 3, пом. 17
* 249500, Калужская область, Куйбышевский район, п. Бетлица, пер. Порошина, д. 8
* 249842, Калужская область, Дзержинский район, с. Льва-Толстого, ул. Спортивная, д. 16
* 249400, Калужская область, г. Людиново, ул. Рагули, д. 14
* 249096, Калужская область, г. Малоярославец, ул. Горького, д. 33, офис № 1
* 249950, Калужская область, г. Медынь, проспект Ленина, д. 9
* 249240, Калужская область, г. Мещовск, проспект Революции, д. 8
* 249930, Калужская область, г. Мосальск, ул. Энгельса, д. 43а
* 249039, Калужская область, г. Обнинск, проспект Маркса, д. 100
* 249130, Калужская область, с. Перемышль, ул. Коммунаров, д. 43
* 249711, Калужская область, Козельский район, г. Сосенский, ул. Мира, д. 4а
* 249610, Калужская область, г. Спас-Деменск, ул. Советская, д. 102, корпус 2
* 249275, г. Сухиничи, ул. Ленина, д. 74а
* 249100, Калужская область, г. Таруса, ул. Ленина, д. 18
* 249855, Калужская область, Дзержинский район, п. Товарково, ул. Ленина, д. 4а
* 249750, Калужская область, с. Ульяново, ул. Большая Советская, д. 85
* 249800, Калужская область, п. Ферзиково, ул. Карпова, д. 21
* 249360, Калужская область, c. Хвастовичи, ул. Талалушкина, д. 4
* 249910, Калужская область, г. Юхнов, ул. Ленина, д. 13
* 248009, Калужская область, город Калуга, Новаторская ул., д. 6
  1. **Цели и задачи выполнения работ**

Работы выполняются с целью обеспечения защиты персональных данных, содержащихся в информационных системах персональных данных ПАО «КСК», перечисленных в Таблице № 1.

Целями выполнения работ является:

* выполнение требований нормативных правовых актов и методических документов Российской Федерации в сфере защиты персональных данных;
* обеспечение непрерывности процесса защиты персональных данных.

Задачи, которые должны быть решены в ходе выполнения работ:

* реализация технических мер защиты персональных данных;
* аттестация информационных систем персональных данных ПАО «КСК» на соответствие требованиям по защите информации.
  1. **Состав работ и срок выполнения работ**

Начало работ – со дня подписания договора.

Окончание работ – не позднее 01.03.2026 г.

В состав работ по организации защиты персональных данных входит:

* поставка оборудования и программного обеспечения;
* выполнение работ по защите информации.

Сведения об этапах выполнения работ приведены в разделе 6 настоящего Технического задания.

* 1. **Нормативно-технические документы, методические материалы, регламентирующие выполнение работ**
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;
* 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 Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;
* Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
* Приказ ФСБ России от 10.06.2014 № 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 защищённости»;
* Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 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 по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
* ГОСТ Р 59793–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
* ГОСТ 34.602–2020 «Техническое задание на создание автоматизированной системы»;
* ГОСТ 34.201–2020 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды, комплектность и обозначение документов»;
* ГОСТ Р 59795–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
* ГОСТ Р 59853–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
  1. **Перечень сокращений**

В настоящем документе приняты следующие сокращения и обозначения (см. Таблицу № 2).

Таблица № 2

| **Сокращение** | **Расшифровка** |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ИСПДн | Информационная система персональных данных |
| ИСПДн ПАО «КСК» | Информационные системы персональных данных публичного акционерного общества «Калужская сбытовая компания», перечисленные в Таблице № 1 |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| ЛВС | Локальная вычислительная сеть |
| СЗИ | Средство защиты информации |
| СЗПДн | Система защиты персональных данных |
| ФСБ России | Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |

1. **ХАРАКТЕРИСТИКИ ОБЪЕКТА ЗАЩИТЫ**

Объектом защиты являются ИСПДн ПАО «КСК».

ИСПДн ПАО «КСК» обеспечивают:

Взаимодействие с потребителями электроэнергии, учет сотрудников, взаимодействие с  
контрагентами, осуществление документооборота.

Краткие сведения о назначении ИСПДн ПАО «КСК» приведены в Таблице № 3.

Таблица № 3

| **№ п/п** | **Полное название ИС** | **Краткое наименование ИС** | **Назначение ИС** |
| --- | --- | --- | --- |
|  | Информационная система персональных данных «Свет и тепло» | ИСПДн «Свет и тепло» | Взаимодействие с потребителями электроэнергии и потребителями тепла |
|  | Информационная система персональных данных «Документооборот» | ИСПДн «Документооборот» | Осуществление документооборота |
|  | Информационная система персональных данных «Бухгалтерия и кадры» | ИСПДн «Бухгалтерия и кадры» | Учет сотрудников, взаимодействие с контрагентами |

* 1. **Характеристики ИСПДн «Свет и тепло»**

ИСПДн «Свет и тепло» предназначена для автоматизации расчетов с клиентами, осуществления энергосбытовой деятельности, предоставления услуг, оказываемых компанией клиентам на договорной основе.

Серверные элементы ИСПДн «Свет и тепло» размещаются на площадке ПАО «КСК» по адресу: г. Калуга, пер. Суворова, д. 8, и включают в себя 8 физических серверов.

Средства виртуализации в ИСПДн включают в себя 3 виртуальных серверов

Пользовательские элементы ИСПДн включают 431 АРМ администраторов и АРМ пользователей, размещенные в помещениях ПАО «КСК»

* 1. **Характеристики ИСПДн «Документооборот»**

ИСПДн «Бухгалтерия и кадры» предназначена для ведения электронного документооборота и делопроизводства. Серверные элементы ИСПДн «Документооборот» размещаются на площадке ПАО «КСК» по адресу: г. Калуга, пер. Суворова, д. 8, и включают в себя 5 физических серверов.

Средства виртуализации в ИСПДн «Документооборот» включат в себя 2 виртуальных серверов.

Пользовательские элементы ИСПДн «Документооборот» включают 458 АРМ администраторов и АРМ пользователей, размещенные в помещениях ПАО «КСК»

* 1. **Характеристики ИСПДн «Бухгалтерия и кадры»**

ИСПДн «Бухгалтерия и кадры» предназначена для соблюдения порядка и правил приема на работу и исполнения условий трудового договора, установленных трудовым законодательством Российской Федерации, а также для заполнения и использования базы данных автоматизированной информационной системы бухгалтерского учета, персонифицированного учета, налогового учета, в целях повышения эффективности, быстрого поиска, формирования отчётов.

Серверные элементы ИСПДн «Бухгалтерия и кадры» размещаются на площадке ПАО «КСК» по адресу: г. Калуга, пер. Суворова, д. 8, и включают в себя 1 физических серверов.

Средства виртуализации в ИСПДн не включают в себя виртуальных серверов

Пользовательские элементы ИСПДн включают 45 АРМ администраторов и АРМ пользователей, размещенные в помещениях ПАО «КСК».

1. **ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ**

СЗПДн ИСПДн ПАО «КСК» предназначены для обеспечения безопасности персональных данных при их обработке в ИСПДн ПАО «КСК».

