**ВЫПОЛНЕНИЕ РАБОТ ПО СОЗДАНИЮ КОМПОНЕНТА ЗАЩИТЫ ИНФОРМАЦИИ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА ВИДЕОДЕТЕКТИРОВАНИЯ И ФОРМИРОВАНИЯ ИНДЕКСНЫХ ДАННЫХ АО «ЭЛЕКТРОННАЯ МОСКВА»**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

Листов 74

**ОГЛАВЛЕНИЕ**

[1. ОБЩИЕ СВЕДЕНИЯ 4](#_Toc53353721)

[1.1. Заказчик и Подрядчик 4](#_Toc53353722)

[1.2. Цели и задачи выполнения работ 4](#_Toc53353723)

[1.3. Состав работ и срок выполнения работ 5](#_Toc53353724)

[1.4. Основание для выполнения работ 5](#_Toc53353725)

[1.5. Нормативно-технические документы, методические материалы, регламентирующие выполнение работ 5](#_Toc53353726)

[1.6. Перечень сокращений 6](#_Toc53353727)

[2. ТРЕБОВАНИЯ К СТРУКТУРЕ 6](#_Toc53353728)

[3. ХАРАКТЕРИСТИКИ АПК «ВИФИД» 7](#_Toc53353729)

[3.1. Место установки 7](#_Toc53353730)

[3.2. Класс защищенности 7](#_Toc53353731)

[3.3. Субъекты доступа 7](#_Toc53353732)

[3.4. Описание структурно-функциональных характеристик АПК «ВИФИД» 7](#_Toc53353733)

[3.4.1. Функциональная архитектура и принципы построения АПК «ВИФИД» 7](#_Toc53353734)

[3.4.2. Описание комплекса технических средств 7](#_Toc53353735)

[3.4.3. Описание программного обеспечения 8](#_Toc53353736)

[3.4.4. Описание сетевой инфраструктуры 8](#_Toc53353737)

[3.4.5. Описание информационного взаимодействия 9](#_Toc53353738)

[4. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ 9](#_Toc53353739)

[4.1. Требования к уровню вычислительной инфраструктуры 9](#_Toc53353740)

[4.2. Требования к уровню сетевой инфраструктуры 10](#_Toc53353741)

[4.3. Требования к уровню защиты информации 10](#_Toc53353742)

[4.3.1. Требования к модулю антивирусной защиты 10](#_Toc53353743)

[4.3.2. Требования к модулю защиты от несанкционированного доступа 10](#_Toc53353744)

[4.3.3. Требования к модулю межсетевого экранирования и обнаружения вторжений 10](#_Toc53353745)

[4.3.4. Требования к модулю криптографической защиты 11](#_Toc53353746)

[4.3.5. Требования к модулю контроля (анализа) защищенности 11](#_Toc53353747)

[4.3.6. Требования к модулю мониторинга событий информационной безопасности 11](#_Toc53353748)

[4.3.7. Требования к модулю контроля привилегированных пользователей 11](#_Toc53353749)

[4.3.8. Требования к модулю доверенной загрузки 11](#_Toc53353750)

[4.3.9. Требования к модулю резервного копирования 11](#_Toc53353751)

[4.3.10. Требования к модулю защиты среды виртуализации 11](#_Toc53353752)

[4.4. Требования к режимам функционирования КЗИ 12](#_Toc53353753)

[5. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ 12](#_Toc53353754)

[5.1. Требования к оборудованию и программному обеспечению уровня вычислительной инфраструктуры 12](#_Toc53353755)

[5.2. Требования к оборудованию и программному обеспечению уровня сетевой инфраструктуры 12](#_Toc53353756)

[5.3. Требования к оборудованию и программному обеспечению уровня защиты информации 12](#_Toc53353757)

[5.4. Общие требования к оборудованию и программному обеспечению 12](#_Toc53353758)

[5.4.1. Требования к качеству 12](#_Toc53353759)

[5.4.2. Требования к надежности 12](#_Toc53353760)

[5.4.3. Требования к гарантийным обязательствам 13](#_Toc53353761)

[5.4.4. Требования к защите от влияния внешних воздействий 14](#_Toc53353762)

[5.4.5. Требования к эргономичности и эстетике исполнения 14](#_Toc53353763)

[5.4.6. Требования по экологии и безопасности исполнения 14](#_Toc53353764)

[5.4.7. Требования к эксплуатации и техническому обслуживанию 14](#_Toc53353765)

[6. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ 14](#_Toc53353766)

[6.1. Требования к работам по Обследованию АПК «ВИФИД» и разработке (проектированию) КЗИ 14](#_Toc53353767)

[6.1.1. Требования к работам по обследованию 14](#_Toc53353768)

[6.1.2. Требования к оформлению Отчета по результатам обследования объекта 15](#_Toc53353769)

[6.1.3. Требования к разработке Технического проекта на создание КЗИ 15](#_Toc53353770)

[6.2. Требования к выполнению работ по Поставке оборудования и программного обеспечения КЗИ 17](#_Toc53353771)

[6.3. Требования к выполнению работ по Внедрению КЗИ 18](#_Toc53353772)

[6.3.1. Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня вычислительной инфраструктуры 19](#_Toc53353773)

[6.3.2. Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня сетевой инфраструктуры 19](#_Toc53353774)

[6.3.3. Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня защиты информации 19](#_Toc53353775)

[6.3.4. Требования к мероприятиям по затруднению несанкционированного физического доступа к средствам вычислительной техники 21](#_Toc53353776)

[6.3.5. Требования к разработке и оформлению Технического паспорта АПК «ВИФИД» 21](#_Toc53353777)

[6.3.6. Требования к разработке проектов организационно-распорядительных документов 21](#_Toc53353778)

[6.3.7. Требования к инструктажу персонала Заказчика 21](#_Toc53353779)

[6.3.8. Требования к предварительным испытаниям КЗИ 21](#_Toc53353780)

[6.3.9. Требования к опытной эксплуатации КЗИ 22](#_Toc53353781)

[6.3.10. Требования к анализу уязвимостей АПК «ВИФИД» 22](#_Toc53353782)

[6.3.11. Требования к приемочным испытаниям КЗИ 22](#_Toc53353783)

[6.4. Требования к выполнению работ по Аттестации АПК «ВИФИД» по требованиям защиты информации 22](#_Toc53353784)

[6.4.1. Требования к разработке Программы и методики аттестационных испытаний АПК «ВИФИД» 22](#_Toc53353785)

[6.4.2. Требования к комплексным аттестационным испытаниям АПК «ВИФИД» 23](#_Toc53353786)

[6.5. Общие требования к документированию 23](#_Toc53353787)

[6.6. Общие требования к безопасности работ 23](#_Toc53353788)

[6.7. Требования к Подрядчику 24](#_Toc53353789)

[7. ТРЕБОВАНИЯ ПО СДАЧЕ РАБОТ 25](#_Toc53353790)

[7.1. Состав и содержание работ 25](#_Toc53353791)

[7.2. Общие требования к приемке работ 29](#_Toc53353792)

[Приложение А Требования к оборудованию и программному обеспечению КЗИ 30](#_Toc53353793)

[Приложение Б Структурная схема АПК «ВИФИД» 64](#_Toc53353794)

[Приложение В Форма Сублицензионного договора 65](#_Toc53353795)

1. **ОБЩИЕ СВЕДЕНИЯ**

Аппаратно-программный комплекс видеодетектирования и формирования индексных данных (далее — АПК «ВИФИД») охватывает городской сегмент единой системы обработки видеоданных города Москва.

В рамках реализации работ в соответствии с настоящим техническим заданием Подрядчик должен создать компонент защиты информации АПК «ВИФИД».

