**Форма запроса технико-коммерческого предложения**

*«15» октября 2018 г.*

**Уважаемые господа!**

В целях расчёта начальной (максимальной) цены товаров, работ, услуг для дальнейшего проведения публичной их закупки прошу Вас предоставить информацию о цене договора на оказание услуг по аттестации информационной системы персональных данных в соответствии с техническим заданием.

Прошу Вас направить коммерческое предложение на фирменном бланке организации за подписью руководителя или лица, имеющего право подписи, до «19» октября 2018 г. с указанием стоимости оказания услуги (в т.ч. с учетом НДС).

Заранее благодарен за сотрудничество.

Контактное лицо: Главный специалист по информационной безопасности Чернецов К.В.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на оказание услуг по аттестации

информационной системы персональных данных

# Общие сведения

Полное наименование системы и её условное обозначение: информационная система ООО ДПИ «Востокпроектверфь» «Зарплата и управление персоналом» (далее – ИСПДн)

Заказчик: Общество с ограниченной ответственностью Дальневосточный проектный институт «Востокпроектверфь» (далее – Общество)

Адрес: 690091, Приморский край, г. Владивосток, ул. Светланская, дом 72

Предполагаемый уровень защищенности ИСПДн: 1УЗ

Объект информатизации:

Таблица 1. Данные объекта информатизации.

|  |  |  |
| --- | --- | --- |
| Местонахождение | Количество  автоматизированных рабочих мест с персональными данными (далее – АРМ) | Количество серверов |
| 690091, Приморский край, г. Владивосток, ул. Светланская, дом 72 | 10 | 2 |

## Цели аттестации ИСПДн

Целью аттестации ИСПДн является оценка эффективности реализованных в рамках системы защиты ИСПДн мер по обеспечению безопасности персональных данных, согласно нормативных актов РФ.

## Общие характеристики информационной системы

В состав ИСПДн Общества входят \_10\_ АРМ и \_2\_ сервера.

На АРМ и серверах, на которых располагаются ИСПДн, установлены операционные системы семейства Microsoft Windows.

ИСПДн, размещенная на серверах Общества, функционирует с использованием виртуализации.

Средства защиты информации, имеющиеся в наличии в Обществе:

* *антивирусное средство Kaspersky Стандартный Certified Media Pack;*
* *система контроля защищенности и соответствия стандартам «MaxPatrol 8»;*
* *программно-аппаратный комплекс «FortiGate» 300D (межсетевой экран и средство обнаружения вторжений).*

Прочие средства защиты информации, необходимые в целях аттестации ИСПДн поставляется Исполнителем (в т.ч. средство от несанкционированного доступа с возможностью централизованного управления с места администратора безопасности, а также средство аппаратной идентификации и аутентификации, позволяющее использовать двухфакторную аутентификацию на АРМ). Требования к указанным средствам представлены в приложении к техническому заданию.

## Требования к системе

## Требования к системе в целом

Меры по защите ИСПДн, ее средств, систем связи и передачи данных должны обеспечивать выполнение требований следующих нормативных актов:

‑ Приказ Федеральной службы по техническому и экспортному контролю 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»;

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

‑ Федеральный закон от 27 июля 2006 г. № 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»;

- иные нормативные правовые акты Российской Федерации в области защиты сведений, не составляющих государственную тайну.

В рамках выполняемой работы исполнитель обязан оказать услуги в составе и объеме, указанном в таблице 1:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | Наименование услуг | Объем оказываемых услуг |
|  | Экспертный аудит текущего состояния организации обработки персональных данных и реализации мер защиты информации | 1 услуга |
|  | Актуализация модели угроз и технического задания | 1 услуга |
|  | Разработка технического проекта системы защиты информации | 1 услуга |
|  | Разработка организационно-распорядительной документации | 1 услуга |
|  | Установка и настройка средств защиты информации | 1 услуга |
|  | Аттестационные испытания информационной системы | 1 услуга |

* 1. Экспертный аудит текущего состояния организации обработки персональных данных и реализации мер защиты информации.