СЗПДн ИСПДн ПАО «КСК» должны обеспечивать реализацию организационных и технических мер по обеспечению безопасности персональных данных, установленных приказом ФСТЭК России от 18.02.2013 № 21.

СЗПДн ИСПДн ПАО «КСК» не должны препятствовать нормальному функционированию ИСПДн ПАО «КСК» и смежных систем.

1. **ТРЕБОВАНИЯ К ПОСТАВЛЯЕМОМУ ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ**

Требования приведены в приложении № 1 к настоящему Техническому заданию.

* 1. **Общие требования к оборудованию и программному обеспечению ИСПДн ПАО «КСК»**
     1. **Требования к качеству**

Оборудование, все его компоненты, а также используемые материалы должны быть новыми, не бывшими в эксплуатации.

Оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Российской Федерации предусмотрена обязательная сертификация, с документальным подтверждением при исполнении Договора.

В комплект используемого оборудования должны входить все кабели, необходимые для его подключения и эксплуатации.

* + 1. **Требования к надежности**

Надёжность СЗПДн ИСПДн ПАО «КСК» должна обеспечиваться следующими методами:

* надежностью работы оборудования в целом и его отдельных компонентов, гарантированной производителем;
* схемами подключения оборудования к коммуникационным сетям и электропитанию;
* выполнением требований к организации технического обслуживания и эксплуатации.
  + 1. **Требования к гарантийным обязательствам**

Гарантийный срок на все поставляемое оборудование должен составлять не менее 12 (двенадцати) месяцев с момента передачи Заказчику. Если для какого-либо оборудования стандартные гарантийные сроки, установленные производителем данного оборудования, превышают запрашиваемый гарантийный срок, то гарантийный срок на данное оборудование устанавливается продолжительностью не менее стандартного гарантийного срока, установленного производителем данного оборудования.

Гарантийный срок на результаты выполнения работ составляет 12 (двенадцать) месяцев с даты завершения работ по Договору. Гарантийные обязательства на результаты работ исчисляются с даты подписания Заказчиком документов о приемке.

* + 1. **Требования к эргономичности исполнения**

Размещение оборудования должно обеспечивать удобство его эксплуатации, обслуживания и ремонта.

* + 1. **Требования по безопасности исполнения**

Используемое оборудование и материалы не должны допускать возможности нанесения вреда здоровью или поражения персонала объекта электрическим током и электромагнитными излучениями при условии соблюдения правил эксплуатации оборудования.

* + 1. **Требования к эксплуатации и техническому обслуживанию**

Условия и режим эксплуатации СЗПДн ИСПДн ПАО «КСК», а также параметры технического обслуживания, должны полностью соответствовать требованиям эксплуатационной документации, поставляемой производителем программных и технических средств.

1. **ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ**
   1. **Требования к выполнению работ по поставке оборудования и программного обеспечения**

В рамках выполнения работ Исполнитель должен обеспечить передачу оборудования и программного обеспечения СЗПДн, а также прав использования программного обеспечения в соответствии с требованиями, приведенными в Приложении № 1 к настоящему Техническому заданию.

Доставка Оборудования для осуществления монтажных и пуско-наладочных работ до места выполнения работ осуществляется силами Исполнителя и за счет его средств. Стороны составляют акт, в котором фиксируется факт доставки оборудования до места выполнения работ. Оборудование принимается в упакованном виде (упаковка должна быть) без видимых повреждений, вскрытию в момент доставки не подлежит. Приемка по качеству и количеству Заказчиком не осуществляется.

Программное обеспечение предоставляется на отдельном носителе или по защищенным каналам связи. Исполнитель обязуется одновременно с передачей экземпляров Программного обеспечения предоставить Заказчику ключи, коды и иные подобные сведения, необходимые для использования Программного обеспечения в соответствии с условиями Договора и настоящего Технического задания.

Заказчику в отношении каждой программы для ЭВМ в составе Программного обеспечения должно быть предоставлено право использования такой программы для ЭВМ в соответствии с ее назначением и указанным в документации на Программное обеспечение функционалом на условиях простой (неисключительной) лицензии. Для реализации этого права Заказчику предоставляется право воспроизведения полной рабочей версии любой программы для ЭВМ в составе Программного обеспечения в памяти Оборудования и ее запуска на Оборудовании.

Заказчику в отношении каждого экземпляра Программного обеспечения, поставляемого в рамках Договора, в силу закона принадлежат также права, предусмотренные ст. 1280 Гражданского кодекса Российской Федерации. Исполнитель гарантирует Заказчику возможность беспрепятственного использования этих прав.

Права использования Программного обеспечения должны предоставляться Заказчику для использования на территории Российской Федерации.

Исполнитель гарантирует Заказчику, что права использования Программного обеспечения будут предоставлены Заказчику в объеме, не меньшем, чем указанный в настоящем Техническом задании, а перечень ограничений на использование Программного обеспечения не будет расширен.

* 1. **Требования к выполнению работ по защите информации**

В рамках выполнения работ по защите информации Исполнитель осуществляет:

* обследование и разработка систем защиты персональных данных в информационных системах персональных данных ПАО «КСК»;
* внедрение систем защиты персональных данных в информационных системах персональных данных ПАО «КСК»;
* аттестация информационных систем персональных данных ПАО «КСК»
  + 1. **Требования к работам по обследованию и разработке СЗПДн ИСПДн ПАО «КСК»**

В рамках обследования и разработки СЗПДн ИСПДн ПАО «КСК» Исполнитель осуществляет:

* обследование ИСПДн ПАО «КСК»;
* формирование требований к СЗПДн ИСПДн ПАО «КСК».
  + - 1. **Требования к работам по обследованию ИСПДн ПАО «КСК»**

Для достижения требуемого результата Исполнитель проводит обследование ИСПДн ПАО «КСК» и документально фиксирует исходные данные по ИСПДн ПАО «КСК» в следующем объёме:

* территориальное размещение ИСПДн ПАО «КСК»;
* границы контролируемой зоны ИСПДн ПАО «КСК»;
* назначение, архитектура и конфигурация ИСПДн ПАО «КСК»;
* правовые, организационные и функциональные условия эксплуатации ИСПДн ПАО «КСК»;
* функции ИСПДн ПАО «КСК»;
* перечень информации, обрабатываемой в ИСПДн ПАО «КСК» и подлежащей защите;
  + оснащение ИСПДн ПАО «КСК» программными и техническими средствами:
  + типы, наименования и модели технических средств;
  + типы, наименования и основные (мажорные) версии программного обеспечения;
* оснащение ИСПДн ПАО «КСК» телекоммуникационным оборудованием:
  + типы, наименования и основные (мажорные) версии;
* оснащение ИСПДн ПАО «КСК» средствами защиты информации:
  + типы, наименования и основные (мажорные) версии, сведения о сертификатах соответствия;

Полученные результаты подлежат документальной фиксации в Отчёт по результатам обследования ИСПДн ПАО «КСК», разрабатываемым Исполнителем.