Результатом выполнения работ по настоящему техническому заданию является КЗИ, смонтированный и настроенный по адресам, указанным в Таблице 1, в соответствии с проектными решениями, состоящий из составных частей, приведенных в разделе 2 настоящего документа, обеспечивающий в полном объеме реализацию требований, установленных законодательством в области защиты информации, а также аттестация АПК «ВИФИД» по требованиям законодательства в области защиты информации (в соответствии с требованиями приказа ФСТЭК от 11 февраля 2013 г. № 17 (п. 13)).

* 1. **Заказчик и Подрядчик**

1.1.1. Сведения о Заказчике:

Наименование: АО »Электронная Москва».

ИНН/КПП: 7707314029/770201001.

Юридический адрес: 127051, г. Москва, пер. Сухаревский Б., д. 11, стр. 1.

1.1.2. Сведения о Подрядчике:

Подрядчик определяется по результатам проведения процедуры определения поставщика в соответствии с требованиями Федерального закона от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ и услуг отдельными видами юридических лиц».

* 1. **Место выполнения работ**

|  |  |  |
| --- | --- | --- |
| Таблица № 1. | | |
| № | Адрес | Характеристика |
|  | г. Москва, Коровинское ш., д. 41 | Центр обработки данных |
|  | г. Москва, Яковоапостольский пер., д. 12, стр. 1 | Помещения АО »Электронная Москва» |

* 1. **Цели и задачи выполнения работ**

Работы выполняются с целью обеспечения защиты информации, содержащейся в АПК «ВИФИД», и заключаются в создании компонента защиты информации АПК «ВИФИД» в соответствии с требованиями законодательства Российской Федерации и нормативными документами в области информационной безопасности и проведения аттестационных испытаний АПК «ВИФИД» на соответствие Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Целями выполнения работ является обеспечение с помощью информационно-коммуникационных технологий, реализуемых КЗИ:

* выполнения требований нормативных правовых актов и методических документов по обеспечению безопасности информации;
* технического обеспечения функционирования КЗИ;
* непрерывности процесса защиты информации;
* затруднение несанкционированного физического доступа к защищаемым средствам вычислительной техники;
* предотвращение или снижение величины ущерба, наносимого   
  АО »Электронная Москва», вследствие реализации угроз безопасности информации.

Задачи, которые должны быть решены в ходе выполнения работ:

* разработка и документирование проектных решений по КЗИ;
* реализация в рамках КЗИ технических мер защиты информации, содержащейся в АПК «ВИФИД»;
* оценка эффективности реализованных в рамках КЗИ мер защиты информации, содержащейся АПК «ВИФИД».
  1. **Состав работ и срок выполнения работ**
     1. Обследование АПК «ВИФИД» и разработка (проектирование) КЗИ: не позднее 10 (десяти) календарных дней с даты заключения Договора;
     2. Поставка оборудования и программного обеспечения КЗИ: не позднее 60 (шестидесяти) календарных дней с даты заключения Договора;
     3. Внедрение КЗИ: не позднее 80 (восьмидесяти) календарных дней с даты заключения Договора;
     4. Аттестация АПК «ВИФИД» по требованиям законодательства в области защиты информации: не позднее 90 (девяноста) календарных дней с даты заключения Договора.
  2. **Основание для выполнения работ**

Основаниями для выполнения работ являются:

– Соглашение о предоставлении субсидии из бюджета города Москвы акционерному обществу «Электронная Москва», заключенное с Департаментом информационных технологий города Москвы;

– Договор на выполнение работ по созданию компонента защиты информации АПК «ВИФИД».

* 1. **Нормативно-технические документы, методические материалы, регламентирующие выполнение работ**
* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
* приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* приказ ФСБ России от 10 июля 2014 г. № 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»;
* методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г.;
* Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России от 14 февраля 2008 г.);
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.);
* Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru);
* ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
* ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
* ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем»;
* ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
* ГОСТ Р 50739-95 »Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
* ГОСТ Р 50922-2006 »Защита информации. Основные термины и определения».
* ГОСТ Р 51583-2014 »Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
* ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
* ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».
  1. **Перечень сокращений**

|  |  |
| --- | --- |
| Таблица № 2. | |
| **Сокращение** | **Расшифровка** |
| АРМ | Автоматизированное рабочее место |
| АПК «ВИФИД» | Аппаратно-программный комплекс видеодетектирования и формирования индексных данных АО «Электронная Москва» |
| НСД | Несанкционированный доступ |
| ОБХД | Объединенная база хранения индексных данных |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| КЗИ | Компонент защиты информации аппаратно-программного комплекса видеодетектирования и формирования индексных данных АО «Электронная Москва» |
| ЛВС | Локальная вычислительная сеть |
| СЗИ | Средство защиты информации |
| СКЗИ | Средство криптографической защиты информации |
| СУБД | Система управления базами данных |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю |
| ФСБ России | Федеральная служба безопасности Российской Федерации |
| ЦОД | Центр обработки данных |

1. **ТРЕБОВАНИЯ К СТРУКТУРЕ**

В рамках выполнения работ, предусмотренных настоящим техническим заданием, должен быть создан КЗИ, состоящий из следующих функциональных уровней:

* уровень вычислительной инфраструктуры;
* уровень сетевой инфраструктуры;
* уровень защиты информации.

Все уровни КЗИ должны размещаться в пределах контролируемой зоны.

Для взаимодействия между территориально удаленными площадками АПК «ВИФИД» и для внешних подключений (при необходимости), осуществляемых посредством каналов связи, выходящих за пределы контролируемой зоны, в КЗИ должно быть предусмотрено использование СКЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации ФСБ России.

КЗИ должна строиться по модульному принципу и предусматривать возможность масштабирования и (или) расширения возможностей ее составных частей в зависимости от условий функционирования АПК «ВИФИД».

1. **ХАРАКТЕРИСТИКИ АПК «ВИФИД»**

АПК «ВИФИД» создается в рамках реализации Государственной программы города Москвы «Умный город», утвержденной постановлением Правительства Москвы   
от 9 августа 2011 г. № 349-ПП «Об утверждении государственной программы города Москвы «Умный город».

АПК «ВИФИД» представляет собой Городской сегмент Единой системы обработки видеоданных в городе Москве.

* 1. **Место установки**

Серверные элементы АПК «ВИФИД» размещаются в центре обработки данных (далее — ЦОД) по адресу: г. Москва, Коровинское ш., д. 41.

Пользовательские элементы (АРМ администраторов АПК «ВИФИД», АРМ администраторов безопасности АПК «ВИФИД») размещаются в помещениях АО »Электронная Москва» по адресу: г. Москва, Яковоапостольский пер., д. 12 стр. 1.

* 1. **Класс защищенности**

В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, Актом классификации АПК «ВИФИД» установлен 3-й класс защищенности.

* 1. **Субъекты доступа**

Субъектами доступа АПК «ВИФИД» являются:

* администраторы АПК «ВИФИД», осуществляющие настройку системного, прикладного и специального программного обеспечения;
* администраторы безопасности АПК «ВИФИД», обеспечивающие настройку средств защиты информации АПК «ВИФИД» и выполнение мероприятий по обеспечению защиты информации в АПК «ВИФИД»;
* работники сторонних организаций, привлекаемых для сопровождения программного обеспечения АПК «ВИФИД» на договорной основе;
* внешние информационные системы.
  1. **Описание структурно-функциональных характеристик АПК «ВИФИД»**
     1. **Функциональная архитектура и принципы построения АПК «ВИФИД»**

АПК «ВИФИД» состоит из модулей, обеспечивающих решение определенного круга функциональных задач.

Основные функциональные модули АПК «ВИФИД»:

* модуль детектирования лиц;
* модуль индексации данных;
* модуль ОБХД.
  + 1. **Описание комплекса технических средств**

Комплекс технических средств АПК «ВИФИД» состоит из следующих элементов:

* вычислительные серверы — обеспечивают функционирование системы:

1. модуль детектирования лиц — 103 сервера;
2. модуль индексации данных — 87 серверов;
3. модуль ОБХД — 71 сервер.