В ходе оказания Исполнитель должен определить:

* ответственных за функционирование информационной системы, перечень приказов о назначении ответственных за функционирование информационной системы и за защиту информации в ней;
* цели создания информационной системы и задачи, решаемые этой информационной системой;
* перечень данных (наименование полей в базах данных, или электронных таблицах, содержание документов), в совокупности позволяющих отнести информацию к определенному уровню значимости;
* места хранения данных информационной системы;
* описание технологического процесса обработки информации в информационной системе;
* перечень защищаемых ресурсов в информационных системах;
* состав программного обеспечения, используемого при обработке информации в информационной системе;
* общесистемные и прикладные программные средства, используемые (планируемые к использованию) в информационной системе;
* технологический процесс обработки данных в информационной системе, включая информацию о наличии дублирующих или альтернативных процессов получения и внесения данных в информационную систему в виде схемы с описанием;
* режимы обработки данных в информационной системе и ее компонентах;
* наличие разграничения прав доступа у пользователей информационной системы;
* уровень доступа сотрудников к данным, обрабатываемым в информационной системе, характер взаимодействия сотрудников между собой;
* физические и логические связи между компонентами информационной системы, другими информационными системами, в том числе с сетями общего пользования;
* функциональные и технологические связи, как внутри информационной системы, так и с другими системами различного уровня и назначения;
* степень ущерба в результате нарушения каждого из свойств безопасности (конфиденциальность, целостность, доступность) в отдельности;
* категории субъектов персональных данных (в случае информационных систем, обрабатывающих персональные данные);
* количество субъектов персональных данных (в случае информационных систем, обрабатывающих персональные данные);
* содержание в информационных системах специальных категорий персональных данных, биометрических или общедоступных (в случае информационных систем, обрабатывающих персональные данные).

Дополнительно необходимо провести анализ наличия организационно-распорядительной и нормативной документации по анализируемой информационной системе, а также наличие средств защиты информации и их настроек. В ходе анализа организационно-распорядительной и нормативной документации на информационную систему необходимо проверить:

* наличие организационной структуры по обеспечению безопасности информации в информационной системе;
* наличие и состав документов, регламентирующих процесс обработки данных в информационной системе (регламенты, соглашения по организации информационного взаимодействия, положения о конфиденциальности и т.п.) в соответствии с требованиями нормативных правовых актов в зависимости от уровня конфиденциальности информации, обрабатываемой в информационной системе;
* наличие и содержание должностных инструкций и оценка уровня подготовки лиц, администрирующих средства защиты информации в информационной системе (методом устного опроса);
* наличие и содержание должностных инструкций персонала (предоставляемых к проверке ответственными исполнителями Заказчика до начала работ по проведению обследования должностным лицом, уполномоченным на сопровождение работ по настоящему Техническому заданию) и оценка уровня подготовки персонала, участвующего в обработке данных;
* правильность классификации (категорирования) информационной системы (в случаях, когда класс (категория) информационной системы уже установлена).

В ходе анализа имеющихся средств защиты информации в анализируемой информационной системе необходимо проверить:

* наличие средств защиты информации в информационной системе, в соответствии с требованиями документов в зависимости от уровня конфиденциальности информации, обрабатываемой в информационных системах;
* наличие сертификатов соответствия на средства защиты информации в информационной системе, а также их соответствие установленному классу защищенности.
  1. Актуализация модели угроз и технического задания

По результатам аудита текущего состояния организации обработки защищаемой информации Исполнитель должен провести анализ существующей документации - модели угроз и технического задания на информационную систему, и провести актуализацию указанной документации.

Документ «Модель угроз безопасности информации при ее обработке в информационной системе» разрабатывается с учетом особенностей функционирования информационной системы, в соответствии с методическими документами уполномоченных органов исполнительной власти, и должен содержать как минимум:

* описание принципов модели угроз;
* описание используемых в информационной системе информационных технологий создания и использования конфиденциальной информации;
* перечень форм представления конфиденциальной информации;
* описание информации, сопутствующей процессам создания и использования конфиденциальной информации;
* описание характеристик безопасности объектов угроз;
* описание факторов угроз, не являющихся атаками;
* описание объектов и субъектов атак;
* описание предположений об имеющейся у нарушителя информации об объектах атак;
* описание предположений об имеющихся у нарушителя средствах атак;
* описание каналов атак;
* описание типов нарушителя;
* список угроз по модели нарушителя;
* частную модель угроз безопасности конфиденциальной информации;
* вычисление показателя исходной защищенности информационной системы;
* вычисление опасности угроз;
* описание источников угроз, связанных с несанкционированным доступом;
* описание уязвимостей информационной системы;
* описание способов реализации угроз;
* описание объектов воздействия;
* описание возможных деструктивных действий;
* описание источников угроз, связанных с техническими каналами утечки;
* описание носителей конфиденциальной информации;
* описание технических каналов утечки;
* список актуальных угроз.