* + - 1. **Требования к формированию требований к СЗПДн ИСПДн ПАО «КСК»**

В рамках формирования требований к СЗПДн ИСПДн ПАО «КСК» Исполнитель осуществляет:

* определение уровня защищенности персональных данных ИСПДн ПАО «КСК»;
* определение актуальных угроз безопасности информации и разработку Модели угроз безопасности информации ИСПДн ПАО «КСК»;
* разработку Частного технического задания на создание СЗПДн ИСПДн ПАО «КСК».
  + - * 1. **Требования к определению уровня защищенности персональных ИСПДн ПАО «КСК»**

Для достижения требуемого результата Исполнитель должен определить уровень защищённости персональных ИСПДн ПАО «КСК» в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Результаты определения уровня защищенности подлежат документальной фиксации в Акте определения уровня защищенности, разрабатываемом Исполнителем для каждой ИСПДн ПАО «КСК» в соответствии с формой, установленной в приложении №3 Приказа Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

* + - * 1. **Требования к определению актуальных угроз безопасности информации и разработке Модели угроз безопасности информации ИСПДн ПАО «КСК»**

Для достижения требуемого результата Исполнитель должен определить угрозы безопасности информации, реализация (возникновение) которых возможна в ИСПДн ПАО «КСК» в условиях их функционирования – актуальных угроз безопасности информации, и для каждой ИСПДн ПАО «КСК» разработать Модель угроз безопасности информации ИСПДн ПАО «КСК» в соответствии с порядком, установленным «Методикой оценки угроз безопасности информации» (ФСТЭК России, 2021).

* + - * 1. **Требования к разработке Частного технического задания на создание СЗПДн ИСПДн ПАО «КСК»**

Для достижения требуемого результата Исполнитель должен разработать для каждой ИСПДн ПАО «КСК» Частное техническое задание на создание СЗПДн ИСПДн ПАО «КСК» в соответствии с ГОСТ 34.602-2020. «Техническое задание на создание автоматизированной системы», который должен содержать организационные и технические требования к СЗПДн ИСПДн ПАО «КСК», подлежащие реализации в СЗПДн ИСПДн ПАО «КСК».

* + 1. **Требования к выполнению работ по внедрению СЗПДн ИСПДн ПАО «КСК»**

Оборудование СЗПДн ИСПДн ПАО «КСК», предназначенное для установки в телекоммуникационные шкафы, должно быть размещено в существующих телекоммуникационных шкафах Заказчика с подключением к существующей системе электроснабжения и ЛВС.

Работы по внедрению СЗПДн ИСПДн ПАО «КСК» должны осуществляется Исполнителем с учетом:

* эксплуатационной документации производителей оборудования и программного обеспечения;
* законодательства в области защиты персональных данных.

Вычислительные мощности для размещения серверных компонент СЗИ ИСПДн ПАО «КСК» предоставляются Заказчиком (при необходимости).

Для выполнения работ по внедрению СЗПДн ИСПДн ПАО «КСК» в части монтажа и коммутации оборудования должны использоваться материалы, предоставляемые Исполнителем.

Работы по внедрению СЗПДн ИСПДн ПАО «КСК» должны включать:

* установку и настройку оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК»;
* разработку и оформление Технического паспорта ИСПДн ПАО «КСК»;
* разработку проектов организационно-распорядительных документов по защите информации.

Заказчик силами своих или привлеченных технических специалистов вправе осуществлять контроль за ведением монтажных работ и пуско-наладочных работ в целях проверки качества и объема проведения соответствующих работ, включая испытания оборудования, на предмет их соответствия условиям Договора и настоящего Технического задания.

* + - 1. **Требования к установке и настройке оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК»**

Установка и настройка оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК» осуществляется Исполнителем и включает:

* базовую инсталляцию поставляемого оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК»;
* настройку поставляемого оборудования и программного обеспечения СЗПДн ИСПДн ПАО «КСК» в объеме достаточном для их корректного функционирования.
  + - 1. **Требования к разработке и оформлению Технического паспорта ИСПДн ПАО «КСК»**

Для достижения требуемого результата Исполнитель должен разработать для каждой ИСПДн ПАО «КСК» Технический паспорт в соответствии с формой, установленной в приложении №1 Приказа Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

* + - 1. **Требования к разработке проектов организационно-распорядительных документов**

Организационно-распорядительные документы разрабатываются Исполнителем и должны определять правила и процедуры, необходимые для обеспечения безопасности информации, обрабатываемой в ИСПДн ПАО «КСК».

Разработка проектов организационно-распорядительных документов по защите информации осуществляется в объеме, достаточном для успешного проведения аттестационных испытаний ИСПДн ПАО «КСК» по требованиям защиты персональных данных.

* + 1. **Требования к выполнению работ по аттестации ИСПДн ПАО «КСК» на соответствие требованиям по защите информации**

Работы по аттестации на соответствие требованиям по защите информации для каждой ИСПДн ПАО «КСК» должны включать:

* разработку Программы и методик аттестационных испытаний ИСПДн ПАО «КСК»;
* аттестационные испытания ИСПДн ПАО «КСК».
  + - 1. **Требования к разработке программы и методик аттестационных испытаний ИСПДн ПАО «КСК»**

Программа и методики аттестационных испытаний ИСПДн ПАО «КСК» разрабатывается Исполнителем и должна содержать описание комплекса мероприятий, по результатам проведения, которых Исполнителем принимается решение о соответствии ИСПДн ПАО «КСК» требованиям по защите информации.

Программа и методики аттестационных испытаний ИСПДн ПАО «КСК» должна разрабатываться в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утверждённым приказом ФСТЭК России от 29.04.2021 № 77, с учётом ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

* + - 1. **Требования к аттестационным испытаниям ИСПДн ПАО «КСК»**

Аттестационные испытания ИСПДн ПАО «КСК» должны проводиться в порядке, установленном приказом ФСТЭК России от 29.04.2021 № 77.

Аттестационные испытания ИСПДн ПАО «КСК», проводимые Исполнителем, должны включать:

* проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СЗПДн ИСПДн ПАО «КСК» установленным требованиям;
* анализ уязвимостей ИСПДн ПАО «КСК»;
* документальное оформление результатов аттестационных испытаний ИСПДн ПАО «КСК», включая:
  + Протокол аттестационных испытаний ИСПДн ПАО «КСК»;
  + Заключение по результатам аттестационных испытаний ИСПДн ПАО «КСК»;
  + Аттестат соответствия ИСПДн ПАО «КСК» требованиям по защите информации (в случае положительных результатов аттестационных испытаний).
  1. **Общие требования к документированию**

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Вся отчетная документация должна быть оформлена и передана Заказчику следующим образом:

* на бумажных носителях в одном экземпляре;
* на USB-носителе в формате Word и PDF.
  1. **Требования к гарантийным обязательствам на результаты выполненных работ**

Гарантийный срок на результаты выполнения работ составляет 12 (двенадцать) месяцев с даты подписания Заказчиком документов о приемке. Гарантийные обязательства на результаты работ исчисляются с даты завершения работ по Договору.

Гарантийное сопровождение осуществляется сотрудниками Исполнителя удаленно, с использованием защищенных каналов связи.

Гарантийная поддержка осуществляется в режиме: Рабочие дни 8х5 (с 9.00 до 18.00 по Московскому времени.