* автоматизированные рабочие места (4 АРМ) — обеспечивают работу администраторов АПК «ВИФИД» и администраторов безопасности АПК «ВИФИД»;
* система хранения данных — обеспечивает хранение информационных ресурсов системы;
* локальная вычислительная сеть — обеспечивает высокоскоростную передачу информации между техническими средствами АПК «ВИФИД», размещенными на одном объекте.

Структурная схема АПК «ВИФИД» приведена в Приложении Б к настоящему документу.

* + 1. **Описание программного обеспечения**

Комплекс программного обеспечения АПК «ВИФИД» можно разделить на следующие основные группы:

* системное ПО;
* прикладное ПО;
* специальное ПО.

Системное ПО:

* операционная система Microsoft Windows 10;
* операционная система Microsoft Windows Server 2016;
* операционная система Ubuntu 18.04 LTS;
* операционная система CentOS 7.7;
* среда виртуализации VMware;
* иные операционные системы, используемые поставщиками решений для модулей индексации.

Прикладное ПО:

* офисный пакет приложений Microsoft Office.

Специальное ПО:

* брокер сообщений Apache Kafka;
* брокер сообщений RabbitMQ;
* СУБД Microsoft SQL Server;
* СУБД MongoDB;
* СУБД Postgres;
* СУБД Tarantool;
* СУБД Scylla;
* СУБД Redis;
* СУБД InfluxDB;
* мультиплексор запросов PgBouncer;
* балансировщик нагрузки HAProxy;
* прокси-сервер Nginx;
* поисковая система Elasticsearch;
* система мониторинга Prometheus;
* хранилище параметров конфигурации Etcd;
* система контейнеризации Docker;
* система оркестрации контейнеров Kubernets;
* система удаленного вызова процедур gRPC;
* система аналитики и визуализации Grafana;
* система сбора и анализа логов Fluentd;
* специальное ПО, разработанное для реализации функций модулей АПК «ВИФИД».
  + 1. **Описание сетевой инфраструктуры**

Технические средства АПК «ВИФИД», размещаемые в ЦОД и в помещениях АО »Электронная Москва», объединяются в рамках объекта размещения средствами локальной вычислительной сети с использованием технологии Ethernet и стека протоколов TCP/IP.

Территориально удаленные площадки АПК «ВИФИД» объединяются с использованием сети связи общего пользования и международного информационного обмена (Интернет).

АПК «ВИФИД» имеет подключение:

* к выделенным сетям связи (два оптических канала связи, обеспечивающих передачу трафика со скоростью до 160 Гбит/c каждый), для организации информационного взаимодействия с внешними информационными системами;
* к сетям связи общего пользования и международного информационного обмена (Интернет) для организации доступа администраторов АПК «ВИФИД» и администраторов безопасности АПК «ВИФИД», а также для взаимодействия с внешними информационными системами.
  + 1. **Описание информационного взаимодействия**

АПК «ВИФИД» осуществляет информационное взаимодействие со следующими внешними информационными системами:

* государственная информационная система «Единый центр хранения и обработки данных» (ГИС ЕЦХД);
* информационная система «Компонент обработки индексных данных ФейсТрафик»;
* информационные системы организаций, привлекаемых для сопровождения программного обеспечения АПК «ВИФИД» на договорной основе.

ГИС ЕЦХД является поставщиком видеоинформации для АПК «ВИФИД». Передача видеоинформации осуществляется по выделенным сетям связи с использованием протокола RTSP. Также обеспечивается интеграция АПК «ВИФИД» с подсистемой автоматической регистрации сценариев индексирования видеоинформации ГИС ЕЦХД.

Для организации взаимодействия АПК «ВИФИД» с информационной системой «Компонент обработки индексных данных ФейсТрафик» и информационными системами организаций, привлекаемых для сопровождения программного обеспечения АПК «ВИФИД» на договорной основе, используются сети связи общего пользования и международного информационного обмена (Интернет).

1. **ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ**

КЗИ предназначена для обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее — информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в АПК «ВИФИД».

КЗИ должна обеспечивать выполнение Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, предъявляемых к информационным системам третьего класса защищенности.

КЗИ не должна препятствовать нормальному функционированию АПК «ВИФИД» и смежных систем.

* 1. **Требования к уровню вычислительной инфраструктуры**

Уровень вычислительной инфраструктуры предназначен для развертывания средств управления и серверных компонент следующих модулей:

* модуль защиты от несанкционированного доступа;
* модуль антивирусной защиты;
* модуль контроля (анализа) защищенности;
* модуль криптографической защиты;
* модуль мониторинга событий информационной безопасности;
* модуль контроля привилегированных пользователей;
* модуль резервного копирования;
* модуль защиты среды виртуализации.

Исполнитель должен произвести поставку компонентов системы хранения данных и серверов типа и комплектации, указанных в Приложении А к настоящему документу.

На серверах уровня вычислительной инфраструктуры должна быть развернута среда виртуализации в объеме, необходимом для обеспечения функционирования модулей КЗИ.

* 1. **Требования к уровню сетевой инфраструктуры**

Уровень сетевой инфраструктуры должен обеспечивать решение следующих задач:

* балансировку сетевого трафика для модуля межсетевого экранирования и обнаружения вторжений;
* агрегацию соединений с элементами уровня вычислительной инфраструктуры АПК «ВИФИД» с обеспечением необходимой пропускной способности коммутации IP пакетов;
* агрегацию соединений интерфейсов управления.

Исполнитель должен произвести поставку коммутаторов типа и комплектации, указанных в Приложении А к настоящему документу, а также необходимых интерфейсных модулей и коммутационных шнуров.

* 1. **Требования к уровню защиты информации**

Уровень защиты информации должен включать:

* модуль антивирусной защиты;
* модуль защиты от несанкционированного доступа;
* модуль межсетевого экранирования и обнаружения вторжений;
* модуль криптографической защиты;
* модуль контроля (анализа) защищенности;
* модуль мониторинга событий информационной безопасности;
* модуль контроля привилегированных пользователей;
* модуль доверенной загрузки;
* модуль резервного копирования;
* модуль защиты среды виртуализации.
  + 1. **Требования к модулю антивирусной защиты**

Модуль антивирусной защиты должен обеспечивать решение следующих задач:

* резидентный антивирусный мониторинг;
* автоматическая проверка наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа;
* сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию;
* настройка шаблонов действий, которые должны выполняться при обнаружении зараженных объектов;
* централизованное управление, мониторинг и обновление программных средств антивирусной защиты, входящих в состав модуля антивирусной защиты.
  + 1. **Требования к модулю защиты от несанкционированного доступа**

Модуль защиты от несанкционированного доступа должен обеспечивать решение следующих задач:

* разграничение и контроль доступа пользователей к защищаемым ресурсам;
* обеспечение защиты от НСД элементов вычислительной инфраструктуры АПК «ВИФИД»;
* контроль целостности элементов АПК «ВИФИД»;
* централизованное управление политиками безопасности;
* управление отчуждаемыми носителями и портами расширения.
  + 1. **Требования к модулю межсетевого экранирования и обнаружения вторжений**

Модуль межсетевого экранирования и обнаружения вторжений должен обеспечивать решение следующих задач:

* фильтрация пакетов на сетевом уровне, на основе сетевых адресов отправителя и получателя;
* фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* фильтрация пакетов с учетом входного и выходного сетевого интерфейса;
* трансляция сетевых адресов в соответствии с заданными правилами трансляции (NAT);
* регистрация событий информационной безопасности и состояния работы модуля межсетевого экранирования;
* оперативное обнаружение компьютерных атак на заданных границах сетевых сегментов;
* централизованное управление политиками безопасности.
  + 1. **Требования к модулю криптографической защиты**