Документ «Техническое задание на создание системы защиты информации в информационной системе» разрабатывается с учетом особенностей функционирования информационной системы, в соответствии с методическими документами уполномоченных органов исполнительной власти, и должен содержать как минимум:

* перечень требуемых мероприятий и мер защиты;
* обоснование разработки системы защиты;
* описание информационной системы (исходные данные);
* адаптация базового набора мер защиты информационной системы;
* уточнение адаптированного базового набора мер защиты информационной системы;
* дополнение уточненного адаптированного набора мер защиты информационной системы;
* требования при использовании криптосредств;
* защита от атак при использовании криптосредств;
* состав, содержание и сроки проведения работ (разработка документации, установка и настройка средств защиты информации).
  1. Разработка технического проекта системы защиты информации

По результатам аудита текущего состояния организации обработки защищаемой информации Исполнитель должен разработать технический проект системы защиты. Проектная документация (эскизный (технический) проект) на информационную систему (систему защиты информации информационной системы) должна соответствовать ГОСТ 34.201 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем".

* 1. Установка и настройка средств защиты информации

В ходе оказания услуги Исполнитель осуществляет:

Установку и настройку средств защиты информации с сертифицированных носителей. В рамках оказания услуги Исполнитель должен выполнить поставку, установку и настройку средств защиты информации, отсутствующие у Заказчика в соответствии с пунктом 3 настоящего технического задания.

* 1. Аттестационные испытания информационной системы

В ходе оказания услуги Исполнитель должен провести оценку эффективности системы защиты информации в виде аттестационных испытаний, а именно:

– разработать документ «Программа и методики аттестационных испытаний» информационной системы Заказчика, который должен содержать:

* цели и задачи аттестационных испытаний;
* организация и условия проведения аттестационных испытаний;
* перечень применяемых методик испытаний;
* применяемые контрольно-измерительные и тестовые средства;
* содержание испытаний системы защиты информационной системы Заказчика.
* провести следующие работы:
* изучение технологического процесса обработки и хранения защищаемой информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации программно-технических средств и систем;
* проверка достаточности представленных документов и соответствия их содержания требованиям по защите информации;
* проверка соответствия предоставленных документов реальным условиям обработки защищаемой информации в информационной системе Заказчика;
* проверка соответствия состава и структуры программно-технических средств информационной системы персональных данных Заказчика представленным документам;
* проверка правильности определения уровня защищенности и (или) классификации информационной системы Заказчика;
* оценка уровня подготовки кадров и распределения ответственности за выполнение требований по обеспечению конфиденциальности защищаемой информации;
* проверка выполнения требований к помещениям, в которых производится обработка защищаемой информации;
* иные проверки, необходимые нормативной документацией, согласованные с Заказчиком в документе Программе и методики аттестационных испытаний;
* описать результаты аттестационных испытаний в соответствующих протоколах;
* разработать документ – Заключение по результатам аттестационных испытаний;
* разработать документ – Аттестат соответствия требованиям по безопасности информации (в случае положительного заключения).

Аттестационные испытания и отчетная документация проводятся и разрабатывается в соответствии:

* Федеральный закон Российской Федерации от 27.06.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* «Методический документ. Меры защиты информации в информационных системах» (утв. ФСТЭК России 11.02.2014);
* Приказ Гостехкомиссии России от 30.08.2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
* Приказ ФАПСИ России от 13.06.2001 года № 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 ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
* Приказ ФСБ России 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»;
* Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
* ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;
* ГОСТ 34.602 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
* ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
* ГОСТ 34.201 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
* ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем»;
* ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;
* ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».
  1. **Обязательные требования к Исполнителю**

Исполнитель должен иметь в наличии и представить Обществу, выданную уполномоченным органом власти копию документа, свидетельствующего о наличии у Исполнителя прав на осуществление видов деятельности, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации   
(утв. Постановлением Правительства РФ от 3 февраля 2012 года № 79).

Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации:

* контроль защищенности конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации;
* аттестационные испытания и аттестация на соответствие требованиям по защите информации: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
* проектирование в защищённом исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
* установка, монтаж, испытания, ремонт средств защиты информации: технических средств защиты информации; защищённых 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 защищённости информации.

Исполнитель должен иметь в наличии и представить Обществу, выданный уполномоченным органом власти заверенную руководителем лицензиата копию лицензии ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (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) (утв. Постановлением Правительства РФ от 16.04.2012 г. № 313).