С целью надлежащего обеспечения гарантийного сопровождения Исполнителем Заказчик обязуется:

* в течение 2 (двух) рабочих дней с даты подписания документов о приемке предоставить Исполнителю акт приема-передачи парольно-ключевой информации, в котором фиксирует всю информацию, необходимую Исполнителю для дистанционной работы с оборудованием и программным обеспечением;
* обеспечить Исполнителю доступ к программным и техническим средствам, подлежащим гарантийному сопровождению в соответствии с документами, устанавливающими порядок предоставления доступа к техническим средствам ИСПДн ПАО «КСК»;

оказывать содействие Исполнителю при организации дистанционного подключения к программным и техническим средствам, подлежащим гарантийному сопровождению.

* 1. **Общие требования к безопасности работ**

Все сведения о составе и характеристиках объектов информатизации Заказчика являются конфиденциальной информацией.

Исполнитель обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;
* не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика;
* не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика;
* не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика;
* не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами.

Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

* 1. **Требования к Исполнителю**

Исполнитель должен соответствовать требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим выполнение работ, являющихся объектом закупки, а именно:

* наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20», «21» Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16.04.2012 № 313;
* наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «г», «д», «е», пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03.02.2012 № 79.

1. **ТРЕБОВАНИЯ ПО СДАЧЕ РАБОТ**
   1. **Состав и содержание работ**

Требования по порядку сдачи работ и составу отчетной документации приведены в Таблице № 4

Исполнитель вправе досрочно выполнить работы, а Заказчик вправе принять и оплатить указанные работы.

Результаты выполнения работ должны быть представлены Заказчику в рабочие часы Заказчика: понедельник – четверг: с 9 часов 00 минут до 18 часов 00 минут (время московское), пятница – с 9 часов 00 минут до 16 часов 45 минут (время московское).

Таблица № 4

| **№** | **Наименование работ** | **Сроки выполнения работ** | | **Стоимость  работ, руб.** | **Результаты работ** |
| --- | --- | --- | --- | --- | --- |
| **Начало работ** | **Окончание работ** |
|  | **Этап № 1. Поставка оборудования и программного обеспечения** | С даты заключения Договора | Не позднее 01.03.2026 г. |  | 1. Документ о приемке, подписанный Заказчиком. |
|  | **Этап № 2. Выполнение работ по защите информации** | С даты заключения Договора | Не позднее 01.03.2026 г. |  | 1. Отчетные документы:  * Отчет по результатам обследования ИСПДн ПАО «КСК»; * Модель угроз безопасности информации ИСПДн ПАО «КСК»; * Акт классификации ИСПДн ПАО «КСК»;   Частное техническое задание на создание СЗПДн ИСПДн ПАО «КСК»;   * Технический паспорт ИСПДн ПАО «КСК»; * Комплект организационно-распорядительных документов по защите информации; * Программа и методики аттестационных испытаний ИСПДн ПАО «КСК»; * Протокол проведения аттестационных испытаний ИСПДн ПАО «КСК»; * Заключение по результатам аттестационных испытаний ИСПДн ПАО «КСК»; * Аттестат соответствия ИСПДн ПАО «КСК» требованиям по защите информации (в случае положительных результатов аттестационных испытаний ИСПДн ПАО «КСК»).  1. Документ о приемке, подписанный Заказчиком. |