Модуль криптографической защиты должен обеспечивать решение следующих задач:

* шифрование и расшифрование и маршрутизация IP-пакетов, передаваемых между сегментами защищенной сети с использованием каналов связи общего пользования (internet) и выделенных сетей связи;
* централизованное управление политиками безопасности защищенной сети.
  + 1. **Требования к модулю контроля (анализа) защищенности**

Модуль контроля (анализа) защищенности должен обеспечивать решение следующих задач:

* аудит уязвимостей системного и прикладного программного обеспечения, выявление недостающих обновлений безопасности элементов вычислительной инфраструктуры АПК «ВИФИД»;
* регистрация информации об обнаруженных уязвимостях для последующего их устранения;
* инвентаризация программного и аппаратного обеспечения элементов вычислительной инфраструктуры АПК «ВИФИД».
  + 1. **Требования к модулю мониторинга событий информационной безопасности**

Модуль мониторинга событий информационной безопасности должен обеспечивать решение следующих задач:

* сбор, обработка, отображение и долгосрочное хранение информации о событиях и подозрениях на инциденты информационной безопасности, выявляемых в инфраструктуре АПК «ВИФИД»;
* предоставление инструментов для анализа событий и расследования инцидентов информационной безопасности.
  + 1. **Требования к модулю контроля привилегированных пользователей**

Модуль контроля привилегированных пользователей должен обеспечивать решение следующих задач:

* мониторинг действий привилегированных пользователей АПК «ВИФИД» в реальном времени;
* регистрация информации о действиях привилегированных пользователей АПК «ВИФИД».
  + 1. **Требования к модулю доверенной загрузки**

Модуль доверенной загрузки должен обеспечивать решение следующих задач:

* доверенная загрузка средств вычислительной техники;
* идентификация и аутентификация пользователей;
* ведение журнала регистрации событий.
  + 1. **Требования к модулю резервного копирования**

Модуль резервного копирования должен обеспечивать решение следующих задач:

* резервное копирование информации модулей уровня вычислительной инфраструктуры КЗИ.
  + 1. **Требования к модулю защиты среды виртуализации**

Модуль защиты среды виртуализации должен обеспечивать:

* доверенную загрузку и контроль целостности виртуальных машин;
* сегментацию виртуальной инфраструктуры;
* управление доступом к объектам виртуальной инфраструктуры;
* регистрацию и аудит событий безопасности;
* защиту от специфических угроз, характерных для виртуальных сред.
  1. **Требования к режимам функционирования КЗИ**

КЗИ должен предусматривать следующие режимы функционирования: штатный, автономный.

Штатный режим является основным режимом функционирования КЗИ, при котором поддерживается выполнение всех заявленных функций.

Автономный режим является вспомогательным режимом функционирования отдельных элементов КЗИ, когда все или отдельные их функции становятся недоступными. В этом режиме осуществляются техническое обслуживание, реконфигурация, модернизация и совершенствование компонентов КЗИ.

1. **ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ**
   1. **Требования к оборудованию и программному обеспечению уровня вычислительной инфраструктуры**

Требования к оборудованию и программному обеспечению уровня вычислительной инфраструктуры приведены в приложении А к настоящему документу.

* 1. **Требования к оборудованию и программному обеспечению уровня сетевой инфраструктуры**

Требования к оборудованию и программному обеспечению уровня сетевой инфраструктуры приведены в приложении А к настоящему документу.

* 1. **Требования к оборудованию и программному обеспечению уровня защиты информации**

Требования к оборудованию и программному обеспечению уровня защиты информации приведены в Приложении А к настоящему документу.

* 1. **Общие требования к оборудованию и программному обеспечению**
     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**

Надежность КЗИ должна обеспечиваться следующими методами:

* надежностью работы оборудования в целом и его отдельных компонентов, гарантированной производителем;
* схемами подключения оборудования к коммуникационным сетям и электропитанию;
* структурной надежностью, обеспечиваемой резервированием ключевых элементов:

1. Уровень сетевой инфраструктуры;
2. Уровень защиты информации:

модуль межсетевого экранирования и обнаружения вторжений;

модуль криптографической защиты;

модуль контроля привилегированных пользователей;

* использованием механизмов автоматического переключения на резервные ключевые элементы в случае сбоя основных;
* выполнением требований к организации технического обслуживания и эксплуатации.
  + 1. **Требования к гарантийным обязательствам**

Гарантийный срок на все поставляемое оборудование КЗИ должен составлять не менее 60 (шестидесяти) месяцев с момента подписания Заказчиком товарной накладной (ТОРГ-12). 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.

Срок действия прав на использование программного обеспечения — простой (неисключительной) лицензии на поставляемое программное обеспечение должен составлять не менее 60 (шестидесяти) месяцев с момента подписания Заказчиком Акта приема-передачи прав на программное обеспечение.

В случае, если правообладателем не предусмотрена возможность передачи прав на использование программного обеспечения (простой (неисключительной) лицензии) на 60 (шестьдесят) месяцев и более, права (лицензии) на использование программного обеспечения передаются на максимальный возможный предлагаемый правообладателем срок, при этом Подрядчик предоставляет обязательство (сертификат) на продление срока действия прав (лицензий) до 60 (шестидесяти) месяцев и более (в совокупности).

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

Для обеспечения функционирования КЗИ в рамках гарантийных обязательств Подрядчик обеспечивает гарантийную поддержку поставляемого оборудования и программного обеспечения, включая:

* регистрацию и первичную обработку обращений Заказчика;
* устранение сбоев в работе поставляемого оборудования и программного обеспечения;

Регистрация обращений осуществляется с использованием:

* Средства мониторинга качества сопровождения систем (веб-сервис Заказчика, размещенный в сети »Интернет»).

Гарантийное сопровождение осуществляется сотрудниками Подрядчика на месте размещения программных и технических средств АПК «ВИФИД», а также 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 Подрядчиком Заказчик обязуется:

* в течение 2 (двух) рабочих дней с момента подписания акта сдачи-приемки выполненных работ предоставить Подрядчику акт приема-передачи парольно-ключевой информации, в котором фиксирует всю информацию, необходимую Подрядчику для дистанционной работы с поставляемым оборудованием и программным обеспечением;
* обеспечить Подрядчику доступ к программным и техническим средствам, подлежащим гарантийному сопровождению в соответствии с документами, устанавливающими порядок предоставления доступа к техническим средствам АПК «ВИФИД»;
* оказывать содействие Подрядчику при организации дистанционного подключения к программным и техническим средствам, подлежащим гарантийному сопровождению.

Подрядчик должен предоставить все необходимые реквизиты (в том числе лицензионные номера, сертификаты, пароли и логины для доступа к личным кабинетам на сайтах производителей) и контактные данные (ФИО, адреса электронной почты, контактные телефоны ответственных лиц) для возможности самостоятельного обращения специалистов Заказчика в службу поддержки производителей оборудования или программного обеспечения, если производителем оборудования предусмотрен такой вид доступа.

* + 1. **Требования к защите от влияния внешних воздействий**

Используемые оборудование и материалы, не должны допускать изменений физико-химических параметров в результате воздействия окружающей среды в течение всего срока эксплуатации.

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

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

* + 1. **Требования по экологии и 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 КЗИ, 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 работам по Обследованию АПК «ВИФИД» и разработке (проектированию) КЗИ**

В рамках обследования и разработки (проектирования) КЗИ Подрядчик осуществляет:

* обследование объекта;
* оформление Отчета по результатам обследования объекта;
* разработку и согласование с Заказчиком Технического проекта на создание КЗИ.
  + 1. **Требования к работам по обследованию**
* сбор и анализ исходных данных об АПК «ВИФИД»;
* анализ состава технических и программных средств АПК «ВИФИД»;
* анализ фактического расположения технических и программных средств АПК «ВИФИД»
* анализ возможных уязвимостей и актуальных угроз безопасности информации, содержащейся в АПК «ВИФИД».
  + - 1. **Требования к сбору и анализу исходных данных об АПК «ВИФИД»**

Сбор и анализ исходных данных об АПК «ВИФИД» осуществляется Подрядчиком с целью разработки и документирования информационных характеристик и организационной структуры АПК «ВИФИД».