Лицензия ФСБ России на выполнение следующих работ и оказание услуг:

* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Приложение к техническому заданию оказание услуг по аттестации информационной системы персональных данных

**1. Передача неисключительных прав на использование средств защиты информации от несанкционированного доступа (далее – СЗИ НСД) – 12 лицензий**

1. СЗИ НСД должен представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов.
2. СЗИ НСД должен быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, , Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, в многопользовательском режиме их эксплуатации.
3. СЗИ НСД должен поддерживать 32- и 64-битные версии операционных систем.
4. СЗИ НСД должен быть предназначен для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа).
5. СЗИ НСД должен быть сертифицирован на соответствие требованиям Руководящих документов (РД СВТ, Гостехкомиссия России, 1992 г.) к 5-му классу защищенности от НСД для СВТ и 4-му уровню контроля отсутствия НДВ (РД НДВ, Гостехкомиссия России, 1999 г.).
6. СЗИ НСД должен включать 3 (три) года технической поддержки, оказываемой производителем.
7. СЗИ НСД должен обеспечивать:
   1. регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере;
   2. идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows;
   3. реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;
   4. возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в операционную систему;
   5. возможность настройки принудительной двухфакторной аутентификации для учётной записи с правами администратора и/или пользователя;
   6. возможность средствами СЗИ НСД выполнить настройку периода действия учётной записи;
   7. возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;
   8. возможность при создании учётной записи выбрать тип учётной записи (внутренний, внешний, системный, приложение, гостевой, временный);
   9. независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;
   10. контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:
   * Android-устройств;
   * iOS-устройств;
   * Bluetooth-устройств;
   * DVD- и CD-ROM-дисководов;
   * устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
   * USB-контроллеров;
   * беспроводных устройств (Wireless Communication Devices);
   * биометрических устройств;
   * дисководов магнитных дисков;
   * звуковых, видео- и игровых устройств;
   * инфракрасных устройств (IrDA);
   * контроллеров магнитных дисков;
   * ленточных накопителей;
   * модемов;
   * переносных устройств;
   * портов (COM и LPT);
   * сенсоров;
   * сетевых адаптеров;
   * сканеров и цифровых фотоаппаратов;
   * принтеров;
   * съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).
   1. предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должнен позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;
   2. преобразование информации:

* на съемных носителях информации для создания доверенной среды при работе со съемными носителями;
* при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);
* при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.
  1. блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;
  2. возможность работы с преобразованными файлами-контейнерами на компьютерах, где программное обеспечение СЗИ НСД не установлено;
  3. сохранение теневых копий файлов, записываемых на съемные носители;
  4. использование дискреционного принципа контроля доступа:
  + обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).
  1. возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);
  2. регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей;
  3. расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;
  4. возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;
  5. возможность разграничения доступа к буферу обмена;
  6. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);
  7. возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;
  8. очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Запрет смены пользователей без перезагрузки;
  9. выполнение регистрации действий по зачистке остаточной информации;
  10. возможность самодиагностики основного функционала СЗИ НСД с возможностью сохранения отчета;
  11. возможность сохранения конфигурации для последующего восстановления СЗИ НСД;
  12. ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;
  13. возможность настройки репликации серверов безопасности;
  14. централизованное управление лицензиями на терминальные подключения и на клиентов в нескольких доменах безопасности при использовании отдельного модуля «Сервер лицензий»;
  15. централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора;
  16. возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании-разработчика СЗИ НСД;
  17. возможность использования SQL базы данных для централизованного хранения событий аудита;
  18. возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:
  + нарушение контроля целостности объекта;
  + попытка работы после блокировки при нарушении целостности;
  + попытка входа на клиентскую рабочую станцию с неправильным паролем;
  + блокировка пользователя после многократного ввода неправильного пароля;
  + СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);
  + клиент недоступен долгое время (с возможностью задания периода времени);
  + попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.
  1. блокировку доступа к файлам по расширению;
  2. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;
  3. возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;
  4. возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления;
  5. возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory. Проверка подписи файлов при обновлении СЗИ НСД;
  6. возможность визуализации сети защищаемых компьютеров;
  7. возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования);
  8. возможность выполнять синхронизацию времени между сервером безопасности и клиентами.