**ПРИЛОЖЕНИЕ № 1  
Требования к поставляемым товарам и программному обеспечению СЗПДн ИСПДн ПАО «КСК»**

Таблица № 1 – Требования к оборудованию и программному обеспечению СЗПДн ИСПДн ПАО «КСК»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Наименование** | **Характеристики** | **Количество, шт.** | Начальная максимальная цена за единицу\*\*, руб. без НДС |
|  | Программное обеспечение средства анализа защищенности.  Код ОКПД 2 – 58.29.50.000 | 1. Срок использования: 12 (двенадцать месяцев). 2. Количество ip-адресов для единовременного сканирования: 480. 3. Способ предоставления: на бумажном носителе. 4. Технические требования.    1. Общие требования       1. Лицензионный программный продукт (далее – Продукт) должен обеспечивать функции: обнаружение хостов, сетевой аудит в режиме «Пентест», идентификация открытых сетевых портов и сервисов, подбор паролей к СУБД и сетевым службам, аудиты уязвимостей системного и прикладного программного обеспечения, выявление недостающих обновлений безопасности, инвентаризацию аппаратного и программного обеспечения сканируемых систем, контроль целостности, формирование отчетов по результатам сканирования.       2. Поставщики Продукта должны предоставить Сертификат соответствия требованиям безопасности информации ФСТЭК России, удостоверяющий соответствие Продукта техническим условиям, средствам контроля (анализа) защищенности информации, Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (ФСТЭК России, 2018г.) – 4 уровень доверия.       3. Продукт должен реализовать меры защиты ОПС.2, АНЗ.1, АНЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.1, ЗСВ.7 согласно документам «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утвержден приказом ФСТЭК России № 17 от 11.02.2013) и «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утвержден приказом ФСТЭК России № 21 от 18.02.2013), меры защиты АУД.1, АУД.2, АУД.7, АУД.10, АУД.11, ОЦЛ.1, УКФ.1, ОПО.1, ОПО.2, ОПО.4 согласно документа «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утвержден Приказом ФСТЭК России № 239 от 25.12.2017г.).       4. Производитель продукта предоставляет техническую (базовую) поддержку Продукта, включающую:  * Предоставление актуальной документации и других информационных материалов по настройке и эксплуатации Продукта; * Предоставление новых релизов, обновлений Продукта в соответствии с их лицензионными соглашениями; * Консультации по порядку доступа и использования «Центра сертифицированных обновлений»; * Консультация по реализации мер защиты с помощью Продукта.   1. Требования к основным параметрам и характеристикам      1. Продукт должен функционировать под управлением операционных систем: * Astra Linux 1.7 (Воронеж).   + 1. Управление Продуктом должно осуществляться с помощью графической консоли, установленной на сервере Продукта, доступной в сети ИТ-инфраструктуры, с использованием стандартизованного веб-браузера.     2. Лицензия на Продукт должна иметь ограничение на не менее 480 (четырехсот восьмидесяти) одновременно добавленных в Продукт элементов ИТ-инфраструктуры, для возможности сканирования, просмотра результатов и контроля. Пользователь должен иметь возможность в пределах имеющейся у него лицензии изменять, добавлять, удалять сканируемые 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 Microsoft SQL Server, PostgreSQL Server, Jatoba.     4. Продукт должен реализовывать обновление базы решающих правил (сигнатур): * с использованием репозитория обновлений базы решающих правил Производителя в сети Интернет, защищенных SSL-сертификатом; * с использованием репозитория обновлений базы данных решающих правил Производителя в сети Интернет, защищенных SSL-сертификатом, с помощью прокси-сервера в сети ИТ-инфраструктуры; * с использованием локального адреса (директории), после загрузки обновлений базы данных решающих правил с сайта Производителя, защищенного парой логин-пароль.   + 1. Продукт должен реализовывать определение перечня сканируемых узлов на основе ключевого атрибута – FQDN (полное доменное имя), IP-адрес элемента ИТ-инфраструктуры: * вводом данных о сканируемых узлах в ручном режиме на основании ключевого атрибута; * интеграцией с единым каталогом домена Microsoft Active Directory для импорта списка узлов из базы данных домена элементов ИТ-инфраструктуры; * импортом данных из CSV-файла, содержащем ключевые атрибуты. * импортом результатов с обнаруженными узлами сети с помощью сетевого сканирования.   + 1. Продукт должен иметь в рамках отдельного задания, выполнения его по расписанию и создания отчета возможность обнаружения узлов сети по заданному диапазону, импорта их в систему, возможность экспорта во внешний файл в формате CSV, содержащего информацию по обнаруженным активам в рамках сетевого сканирования.     2. Результаты сетевого аудита «Обнаружение хостов» в рамках обнаружения узлов сети должны отображаться в графическом окне Продукта и содержать: * Количество обнаруженных узлов сети; * Количество новых узлов сети в сравнении с ранее добавленными; * Способ обнаружения; * IP-адрес; * DNS-имя; * FQDN; * NetBIOS; * Данные об установленной операционной системе в виде CPE; * Информацию о наличии доступного агента Продукта.   + 1. Продукт должен реализовывать аудит в режиме «Пентест» в рамках сетевого сканирования: * 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; * Продукт должен обеспечивать поиск уязвимостей с возможностью выбора точности сканирования; * Продукт должен обеспечивать возможность создания и сохранения для дальнейшего использования собственного профиля сканирования; * Продукт должен обеспечивать подбор паролей в виде пары «логин-пароль» для локальных учетных данных к опубликованным сетевым службам Microsoft SQL, PostgreSQL, OracleDB, MySQL, SSH, FTP, POP3 методом полного перебора с возможностью использования внешних словарей, результаты которого должны отображаться в графическом окне Продукта; * Продукт должен иметь встроенную базу «логин-пароль», содержащую не менее 3000 записей, а также иметь возможность подключения собственных словарей.   + 1. Результаты сетевого аудита в режиме «Пентест» в рамках поиска уязвимостей должны отображаться в графическом окне Продукта и содержать: * идентификатор уязвимости ALTXID, BDU ID, CVE (при наличии); * сетевой порт, на котором обнаружена уязвимость; * уровень риска обнаруженной уязвимости; * уровень точности, используемый при сканировании. * описание уязвимости; * продукты, в которых обнаружена уязвимость; * определение применимости уязвимости CPE; * векторы уязвимости CWE, CVSSv2, CVSSv3; * детализация программного обеспечения обнаруженной уязвимости;   + 1. Продукт должен реализовывать системный аудит уязвимостей системного и прикладного программного обеспечения: * Продукт должен обеспечивать сигнатурный анализ данных, собранных при системном сканировании сетевого узла и предоставлять информацию об обнаруженных уязвимостях; * Продукт должен обеспечивать сканирование группы сетевых узлов; * Продукт должен обеспечивать сканирование следующих платформ: * Microsoft Windows: * Microsoft Windows 10; * Отечественные ОС: * Astra Linux SE Орел/Воронеж/Смоленск 1.7;   + 1. Результаты аудита уязвимостей должны отображаться в графическом окне Продукта и содержать: * название уязвимости; * идентификатор уязвимости CVE; * векторы уязвимости CVSSv2, CVSSv3, CWE; * уровень опасности обнаруженной уязвимости; * описание уязвимости; * рекомендуемые меры по устранению уязвимости; * наименование ПО, подверженного уязвимости; * детализация пути расположения уязвимого ПО; * ссылки на БДУ УБИ и ресурсы-источники, в которых содержатся сведения об обнаруженных уязвимостях.   + 1. Продукт должен реализовывать системный аудит обновлений безопасности, результаты которого должны отображаться в графическом окне Продукта и для каждого узла содержать: * наименование обновления; * сведения о рисках, связанных с отсутствием недостающего обновления на узле; * ссылку на производителя, заявившего о выходе обновления; * ссылку на доступное для загрузки обновление в репозитории производителя или аналогичном доверенном хранилище.   + 1. 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.     2. Продукт должен реализовывать инвентаризацию программного и аппаратного обеспечения, результаты которой должны отображаться в графическом окне Продукта и для каждого узла содержать: * для сканируемых узлов с операционной системой Microsoft Windows:   Аппаратное обеспечение:   * Список CPU; * Материнская плата; * BIOS; * Слоты памяти; * Видео контроллеры; * Сетевые адаптеры; * Физические диски; * Логические диски; * Приводы чтения лазерных дисков;   Программное обеспечение:   * Операционная система; * Службы; * Установленное ПО; * Переменные среды; * Локальные группы; * Локальные пользователи; * Общие папки. * для сканируемых узлов с операционной 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. Продукт должен реализовывать установку выполненных заданий аудита уязвимостей, 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 в рамках отдельного задания, выполнения его по расписанию и создания отчета возможность проверки сетевого туннеля в агентном и безагентном режимах системного сканирования, с возможностью множественного выбора привилегированных учетных записей и соответствующих стандартизованных протоколов SSH, HTTP, WinRM c использованием протокола Kerberos.     2. Продукт должен реализовывать формирование отчетов по предварительно заданному профилю сканирования с возможностью определять количественные оценки уязвимостей в безопасности компьютерной системы по стандартам CVSSv2 и CVSSv3 по результатам сканирования в форматах HTML, PDF, MHT, CSV, XML: * 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. Продукт должен обеспечивать возможность формирования отчетов по заранее созданному шаблону и отправку отчетов по результатам сканирования заданному списку получателей на электронный почтовый ящик, сетевой каталог.     2. Продукт должен обеспечивать удаление неактуальных результатов сканирований и отчётов для уменьшения размера баз данных вручную и по заданному расписанию, а также уведомлять о превышении размеров баз данных на указанный адрес электронной почты.     3. Продукт должен обеспечивать контроль целостности собственных исполняемых файлов, отвечающих за реализацию механизмов безопасности, с использованием метода контрольного суммирования.     4. 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.     5. Производитель Продукта должен предоставить доступ к описаниям уязвимостей, хранящимся на специализированном портале, доступном в сети Интернет: * На специализированном портале Производителя должны содержаться описания уязвимостей и ссылки на источники информации, базы знаний; * 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»; * В качества языка описания уязвимостей должен использоваться стандартизованный язык OVAL; * Классификаторы уязвимостей, перечни идентифицируемых продуктов, степень опасности, критерии опасности и другая информация о выявленных проблемах безопасности должны быть стандартизованы и выполнены с поддержкой протокола SCAP (Security Content Automation Protocol).   + 1. Продукт должен иметь возможность импорта и использования сторонних OVAL-определений, предоставляемых Производителем продукта или другими авторитетными источниками.     2. Продукт должен обеспечивать возможность аутентификации в единой Web-консоли управления с помощью внутренних локальных учетных записей, а также с помощью Windows-аутентификации с использованием протокола Kerberos.     3. Продукт должен обеспечивать разграничение прав доступа пользователей на основе групп безопасности единого каталога домена Microsoft Active Directory, 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 | 398 400,00 |
|  | Установочный комплект средства анализа защищенности.  Код ОКПД 2 – 58.29.12.000 | 1. Установочный комплект САЗС должен быть полностью совместим с САЗС, характеристики которого представлены в п.п. 1 настоящей таблицы. 2. Установочный комплект САЗС должен поставляться в виде CD-диска в комплекте с заверенной копией сертификата ФСТЭК России, формуляром и кратким руководством | 1 | 1 583,33 |
|  | Ключ активации сервиса технической поддержки для АПКШ "Континент" \*  Код ОКПД 2 – 62.02.30.000 | 1. Ключ активации сервиса прямой технической поддержки уровня "Стандартный" для АПКШ "Континент" 3.9. Отказоустойчивый (HA) кластер 2-х Криптошлюзов. Платформа IPCR50. KC3. 2. Количество поддерживаемых АПКШ "Континент": 2. 3. Срок действия технической поддержки: 12 (двенадцать) месяцев. 4. Способ предоставления: посредством отправки на электронную почту представителя Заказчика, в виде электронной скан-копии формата PDF. 5. Общие требования:  * Самостоятельная регистрация и контроль обращений через портал самообслуживания * Работа над инцидентами в режиме 8х5 (рабочие дни МСК 10:00–18:00) * Консультирование по установке и использованию продукта * Информирование о доступных обновлениях продукта по запросу * Доступ к пакетам обновлений продукта * Доступ к БЗ (известные ошибки и типовые решения) * Прием предложений по улучшению продукта. | 1 | 491 472,00 |
|  | Продление права на использование АПКШ "Континент" (платформа IPC-25) \*  Код ОКПД 2 – 58.29.50.000 | 1. Продление права на использование АПКШ "Континент". Версия 3.9" на платформе IPC-25. Криптошлюз. 2. Количество АПКШ, на которые продлеваются права на использование АПКШ: 2 3. Срок действия права: бессрочно. 4. Уровень включенной технической поддержки: базовый. 5. Срок действия включенной технической поддержки: 12 (двенадцать) месяцев. 6. Способ предоставления: посредством отправки на электронную почту представителя Заказчика, в виде электронной скан-копии формата PDF. | 1 | 266 964,00 |
|  | Продление права на использование АПКШ "Континент" (платформа IPC-100) \*  Код ОКПД 2 – 58.29.50.000 | 1. Продление права на использование АПКШ "Континент". Версия 3.9" на отказоустойчивом кластере из 2-х платформ IPC-100. Криптошлюз. КС3. 2. Количество АПКШ в виде отказоустойчивого кластера, на которые продлеваются права на использование АПКШ: 2. 3. Срок действия права: бессрочно. 4. Уровень включенной технической поддержки: базовый. 5. Срок действия включенной технической поддержки: 12 (двенадцать) месяцев. 6. Способ предоставления: посредством отправки на электронную почту представителя Заказчика, в виде электронной скан-копии формата PDF. | 1 | 428 828,00 |
|  | Установочный комплект для обновления АПКШ "Континент" \*  Код ОКПД 2 – 58.29.12.000 | 1. Установочный комплект АПКШ должен быть полностью совместим с АПКШ, характеристики которого представлены в п.п. 4,5 настоящей таблицы. 2. Установочный комплект АПКШ должен поставляться в виде CD-диска в комплекте с заверенной копией сертификата ФСТЭК России, формуляром и кратким руководством. | 3 | 1 333,33 |