Для достижения требуемого результата Подрядчик документально фиксирует данные:

* территориальное размещении инфраструктуры АПК «ВИФИД»:
* перечень объектов информатизации;
* границы контролируемой зоны АПК «ВИФИД»;
* назначение, архитектура и конфигурация АПК «ВИФИД»;
* организационные и функциональные условия эксплуатации АПК «ВИФИД»;
* функции АПК «ВИФИД».

Полученные результаты подлежат документальной фиксации в Отчете по результатам обследования объекта, разрабатываемом Подрядчиком.

* + - 1. **Требования к анализу состава технических и программных средств АПК «ВИФИД»**

Анализ состава технических и программных средств АПК «ВИФИД» осуществляется Подрядчиком с целью структурирования информации и документирования текущего материально-технического состояния АПК «ВИФИД».

Для достижения требуемого результата анализа Подрядчик документально фиксирует следующие параметры программных и технических средств:

* производителя технических средств;
* модели технических средств;
* серийные номера технических средств (в случае отсутствия серийного номера технического средства производится нанесение произвольного номера на корпус устройства);
* типы программных средств;
* наименования программных средств;
* версии программных средств;
* производителя программных средств;
* серийные номера программных средств (в случае отсутствия серийного номера программного средства номером может служить уникальный идентификатор лицензии).

Полученные результаты подлежат документальной фиксации в Отчете по результатам обследования объекта, разрабатываемом Подрядчиком.

* + - 1. **Требования к анализу фактического расположения технических и программных средств АПК «ВИФИД»**

Для достижения требуемого результата анализа фактического расположения технических средств Подрядчиком осуществляется разработка:

* схем расположения технических средств АПК «ВИФИД» относительно границ контролируемой зоны;
* схем расположения технических средств АПК «ВИФИД» в помещениях.

Разработанные схемы расположения технических средств АПК «ВИФИД» в помещениях и относительно границ контролируемой зоны, должны быть включены Подрядчиком в Отчет по результатам обследования объекта.

* + - 1. **Требования к анализу возможных уязвимостей и актуальных угроз безопасности информации, содержащейся в АПК «ВИФИД»**

Для достижения требуемого результата анализа возможных уязвимостей и актуальных угроз безопасности информации, содержащейся АПК «ВИФИД», Подрядчиком осуществляется ознакомление с согласованной с ФСТЭК России Моделью угроз безопасности информации АПК «ВИФИД» и документально фиксируются следующие параметры АПК «ВИФИД»:

* структурно-функциональные характеристики АПК «ВИФИД»;
* режимы обработки информации в АПК «ВИФИД»;
* возможности потенциального нарушителя безопасности информации, содержащейся в АПК «ВИФИД».

Результаты анализа возможных уязвимостей и актуальных угроз безопасности информации, содержащейся в АПК «ВИФИД», должны быть включены Подрядчиком в Отчет по результатам обследования объекта.

* + 1. **Требования к оформлению Отчета по результатам обследования объекта**

Для достижения требуемого результата Подрядчик должен разработать Отчет по результатам обследования объекта, содержащий документально зафиксированные результаты работ, перечисленные в п. 6.1.1 настоящего документа.

* + 1. **Требования к разработке Технического проекта на создание КЗИ**

Разработка Технического проекта на создание КЗИ включает:

* разработку и оформление Пояснительной записки к техническому проекту на создание КЗИ;
* разработку и оформление Ведомости технического проекта на создание КЗИ;
* разработку и оформление Ведомости покупных изделий КЗИ;
* разработку и оформление Спецификации средств защиты информации КЗИ;
* разработку и оформление Схемы функциональной структуры КЗИ;
* разработку и оформление Схемы организационной структуры КЗИ;
* разработку и оформление Схемы комплекса технических средств КЗИ;
* разработку и оформление Таблицы кабельных соединений и подключений КЗИ;
* разработку эксплуатационной документации на КЗИ;
* разработка программ и методик испытаний КЗИ.

Разработка рабочей и проектной документации должна выполняться в соответствии с требованиями ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 в объеме и качестве, необходимыми для выполнения монтажных и пусконаладочных работ и для дальнейшей эксплуатации КЗИ.

Формальное полное соответствие документов требованиям ГОСТ серии 34 по составу и структуре разделов не требуется. При этом должно быть предоставлено описание всех видов обеспечения КЗИ, достаточное для развертывания, эксплуатации и сопровождения КЗИ по всем позициям, определяемым ГОСТ серии 34 для отдельных документов.

Документам на КЗИ должны присваиваться уникальные децимальные номера в соответствии с порядком, установленным в ГОСТ 34.201-89.

При разработке (проектировании) КЗИ должны быть учтены требования по интеграции уровней и модулей в единый комплекс технических средств. Должна учитываться необходимость полноценной и эффективной работы КЗИ на длительный период, возможность дальнейшего расширения и наращивания КЗИ, принимая во внимание потребности технического роста и перспективы развития информационных технологий.

* + - 1. **Требования к разработке и оформлению Пояснительной записки к техническому проекту на создание КЗИ**

Пояснительная записка к техническому проекту на создание КЗИ разрабатывается Подрядчиком и должна содержать:

* общие сведения о проектируемой КЗИ;
* общие сведения о функционировании проектируемой КЗИ:
* типы субъектов доступа;
* типы объектов доступа;
* методы управления доступом;
* типы доступа;
* порядок разграничения доступа субъектов доступа к объектам доступа;
* меры защиты информации, содержащейся в АПК «ВИФИД»;
* описание структуры КЗИ, включая:
* модуль антивирусной защиты;
* модуль защиты от несанкционированного доступа;
* модуль межсетевого экранирования и обнаружения вторжений;
* модуль криптографической защиты;
* модуль контроля (анализа) защищенности;
* модуль мониторинга событий информационной безопасности;
* модуль контроля привилегированных пользователей;
* модуль доверенной загрузки;
* модуль резервного копирования;
* модуль защиты среды виртуализации;
* описание и обоснование выбранных технических решений:
* виды и типы используемых средств защиты информации;
* состав средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации;
* меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
* действия по подготовке КЗИ к вводу в действие.
  + - 1. **Требования к разработке и оформлению Ведомости технического проекта на создание КЗИ**

Ведомость технического проекта на создание КЗИ разрабатывается Подрядчиком и должна содержать перечень всех документов, разработанных на соответствующих стадиях создания КЗИ.

* + - 1. **Требования к разработке и оформлению Ведомости покупных изделий КЗИ**

Ведомость покупных изделий разрабатывается Подрядчиком и должна содержать информацию об оборудовании и программном обеспечении, поставляемых для создания КЗИ.

* + - 1. **Требования к разработке и оформлению Спецификации средств защиты информации КЗИ.**

Спецификация средств защиты информации КЗИ разрабатывается Подрядчиком и должна содержать состав средств защиты информации, используемых в составе КЗИ.

* + - 1. **Требования к разработке и оформлению схемы функциональной структуры КЗИ**

Схема функционально структуры КЗИ содержит элементы функциональной структуры КЗИ, информационные связи между элементами.

* + - 1. **Требования к разработке и оформлению схемы организационной структуры КЗИ**

Схема организационной структуры КЗИ содержит состав подразделений (должностных лиц) организаций, обеспечивающих функционирование КЗИ, основные функции и связь между подразделениями (должностными лицами) организаций.