**2. Передача неисключительных прав на использование сервера безопасности для** **средства защиты информации от несанкционированного доступа** - **1 лицензия**

1. Сервер безопасности (далее СБ) должен представлять собой отдельный программный модуль с аппаратным лицензионным ключом, в операционных системах семейства Windows, предназначенный для удаленного и централизованного управления средствами защиты информации от несанкционированного доступа.
2. Лицензия на СБ должны предусматривать подключение не менее 10 клиентов.
3. СБ должен быть предназначен для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, в многопользовательском режиме их эксплуатации.
4. СБ должен поддерживать 32- и 64-битные версии операционных систем.
5. СБ должен быть предназначен для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах, также поддерживать виртуальные среды.
6. СБ должен быть сертифицирован на соответствие 4-му уровню контроля отсутствия НДВ (РД НДВ, Гостехкомиссия России, 1999 г.).
7. СБ может быть использован при создании защищенных автоматизированных систем до класса защищенности 1Г включительно, для обеспечения 1 уровня защищенности персональных данных, в государственных информационных системах 1 класса защищённости и в автоматизированных системах управления до 1 класса защищённости включительно.
8. СБ должен включать 3 (три) года технической поддержки, оказываемой производителем.
9. СБ должен обеспечивать:
   1. централизованное управление защищенными рабочими станциями с возможностью объединения рабочих станций в группы. Должна поддерживаться многоуровневая иерархия групп и наследование установленных параметров;
   2. возможность удаленной блокировки, выключения или перезагрузки защищённой рабочей станции, завершения сеанса работы пользователя по команде администратора;
   3. централизованное управление учетными записями пользователей и группами учетных записей пользователей на защищенных рабочих станциях;
   4. централизованное управление политиками безопасности СЗИ, удаленное управление доступом к ресурсам файловой системы на защищенных рабочих станциях;
   5. периодический сбор журналов аудита с защищенных рабочих станций;
   6. графическое отображение состояния защищаемых рабочих станции;
   7. централизованную блокировку доступа к файлам по расширению на защищенных рабочих станциях;
   8. централизованный контроль аппаратной конфигурации защищенных рабочих станции и подключаемых устройств;
   9. централизованное управление преобразованными съемными носителями информации;
   10. возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:
   * нарушение контроля целостности объекта;
   * попытка работы после блокировки при нарушении целостности;
   * попытка входа на клиентскую рабочую станцию с неправильным паролем;
   * блокировка пользователя после многократного ввода неправильного пароля;
   * СЗИ НСД на клиенте не отвечает (возможная причина − несанкционированная деактивация системы защиты);
   * клиент недоступен долгое время (с возможностью задания периода времени);
   * попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.
   1. возможность автоматического оповещения о событии НСД на клиенте по электронной почте;
   2. возможность визуализации сети защищаемых компьютеров;
   3. возможность настройки репликации серверов безопасности;
   4. возможность использования SQL базы данных для централизованного хранения событий аудита;
   5. возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления (СБ);
   6. возможность удаленной установки, обновления и удаления СЗИ на рабочих станциях в составе домена безопасности;
   7. возможность выполнять синхронизацию времени между сервером безопасности и клиентами;
   8. возможность сохранения конфигурации СБ для последующего восстановления настроек;
   9. возможность централизованного управления СЗИ следующих типов: СЗИ НСД для ОС семейства Windows.
   10. возможность нотификации о наличии обновлений для СБ на сервере компании-разработчика;
10. Реализация СБ должна быть программной, с возможностью подключения аппаратного лицензионного ключа и аппаратных средств считывания индивидуальных идентификаторов пользователей.