|  | Средство защиты информации для ОС Linux (модуль межсетевого экрана).  Код ОКПД 2 – 58.29.50.000 | 1. Срок использования: бессрочно. 2. Количество защищаемых объектов: 111. 3. Способ предоставления: посредством отправки на электронную почту представителя Заказчика, в виде электронной скан-копии формата PDF. 4. Уровень включенной технической поддержки: базовый. 5. Срок действия включенной технической поддержки: 12 (двенадцать) месяцев. 6. Технические требования.    1. Средство защиты информации должно осуществлять:  * контроль входа пользователей в систему, в том числе с использованием аппаратных средств защиты; * уничтожение (затирание) содержимого файлов при их удалении; * очистку освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств); * контроль целостности ключевых компонентов Secret Net LSP и объектов файловой системы; * межсетевое экранирование сетевого трафика; * регистрацию событий безопасности в журналах; * проведение аудита действий субъектов (пользователей, процессов) с объектами файловой системы и аудита сетевых соединений   1. Требования к операционной системе и аппаратной части: * Операционные системы:  | ОС | Версия ядра | | | | --- | --- | --- | --- | | Ред ОС 7.3  (DE: MATE) | 5.10.29-1.el7.x86\_64  5.15.35-1.el7.3.x86\_64  5.15.87-1.el7.3.x86\_64  5.15.106-1.el7.3.x86\_64  5.15.117-1.el7.3.x86\_64  5.15.125-1.el7.3.x86\_64  5.15.131-1.el7.3.x86\_64  6.1.20-2.el7.3.x86\_64  6.1.44-1.el7.3.x86\_64  6.1.52-1.el7.3.x86\_64  6.1.85-1.el7.3.x86\_64  6.1.94-1.el7.3.x86\_64  6.1.110-1.el7.3.x86\_64 | | | | Ред ОС 8  (DE: MATE) | 6.6.6-1.red80.x86\_64  6.6.26-1.red80.x86\_64  6.6.51-1.red80.x86\_64 | | | | Альт 8 СП релиз 9  (DE: MATE) | 5.10.110-std-def-alt0.c9f.2  5.10.176-std-def-alt0.c9f.2  5.10.185-std-def-alt0.c9f.2  5.10.188-std-def-alt0.c9f.2  5.10.198-std-def-alt0.c9f.2  5.10.199-std-def-alt0.c9f.2  5.10.206-std-def-alt0.c9f.2  5.10.214-std-def-alt0.c9f.2  5.10.219-std-def-alt0.c9f.2  5.10.221-std-def-alt0.c9f.2  5.10.224-std-def-alt0.c9f.2 | | | | Альт 8 СП релиз 10  (DE: MATE) | 6.1.29-un-def-alt1  6.1.85-un-def-alt0.c10f.1 | | | | Альт Рабочая станция/Сервер 9  (DE: MATE) | 5.4.236-std-def-alt1  5.4.238-std-def-alt1  5.4.240-std-def-alt1  5.4.242-std-def-alt1  5.4.243-std-def-alt1  5.4.244-std-def-alt1  5.4.245-std-def-alt1  5.4.247-std-def-alt1  5.4.248-std-def-alt1  5.4.249-std-def-alt1  5.4.250-std-def-alt1  5.4.251-std-def-alt1  5.4.252-std-def-alt1  5.4.254-std-def-alt1  5.4.256-std-def-alt1  5.4.257-std-def-alt1  5.4.258-std-def-alt1  5.4.259-std-def-alt1  5.4.260-std-def-alt1  5.4.261-std-def-alt1  5.4.265-std-def-alt1  5.4.266-std-def-alt1  5.4.267-std-def-alt1 | 5.4.268-std-def-alt2  5.4.269-std-def-alt1  5.4.271-std-def-alt1  5.4.272-std-def-alt1  5.4.273-std-def-alt1  5.4.274-std-def-alt1  5.4.275-std-def-alt1  5.4.277-std-def-alt1  5.4.278-std-def-alt1  5.4.279-std-def-alt1  5.4.281-std-def-alt1  5.4.282-std-def-alt1  5.4.284-std-def-alt1  5.10.118-un-def-alt1  5.10.174-un-def-alt1  5.10.176-un-def-alt1  5.10.177-un-def-alt1  5.10.179-un-def-alt1  5.10.180-un-def-alt1  5.10.181-un-def-alt1  5.10.182-un-def-alt1  5.10.184-un-def-alt1 | 5.10.185-un-def-alt1  5.10.186-un-def-alt1  5.10.187-un-def-alt1  5.10.188-un-def-alt1  5.10.189-un-def-alt1  5.10.191-un-def-alt1  5.10.192-un-def-alt1  5.10.194-un-def-alt1  5.10.195-un-def-alt1  5.10.197-un-def-alt1  5.10.198-un-def-alt1  5.10.199-un-def-alt1  5.10.200-un-def-alt1  5.10.205-un-def-alt1  5.10.206-un-def-alt1  5.10.208-un-def-alt1  5.10.209-un-def-alt2  5.10.215-un-def-alt1  5.10.216-un-def-alt2  5.10.218-un-def-alt1  5.10.219-un-def-alt1  5.10.226-un-def-alt1 | | Альт Рабочая станция/Сервер 10  (DE: MATE)  Альт Рабочая Станция К 10  (DE: KDE) | 5.10.82-std-def-alt1  5.10.164-std-def-alt1  5.10.198-std-def-alt1  5.10.199-std-def-alt2  5.10.200-std-def-alt1  5.10.204-std-def-alt1  5.10.205-std-def-alt1  5.10.206-std-def-alt1  5.10.207-std-def-alt1  5.10.208-std-def-alt1  5.10.209-std-def-alt2  5.10.211-std-def-alt1  5.10.212-std-def-alt1  5.10.213-std-def-alt1  5.10.216-std-def-alt1  5.10.217-std-def-alt1  5.10.218-std-def-alt1  5.10.219-std-def-alt1 | 5.10.220-std-def-alt2  5.10.221-std-def-alt1  5.10.223-std-def-alt1  5.10.224-std-def-alt1  5.10.226-std-def-alt1  5.15.37-un-def-alt1  5.15.104-un-def-alt1  5.15.105-un-def-alt1  5.15.106-un-def-alt1  5.15.109-un-def-alt1  6.1.61-un-def-alt1  6.1.62-un-def-alt1  6.1.63-un-def-alt1  6.1.65-un-def-alt1  6.1.67-un-def-alt1  6.1.68-un-def-alt1  6.1.69-un-def-alt1  6.1.71-un-def-alt1 | 6.1.72-un-def-alt1  6.1.73-un-def-alt1  6.1.74-un-def-alt1  6.1.75-un-def-alt1  6.1.77-un-def-alt1  6.1.78-un-def-alt1  6.1.79-un-def-alt1  6.1.80-un-def-alt1  6.1.81-un-def-alt1  6.1.82-un-def-alt1  6.1.83-un-def-alt1  6.1.84-un-def-alt1  6.1.85-un-def-alt1  6.1.90-un-def-alt1  6.1.94-un-def-alt1  6.1.96-un-def-alt1  6.1.99-un-def-alt1  6.1.100-un-def-alt1 | | CentOS 7.9  (DE: GNOME)  Red Hat Enterprise Linux 7.9  (DE: GNOME) | 3.10.0-1160.el7.x86\_64  3.10.0-1160.66.1.el7.x86\_64  3.10.0-1160.76.1.el7.x86\_64  3.10.0-1160.83.1.el7.x86\_64  3.10.0-1160.88.1.el7.x86\_64  3.10.0-1160.90.1.el7.x86\_64  3.10.0-1160.99.1.el7.x86\_64  3.10.0-1160.102.1.el7.x86\_64  3.10.0-1160.105.1.el7.x86\_64  3.10.0-1160.108.1.el7.x86\_64  3.10.0-1160.114.2.el7.x86\_64  3.10.0-1160.118.1.el7.x86\_64  3.10.0-1160.119.1.el7.x86\_64 | | | | CentOS 8.5  (DE: GNOME)  Oracle Linux 8.6  (DE: GNOME)  Red Hat Enterprise Linux 8.5/8.6  (DE: GNOME) | 4.18.0-348.7.1.el8\_5.x86\_64  4.18.0-372.9.1.el8.x86\_64  4.18.0-477.15.1.el8\_8.x86\_64  4.18.0-513.9.1.el8\_9.x86\_64  5.4.17-2136.307.3.4.el8uek.x86\_64  5.4.17-2136.328.3.el8uek.x86\_64 | | | | Роса "Хром" Рабочая Станция/Сервер 12  (DE: KDE) | 5.4.150-generic-1rosa2021.1-x86\_64  5.17.11-generic-121rosa2021.1-x86\_64  6.1.89-generic-2rosa2021.1-x86\_64  6.6.27-generic-3rosa2021.1-x86\_64 | | | | SUSE Linux Enterprise Server 12 SP5  (DE: GNOME) | 4.12.14-120-default | | | | SUSE Linux Enterprise Server 15 SP3  (DE: GNOME) | 5.3.18-57-default  5.3.18-150300.59.106-default | | | | Astra Linux Common Edition 2.12  (DE: FLY) | 4.15.3-141-generic/hardened  5.4.0-54-generic/hardened  5.4.0-71-generic/hardened  5.10.0-1038.40-generic/hardened | | | | Astra Linux Special Edition 1.6  (DE: FLY) | 4.15.3-177-generic/hardened#astra28+ci25  5.4.0-110-generic/hardened#astra35+ci109  5.4.0-162-generic/hardened#astra1+ci21  5.10.142-1-generic/hardened#astra6+ci38  5.10.190-1-generic/hardened#astra1+ci17  5.15.0-33-generic/hardened#astra2+ci122  5.15.0-83-generic/hardened#astra1+ci36 | | | | Astra Linux Special Edition 1.7  (DE: FLY) | 5.4.0-54-generic/hardened#astra31+ci49  5.4.0-81-generic/hardened#astra34+ci17  5.4.0-81-generic/hardened#astra34+ci22  5.4.0-110-generic/hardened#astra35+ci47  5.4.0-110-generic/hardened#astra35+ci91  5.4.0-110-generic/hardened#astra35+ci107  5.4.0-110-generic/hardened#astra35+ci130  5.4.0-110-generic/hardened#astra35+ci194  5.4.0-110-generic/hardened#astra35+ci221  5.4.0-162-generic/hardened#astra1+ci6  5.4.0-162-generic/hardened#astra1+ci29  5.4.0-186-generic/hardened  5.4.0-186-generic/hardened#astra2+ci2  5.10.0-1045-generic/hardened#astra34+ci9  5.10.0-1045-generic/hardened#astra5+ci27  5.10.0-1057-generic/hardened#astra6+ci79  5.10.142-1-generic/hardened#astra6+ci24  5.10.142-1-generic/hardened#astra6+ci38  5.10.142-1-generic/hardened#astra6+ci56  5.10.176-1-generic/hardened#astra1+ci5  