* + - 1. **Требования к разработке и оформлению схемы комплекса технических средств КЗИ**

Схема комплекса технических средств КЗИ содержит состав комплекса технических средств и связи между этими техническими средствами или группами технических средств, объединенными по каким-либо логическим признакам.

* + - 1. **Требования к разработке и оформлению Таблицы кабельных соединений и подключений КЗИ**

Таблица кабельных соединений и подключений КЗИ разрабатывается Подрядчиком и должна содержать информацию о сетевых подключениях технических средств КЗИ к имеющейся ИТ-инфраструктуре Заказчика.

* + - 1. **Требования к разработке эксплуатационной документации на КЗИ**

Эксплуатационная документация разрабатывается Подрядчиком и предназначена для эксплуатации КЗИ, ознакомления с ее структурой, изучения правил эксплуатации, отражения сведений, удостоверяющих гарантированные разработчиком значения основных параметров и характеристик КЗИ.

Эксплуатационная документация должна содержать сведения, необходимые для выполнения персоналом работ по поддержанию уровня эксплуатационных характеристик КЗИ, установленных в проектных решениях.

Эксплуатационная документация должна, в том числе включать:

* Руководство администратора;
* Руководство пользователя.
  + - 1. **Требования к разработке программ и методик испытаний КЗИ**

Программы и методики испытаний КЗИ разрабатываются Подрядчиком и согласовываются с Заказчиком с целью регламентации порядка проверки соответствия КЗИ установленным требованиям и включают следующие документы:

* Программа и методики предварительных испытаний КЗИ;
* Программа опытной эксплуатации КЗИ;
* Программа и методики приемочных испытаний КЗИ.
  1. **Требования к выполнению работ по Поставке оборудования и программного обеспечения КЗИ**
     1. В рамках выполнения работ Подрядчик должен обеспечить закупку, поставку и передачу оборудования и программного обеспечения КЗИ, а также прав использования программного обеспечения в соответствии с требованиями, приведенными в Приложении А к настоящему документу.

Доставка Оборудования для осуществления монтажных и пуско-наладочных работ до места поставки осуществляется организационным и финансовым иждивением Подрядчика и под его ответственность. Стороны составляют акт, в котором фиксируется факт доставки оборудования в место поставки. 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.

* + 1. Программное обеспечение предоставляется на отдельном носителе или по защищенным каналам связи. Подрядчик 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 Технического задания.

Права использования программного обеспечения по настоящему договору предоставляются Заказчику путем заключения cублицензионного соглашения (Приложение В к настоящему документу).

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. Подрядчик гарантирует Заказчику возможность беспрепятственного использования этих прав.

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

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

* 1. **Требования к выполнению работ по Внедрению КЗИ**

Для осуществления монтажных и пуско-наладочных работ Заказчик передает, а Подрядчик принимает оборудование в упакованном виде, без видимых повреждений, по Акту передачи оборудования в монтаж. Ответственность за сохранность оборудования на время проведения монтажных и пуско-наладочных работ несет Подрядчик.

Поставляемое оборудование, предназначенное для установки в телекоммуникационные шкафы, должно быть размещено в существующие телекоммуникационные шкафы с подключением к существующей системе электроснабжения и ЛВС.

Работы по внедрению КЗИ должны осуществляется Подрядчиком с учетом:

* эксплуатационной документации производителей поставляемого оборудования и программного обеспечения;
* законодательства в области защиты информации;
* проектной документации на КЗИ, разрабатываемой Подрядчиком, и настоящего технического задания;

Для выполнения работ по внедрению КЗИ в части монтажа и коммутации поставляемого оборудования должны использоваться материалы, предоставляемые Подрядчиком.

Работы по внедрению КЗИ должны включать:

* установку и настройку поставляемого Подрядчиком оборудования и программного обеспечения уровня вычислительной инфраструктуры;
* установку и настройку поставляемого Подрядчиком оборудования и программного обеспечения уровня сетевой инфраструктуры;
* установку и настройку поставляемого Подрядчиком оборудования и программного обеспечения уровня защиты информации;
* мероприятия по затруднению несанкционированного физического доступа к средствам вычислительной техники АПК «ВИФИД»;
* разработку Технического паспорта АПК «ВИФИД»;
* разработку проектов организационно-распорядительных документов по защите информации;
* инструктаж персонала Заказчика;
* предварительные испытания КЗИ;
* опытную эксплуатацию КЗИ;
* анализ уязвимостей АПК «ВИФИД»;
* приемочные испытания КЗИ.

Разработка проектов организационно-распорядительных документов по защите информации осуществляется в объеме, достаточном для успешного проведения аттестационных испытаний АПК «ВИФИД» по требованиям защиты 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 документа.

* + 1. **Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня вычислительной инфраструктуры**

Установка и настройка поставляемого оборудования и программного обеспечения уровня вычислительной инфраструктуры осуществляется Подрядчиком и включает:

* монтаж оборудования в телекоммуникационные стойки;
* подключение оборудования к электропитанию в телекоммуникационных стойках;
* коммутацию оборудования;
* маркировку коммутационных элементов;
* подключение оборудования к инфраструктуре Заказчика (в пределах коммуникационного шкафа);
* подключение оборудования к каналам связи (в пределах коммуникационного шкафа);
* инсталляцию и настройку операционных систем.
  + 1. **Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня сетевой инфраструктуры**

Установка и настройка поставляемого оборудования и программного обеспечения уровня сетевой инфраструктуры осуществляется Подрядчиком и включает:

* монтаж оборудования в телекоммуникационные стойки;
* подключение оборудования к электропитанию в телекоммуникационных стойках;
* коммутацию оборудования;
* подключение оборудования к инфраструктуре Заказчика (в пределах коммуникационного шкафа);
* подключение оборудования к каналам связи (в пределах коммуникационного шкафа);
* маркировка подключений;
* настройка интерфейсов оборудования;
* настройка маршрутизации оборудования;
* настройка систем управления (при наличии);
* настройка логирования;
* проверка резервирования технических средств (при необходимости);
* проверка резервирования питания (при необходимости);
* инсталляцию программного обеспечения;
* активацию лицензий программного обеспечения.
  + 1. **Требования к установке и настройке поставляемого оборудования и программного обеспечения уровня защиты информации**

Установка и настройка поставляемого оборудования и программного обеспечения уровня защиты информации осуществляется Подрядчиком и включает установку и настройку следующих функциональных модулей:

модуля антивирусной защиты, включая:

* установку, настройку программных комплексов клиентских модулей;
* установку, настройку программного комплекса центра управления.

модуля защиты от несанкционированного доступа, включая:

* установку, настройку программных комплексов клиентских модулей;
* установку, настройку программных комплексов центра управления.

модуля межсетевого экранирования и обнаружения вторжений, включая:

* монтаж в телекоммуникационные стойки;
* подключение к электропитанию в телекоммуникационных стойках;
* коммутацию оборудования;
* маркировку коммутационных элементов;
* подключение к инфраструктуре Заказчика;
* подключение оборудования к каналам связи (в пределах коммуникационного шкафа);
* настройку маршрутизации;
* настройку правил фильтрации межсетевого экранирования;
* настройку логирования;
* проверку резервирования технических средств;
* настройку правил фильтрации трафика.

модуля криптографической защиты, включая:

* монтаж в телекоммуникационные стойки;
* подключение к электропитанию в телекоммуникационных стойках;
* коммутацию оборудования;
* маркировку коммутационных элементов;
* подключение к инфраструктуре Заказчика;
* подключение оборудования к каналам связи (в пределах коммуникационного шкафа);
* настройку программно-аппаратных комплексов криптографической защиты;
* установку, настройку программного комплекса централизованного управления ПАК криптографической защиты;
* проверку резервирования технических средств;
* настройку маршрутизации.

модуля контроля (анализа) защищенности:

* установку, настройку программного комплекса модуля анализа защищенности;
* установку, настройку программного комплекса консоли управления.