**3. Поставка электронных идентификаторов - 12 штук**

|  |  |
| --- | --- |
| **Основные характеристики** | |
| Аппаратная часть | Наличие защищенного микроконтроллера со встроенной энергонезависимой памятью |
| Поддержка интерфейса USB 1.1 и выше | Да |
| Поддерживаемые операционные системы | Microsoft Windows 10/2016/8.1/8/2012/7/2008/ |
| Использование в российских системах PKI, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной подписи | Да |
| **Поддерживаемые интерфейсы и стандарты** | |
| PKCS#11 версии 2.20, включая российский профиль | Да |
| PC/SC | Да |
| Microsoft Crypto API | Да |
| Microsoft Smartcard API | Да |
| USB CCID (работа без установки драйверов устройства в современных версиях операционных систем) | Да |
| ISO/IEC 7816 | ISO/IEC 7816-4, 7816-8, 7816-12 |
| Криптопровайдер | Собственный Crypto Service Provider |
| Сертификаты X.509 версии 3 на уровне программного обеспечения | Да |
| **Криптографические возможности** | |
| **Поддержка алгоритма ГОСТ 28147-89** | Аппаратная реализация |
| Режимы шифрования | Простая замена, гаммирование, гаммирование с обратной связью |
| Режим выработки имитовставки | Да |
| Генерация ключей шифрования | Да |
| Импорт ключей шифрования | Нет |
| Запрет экспорта ключей шифрования | Да |
| **Поддержка алгоритма ГОСТ Р 34.10-2012** | Аппаратная реализация |
| Формирование и проверка электронной подписи | Да |
| Генерация ключевых пар | Да, с проверкой качества |
| Импорт ключевых пар | Нет |
| Запрет экспорта ключевых пар | Да |
| Срок действия закрытых ключей | До 3-х лет |
| Размер закрытого ключа | 256 и 512 бит |
| **Поддержка алгоритма ГОСТ Р 34.10-2001** | Аппаратная реализация |
| Формирование и проверка электронной подписи | Да |
| Генерация ключевых пар | Да, с проверкой качества |
| Импорт ключевых пар | Нет |
| Запрет экспорта ключевых пар | Да |
| Срок действия закрытых ключей | До 3-х лет |
| Размер закрытого ключа | 256 бит |
| **Поддержка алгоритма ГОСТ 34.11-2012** | Аппаратная реализация |
| Вычисление значения хэш-функции | Да, в т.ч. с возможностью последующего формирования ЭП |
| **Поддержка алгоритма ГОСТ 34.11-94** | Аппаратная реализация |
| Вычисление значения хэш-функции | Да, в т.ч. с возможностью последующего формирования ЭП |
| **Выработка сессионных ключей (ключей парной связи)** | Да (по схеме VKO GOST R 34.10-2001 согласно RFC 4357, по схеме VKO GOST R 34.10-2012 согласно RFC 7836) |
| **Расшифрование по схеме EC El-Gamal** | Да |
| **Поддержка алгоритма RSA** | Аппаратная реализация расшифрования и подписи |
| Формирование электронной подписи | Да |
| Генерация ключевых пар | Да, с проверкой качества |
| Импорт ключевых пар | Да |
| Запрет экспорта ключевых пар | Да |
| Размер ключей | До 2048 бит |
| **Поддержка алгоритмов DES (3DES), AES, RC2, RC4, MD4, MD5, SHA-1, SHA-256** | Хранение экспортируемых ключей в EF, программная реализация SHA-1, MD5 в PKCS#11, RC4, MD4, MD5, SHA-1, SHA-256, 3DES, AES в minidriver |
| **Сведения о сертификации** | |
| Наличие сертификата ФСБ России | [Да](http://www.rutoken.ru/products/all/rutoken-ecp-flash/#certify) |
| **Файловая система** | |
| Запрет экспорта закрытых и симметричных ключей | Да |
| Шифрование файловой системы | Да, прозрачное, алгоритм ГОСТ 28147-89, уникальный ключ шифрования для каждого экземпляра устройства |
| **Аутентификация и конфиденциальность** | |
| Двухфакторная аутентификация | Да, предъявление токена + ввод PIN-кода |
| Уровни доступа | Гость, Пользователь, Администратор |
| Разграничение доступа к файловым объектам в соответствии с уровнем доступа | Да |
| Ограничение числа попыток ввода PIN-кода | Да, настраиваемое |
| Поддержка PIN-кодов | Глобальные PIN-коды: Администратора и Пользователя; локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов) |
| Ограничение минимального размера PIN-кода | Да, настраивается независимо для любого PIN-кода |
| Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам. | Да |
| Создание локальных PIN-кодов для дополнительной защиты части ключевой информации | Да |
| Возможность одновременной работы с несколькими локальными PIN-кодами | Да, до 7 шт. |
| **Пластиковый брелок с полем для метки** | **Да** |
| **Встроенный контроль и индикация** | |
| Контроль целостности прошивки | Да |
| Контроль целостности системных областей памяти | Да |
| Типы счетчиков | * Счетчик изменений файловой системы; * счетчик изменений PIN-кодов; * счетчики последовательных неудачных попыток ввода PIN-кодов; * счетчик успешных операций электронной подписи. |
| Проверка правильности функционирования криптографических алгоритмов | Да |
| Светодиодный индикатор | Да, с режимами работы: готовность к работе, выполнение операции, нарушения в системной области памяти. |