5.10.176-1-generic/hardened#astra1+ci5  5.10.190-1-generic/hardened#astra1+ci6  5.10.190-1-generic/hardened#astra1+ci32  5.10.216-1-generic/hardened  5.10.216-1-generic/hardened#astra2+ci2  5.15.0-33-generic/hardened#astra2+ci56  5.15.0-33-generic/hardened/lowlatency#astra2+ci96  5.15.0-33-generic/hardened/lowlatency#astra2+ci112  5.15.0-33-generic/hardened/lowlatency#astra2+ci162  5.15.0-70-generic/hardened/lowlatency  5.15.0-70-generic/hardened/lowlatency#astra2+ci6  5.15.0-83-generic/hardened/lowlatency#astra1+ci14  5.15.0-83-generic/hardened/lowlatency#astra1+ci50  5.15.0-111-generic/hardened/lowlatency  5.15.0-111-generic/hardened/lowlatency#astra2+ci1  6.1.50-1-generic#astra2+ci6  6.1.50-1-generic#astra4+ci68  6.1.90-1-generic#astra3+ci5  6.1.90-1-generic#astra3+ci20 | | | | Astra Linux Special Edition 1.8 (DE: FLY) | 6.1.50-1-generic#astra4+ci95  6.1.90-1-generic#astra2+ci10  6.1.90-1-generic/debug#astra2+ci15  6.6.28-1-generic#astra2+ci12  6.6.28-1-generic/debug#astra2+ci23 | | | | Debian 11.3  (DE: GNOME) | 5.10.0-10-amd64  5.10.0-13-amd64  5.10.0-28-amd64 | | | | Ubuntu 18.04  (DE: GNOME) | 5.4.0-42-generic  5.4.0-110-generic  5.4.0-150-generic  5.4.134-19 | | | | Ubuntu 20.04  (DE: GNOME) | 5.4.0-26-generic  5.4.0-156-generic  5.10.65+yc0.406  5.11.0-27-generic  5.13.0-41-generic  5.15.0-94-generic | | | | Ubuntu 22.04  (DE: GNOME) | 5.15.0-30-generic  5.15.0-73-generic  5.15.0-78-generic  5.15.0-87-generic  5.19.0-50-generic  6.2.0-39-generic  6.2.0-1014-azure  6.2.0-1015-azure  6.2.0-1016-azure  6.2.0-1018-azure  6.5.0-17-generic  6.5.0-26-generic | | |  * Наличие привода CD-ROM. * Оперативная память: минимально - 2 Гбайт, рекомендуется – 4 Гбайт. * Свободное пространство на жестком диске: минимально – 1 Гбайт. * Поддерживаемые файловые системы: ext2, ext3, ext4. * В случае совместного применения средств доверенной загрузки – наличие свободного разъема системной шины стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В, либо стандарта PCIe (версии 1.0а и выше), либо стандарта Mini PCI Express, либо стандарта M.2   1. Требования по сертификации:   СЗИ должно соответствовать требованиям руководящих документов:   * «Требования к межсетевым экранам» (ФСТЭК России, 2016) – не ниже 4 класса защиты, * «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), * «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - не ниже 4 уровня доверия.   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 (включительно); * автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно).   1. Требования к функциональности:   СЗИ должно выполнять следующие функции по защите информации:   * Контроль входа пользователей в систему как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации. * Совместное функционирование с программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей. * Поддержка аппаратных средств усиленной аутентификации: * персональные идентификаторы iButton (поддерживаемые типы DS1993 — DS1996 при совместном использовании со средствами доверенной загрузки); * USB-ключи: eRutoken (Rutoken S), Rutoken S RF, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken ЭЦП PKI, Rutoken Lite, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ, ESMART Token, vdToken, GuardantID * Смарт-карты: Rutoken ЭЦП, Rutoken Lite, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, ESMART Token SC. * iButton: DS1993, DS1994, DS1995, DS1996. * Затирание освобождаемых страниц оперативной памяти, при этом должна быть предусмотрена возможность разбиения больших страниц на более мелкие непосредственно перед очисткой; затирание освобождаемых блоков на файловых системах EXT2, EXT3, EXT4 и VFAT; безопасное удаление информации на жестких дисках и внешних носителях; затирание страниц SWAP при выключении компьютера или перезагрузке операционной системы. * Функциональный самоконтроль средства защиты. * Контроль целостности критических объектов операционной системы и ресурсов файловой системы компьютера, поставленных на контроль администратором. Администратор может определять необходимость запуска выполнения контроля целостности при загрузке операционной системы. Администратор должен иметь возможность задать расписание, по которому должно происходить выполнение контроля целостности для защищаемых объектов. Для защищаемых объектов должна быть доступна возможность включения контроля в реальном времени. В случае, если для объекта не установлен контроль в реальном времени, тогда проверка объектов должна осуществляться по расписанию. Администратор должен иметь возможность указать уровень полноты контроля целостности для объекта. * Поддержка следующих режимов реакции СЗИ на нарушение целостности объектов: только регистрация события безопасности; блокировка АС в случае нарушения безопасности; восстановление из эталонного значения (для файловых объектов) и блокировка АС. * Межсетевое экранирование сетевого трафика на основе формируемых правил фильтрации на сетевом, транспортном и прикладном уровне запросов. Должна осуществляться фильтрация с учетом полей сетевых пакетов, направления трафика, сетевого интерфейса, с учетом расписания. * Регистрация событий безопасности в журнале безопасности, контроль действий пользователей. * Аудит действий субъектов с объектами файловой системы и сетевых соединений, аудит отчуждения информации. * Аудит действий администратора при доступе к файловым объектам. * Фильтрация событий безопасности, контекстный поиск в журнале безопасности. * Автоматическое построение отчетов по результатам аудита. * Управление СЗИ: с помощью командной строки. * Управление централизованной установкой клиентов СЗИ. * Централизованное управление лицензиями средствами сервера безопасности. * Поддержка работы через доменные службы Winbind или sssd. | 1 | 160 950,00 |
|  | Установочный комплект средства антивирусной защиты Kaspersky Endpoint Security для бизнеса Стандартный.  Код ОКПД 2 – 58.29.12.000 | 1. Установочный комплект средства антивирусной защиты Kaspersky Endpoint Security для бизнеса – Стандартный 2. Установочный комплект средства антивирусной защиты должен поставляться в виде CD-диска в комплекте с заверенной копией сертификата ФСТЭК России и формуляром. | 1 | 1 453,59 |
|  | Право на использование СКЗИ «Континент-АП» (1 дополнительное подключение пользователя "Континент ZTN Клиент" к СД), ПО-renewal.\*  Код ОКПД 2 – 58.29.50.000 | 1. Продление права на использование "Континент ZTN Клиент" (1 дополнительное подключение пользователя "Континент ZTN Клиент" к СД). 2. Срок действия права: бессрочно. 3. Уровень включенной технической поддержки: базовый. 4. Срок действия включенной технической поддержки: 12 (двенадцать) месяцев. 5. Способ предоставления: посредством отправки на электронную почту представителя Заказчика, в виде электронной скан-копии формата PDF. | 111 | 3 669,00 |
|  | Установочный комплект СКЗИ «Континент-АП».  Код ОКПД 2 – 58.29.12.000 | 1. Установочный комплект Континент ZTN Клиент". 2. Установочный комплект Континент ZTN Клиент" должен поставляться в виде CD-диска в комплекте с заверенной копией сертификата ФСБ России и формуляром. | 1 | 1 333,33 |

\* С целью обеспечения совместимости с программными и техническими средствами, функционирующими в ПАО «Калужская сбытовая компания», поставка эквивалента не допускается.

\*\* Цена за единицу продукции не может превышать указанную начальную максимальную цену.