модуля мониторинга событий информационной безопасности, включая:

* установку, настройку программного комплекса модуля мониторинга событий информационной безопасности;
* установку, настройку программного комплекса консоли управления;
* настройку правил корреляции событий.

модуля контроля привилегированных пользователей:

* установку, настройку программного комплекса модуля контроля привилегированных пользователей;
* установку, настройку программного комплекса консоли управления;
* проверку резервирования программных средств.

модуля доверенной загрузки:

* установку, настройку программно-аппаратного комплекса модуля доверенной загрузки.

модуля резервного копирования:

* установку, настройку программного комплекса модуля резервного копирования.

модуля защиты среды виртуализации:

* установку, настройку программного комплекса модуля защиты среды виртуализации.
  + 1. **Требования к мероприятиям по затруднению несанкционированного физического доступа к средствам вычислительной техники**

В целях затруднения несанкционированного физического доступа к средствам вычислительной техники АПК «ВИФИД», размещенным в ЦОД, Подрядчик осуществляет:

* замену замков от шкафов, в которых размещаются технические средства АПК «ВИФИД», на замки, имеющие уникальные ключи;
* опечатывание шкафов, в которых размещаются технические средства АПК «ВИФИД»;
* опечатывание корпусов серверов АПК «ВИФИД»;
* разработку документов, регламентирующих разграничение ответственности по обеспечению физической безопасности и устанавливающих порядок предоставления доступа к техническим средствам АПК «ВИФИД», размещенным в ЦОД.
  + 1. **Требования к разработке и оформлению Технического паспорта АПК «ВИФИД»**

Технический паспорт АПК «ВИФИД» разрабатывается Подрядчиком и содержит сведения об АПК «ВИФИД» в объеме, достаточном для полного и своевременного контроля всех стадий жизненного цикла АПК «ВИФИД»: разработки, введения в эксплуатацию, функционирования АПК «ВИФИД» и оценки его эффективности.

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

Организационно-распорядительные документы разрабатываются Подрядчиком и должны определять правила и процедуры эксплуатации КЗИ, необходимые для обеспечения безопасности. Перечень разрабатываемых документов определяется на в момент разработки (проектирования) КЗИ.

* + 1. **Требования к инструктажу персонала Заказчика**

Подрядчик должен организовать инструктаж администраторов безопасности АПК «ВИФИД» в соответствии со следующими требованиями:

* инструктаж проводится в виде одного или нескольких занятий;
* продолжительность занятия — не менее 2-х часов;
* кол-во персонала Заказчика (администраторы), проходящих инструктаж — не более   
  3-х сотрудников на каждый модуль уровня защиты информации.

Форма проведения каждого занятия (очно или удаленно), дата и время проведения определяются по согласованию сторон.

Подрядчик вправе привлекать к проведению инструктажа специализированные обучающие организации.

Место проведения (в случае проведения очного инструктажа) определяется Подрядчиком и согласуется с Заказчиком.

По результатам проведения инструктажа Подрядчик формирует Протокол проведения инструктажа.

* + 1. **Требования к предварительным испытаниям КЗИ**

Предварительные испытания КЗИ должны представлять собой комплекс мероприятий, по результатам проведения которых документально фиксируется факт работоспособности КЗИ и принимается решение о приемке КЗИ в опытную эксплуатацию.

Предварительные испытания КЗИ проводятся в соответствии с документом Программа и методики предварительных испытаний КЗИ, разрабатываемой Подрядчиком, и включают следующие мероприятия:

* испытания КЗИ на работоспособность во всех режимах функционирования, установленных в Техническом задании на создание КЗИ;
* оформление Протокола предварительных испытаний КЗИ;
* устранение недостатков, выявленных в процессе испытаний, и внесение изменений в документацию на КЗИ, в соответствии с Протоколом предварительных испытаний КЗИ (в случае необходимости);
* принятие решения о возможности приемки КЗИ в опытную эксплуатацию.
  + 1. **Требования к опытной эксплуатации КЗИ**

Опытная эксплуатация проводится с целью определения фактических значений количественных и качественных характеристик КЗИ, готовности персонала к работе в условиях функционирования КЗИ, определения фактической эффективности КЗИ.

Опытная эксплуатация проводится в соответствии с Программой опытной эксплуатации КЗИ, разрабатываемой Подрядчиком, включает следующие мероприятия:

* проверку функционирования КЗИ;
* доработку, наладку КЗИ (в случае необходимости);
* проверку готовности пользователей и администраторов к эксплуатации КЗИ;
* оформление проекта Акта о завершении опытной эксплуатации КЗИ.
  + 1. **Требования к анализу уязвимостей АПК «ВИФИД»**

Анализ уязвимостей АПК «ВИФИД» должен представлять собой комплекс мероприятий, по результатам которых проводится оценка возможности преодоления нарушителем КЗИ.

Анализ уязвимостей должен включать:

* проверку отсутствия в программном обеспечении АПК «ВИФИД» уязвимостей, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, которые могут быть использованы нарушителем;
* проверку правильности установки и настройки средств защиты информации;
* проверку корректности работы средств защиты информации при их взаимодействии с техническими и программными средствами АПК «ВИФИД»;
* оформление Протокола анализа уязвимостей АПК «ВИФИД».
  + 1. **Требования к приемочным испытаниям КЗИ**

Приемочные испытания КЗИ должны проводиться в соответствии с Программой и методиками приемочных испытаний КЗИ, разрабатываемой Подрядчиком, и должны включать:

* проверку соответствия КЗИ требованиям Технического задания на создание КЗИ;
* проверку качества опытной эксплуатации КЗИ;
* проверку комплектности и качества рабочей документации КЗИ;
* оформление Протокола приемочных испытаний КЗИ;
* разработку и оформление Заключения по результатам приемочных испытаний КЗИ.
  1. **Требования к выполнению работ по Аттестации АПК «ВИФИД» по требованиям защиты информации**

Работы по аттестации АПК «ВИФИД» по требованиям защиты информации должны включать:

* разработку Программы и методики аттестационных испытаний АПК «ВИФИД»;
* комплексные аттестационные испытания АПК «ВИФИД».
  + 1. **Требования к разработке Программы и методики аттестационных испытаний АПК «ВИФИД»**

Программа и методики аттестационных испытаний АПК «ВИФИД» разрабатывается Подрядчиком и должна содержать описание комплекса мероприятий, по результатам проведения которых Подрядчиком принимается решение о соответствии АПК «ВИФИД» требованиям законодательства области защиты информации.

Программа и методики аттестационных испытаний АПК «ВИФИД» должна разрабатываться в соответствии с ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

Содержание Программы и методики аттестационных испытаний АПК «ВИФИД» должно включать:

* перечень работ и их продолжительность;
* методики испытаний;
* количественный и профессиональный состав аттестационной комиссии;
* используемые технические, программные средства и измерительную аппаратуру.
  + 1. **Требования к комплексным аттестационным испытаниям АПК «ВИФИД»**

Комплексные аттестационные испытания АПК «ВИФИД» должны проводиться в реальных условиях эксплуатации АПК «ВИФИД» путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки информации, содержащейся в АПК «ВИФИД».

Комплексные аттестационные испытания АПК «ВИФИД» должны проводиться в соответствии с ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Комплексные аттестационные испытания, проводимые Подрядчиком, должны включать:

* анализ организационной структуры АПК «ВИФИД», информационных потоков, состава и структуры комплекса технических и программных средств КЗИ на объекте, разработанной документации и ее соответствия требованиям нормативной документации;
* проверку правильности определения класса защищенности, выбора и применения сертифицированных средств защиты информации;
* проверку уровня подготовки персонала и распределения ответственности персонала за обеспечение выполнения требований по безопасности информации;
* анализ уязвимостей АПК «ВИФИД»;
* проверку соответствия АПК «ВИФИД» требованиям законодательства в области защиты информации;
* испытания КЗИ путем осуществления попыток несанкционированного доступа (воздействия) к АПК «ВИФИД» в обход КЗИ.
* документальное оформление результатов аттестационных испытаний, включая:
* Протокол проведения аттестационных испытаний АПК «ВИФИД»;
* Заключение по результатам аттестационных испытаний АПК «ВИФИД»;
* Аттестат соответствия АПК «ВИФИД» требованиям безопасности информации (в случае положительных результатов аттестационных испытаний АПК «ВИФИД»).
  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, совместимом с MS Word, и PDF.
  1. **Общие требования к безопасности работ**

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

Подрядчик 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 влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

* 1. **Требования к Подрядчику**

6.7.1. Подрядчик 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, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания 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), 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, утвержденного постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 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», «е», «г», «д» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

6.7.2. Подрядчик дает свое согласие на осуществление Департаментом информационных технологий города Москвы и органами государственного финансового контроля проверок по исполнению Договора с целью соблюдения условий, целей и порядка предоставления субсидии Заказчику.

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

Требования по порядку сдачи работ и составу отчетной документации приведены в Таблице № 3.

Подрядчик 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 № 3. | | | | | |
| --- | --- | --- | --- | --- | --- |
| **№** | **Наименование работ** | **Сроки выполнения работ** | | **Стоимость  работ, руб.** | **Результаты работ** |
| **Начало работ** | **Окончание работ** |
| 1. | **Обследование АПК «ВИФИД» и разработка (проектирование) КЗИ** | С даты заключения Договора | Не позднее 10 (десяти) календарных дней с даты заключения Договора. |  | Отчетные документы:   * Отчет по результатам обследования объекта; * Технический проект на создание КЗИ в составе: * Пояснительная записка к техническому проекту на создание КЗИ; * Ведомость технического проекта на создание КЗИ; * Ведомость покупных изделий КЗИ; * Спецификация средств защиты информации КЗИ; * Схема функциональной структуры КЗИ; * Схема организационной структуры КЗИ; * Схемы комплекса технических средств КЗИ; * Таблица кабельных соединений и подключений КЗИ; * Руководство администратора; * Руководство пользователя; * Программа и методики предварительных испытаний КЗИ; * Программа опытной эксплуатации КЗИ; * Программа и методики приемочных испытаний КЗИ. |
|  | Обследование объекта |
|  | Оформление Отчета по результатам изучения объекта |
|  | Разработка и согласование с Заказчиком Технического проекта на создание КЗИ |
| 2. | **Поставка оборудования и программного обеспечения КЗИ** | С даты заключения Договора | Не позднее 60 (шестидесяти) календарных дней с даты заключения Договора |  | Отчетные документы:   * Акты фиксации поставки. |
| 3. | **Внедрение КЗИ** | С даты заключения Договора | Не позднее80 (восьмидесяти) календарных дней с даты заключения Договора |  | Отчетные документы:   * Технический паспорт АПК «ВИФИД»; * Комплект организационно-распорядительной документации на реализацию КЗИ (перечень разрабатываемых документов определяется в момент разработки (проектирования) КЗИ); * Протокол проведения инструктажа; * Протокол предварительных испытаний КЗИ; * Акт о завершении опытной эксплуатации КЗИ; * Доработанная документация на КЗИ (в случае необходимости); * Протокол анализа уязвимостей АПК «ВИФИД»; * Протокол приемочных испытаний КЗИ; * Заключения по результатам приемочных испытаний КЗИ. |
|  | Установка и настройка поставляемого оборудования и программного обеспечения уровня вычислительной инфраструктуры |
|  | Установка и настройка поставляемого оборудования и программного обеспечения уровня сетевой инфраструктуры |
|  | Установка и настройка поставляемого оборудования и программного обеспечения уровня защиты информации |
|  | Мероприятия по затруднению несанкционированного физического доступа к средствам вычислительной техники АПК «ВИФИД» |
|  | Разработка Технического паспорта АПК «ВИФИД» |
|  | Разработка проектов организационно-распорядительных документов |
|  | Инструктаж персонала Заказчика |
|  | Предварительные испытания КЗИ |
|  | Опытная эксплуатация КЗИ |
|  | Анализ уязвимостей АПК «ВИФИД» |
|  | Приемочные испытания КЗИ |
| 4. | Аттестация АПК «ВИФИД» по требованиям защиты информации | С даты заключения Договора | Не позднее 90 (девяноста) календарных дней с даты заключения Договора |  | Отчетные документы:   * Программа и методики аттестационных испытаний АПК «ВИФИД»; * Протокол проведения аттестационных испытаний АПК «ВИФИД»; * Заключение по результатам аттестационных испытаний АПК «ВИФИД»; * Аттестат соответствия АПК «ВИФИД» требованиям безопасности информации (в случае положительных результатов аттестационных испытаний АПК «ВИФИД»); * Товарные накладные (ТОРГ-12) на поставляемое оборудование; * Акты приема-передачи прав на программное обеспечение; * Акт сдачи-приемки выполненных работ. |
| 4.1. | Разработка Программы и методики аттестационных испытаний АПК «ВИФИД» |
| 4.2. | Комплексные аттестационных испытания АПК «ВИФИД» |

* 1. **Общие требования к приемке работ**

Все отчетные материалы передаются Подрядчиком с сопроводительными письмами. Подрядчик предоставляет Заказчику утвержденную со своей стороны и согласованную с Пользователем отчетную документацию, оформленную в 1 (одном) экземпляре на бумажных и машинных носителях информации. Первичные бухгалтерские документы предоставляются в соответствии с требованиями действующего законодательства.

Поставка оборудования и программного обеспечения проводится в установленном настоящим техническим заданием порядке.

Сведения о выполнении всех требований настоящего документа и о результатах создания КЗИ в рамках выполнения работ по договору отражаются в акте сдачи-приемки выполненных работ по договору.

Место поставки и передачи оборудования и дистрибутивов программного обеспечения КЗИ определяется по согласованию с Заказчиком в течение 5 (пяти) календарных дней с момента поступления соответствующего запроса от Подрядчика.

По завершению каждого вида работ Подрядчик обязан в течение 2 (двух) рабочих дней передать Заказчику надлежащим образом оформленные документы, перечисленные в п. 7.1 настоящего документа.

Заказчик в течение 5 (пяти) рабочих дней с даты получения указанных документов рассматривает их на предмет соответствия требованиям договора и настоящего технического задания. В случае отсутствия замечаний или наличия замечаний, не препятствующих приемке Работ, Заказчик уведомляет об этом Подрядчика и оформляет в установленном порядке предоставленные Заказчиком документы со своей стороны с направлением Подрядчику одного экземпляра (при необходимости). В случае наличия замечаний, препятствующих приемке Работ, Заказчик уведомляет об этом Подрядчика. Мотивированные замечания подлежат устранению Подрядчиком в течение 5 (пяти) рабочих дней с момента их получения от Заказчика.

Приемка результатов работ по Договору осуществляется после их завершения в полном объеме и оформляется Сторонами путем подписания акта сдачи-приемки выполненных работ.

Вместе с актом сдачи-приемки выполненных работ Подрядчик передает всю отчетную документацию на поставленные в рамках договора оборудование, программное обеспечение и права на программное обеспечение (простая (неисключительная) лицензия), в том числе товарные накладные (ТОРГ 12), сертификаты (декларации о соответствии), обязательные для поставленного оборудования и программного обеспечения, акты приема-передачи прав на программное обеспечение.

**Приложение А  
Требования к оборудованию и программному обеспечению КЗИ**

**Таблица А.1 — Требования к оборудованию и программному обеспечению уровня вычислительной инфраструктуры**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование** | **Характеристики** |
| 1. | Уровень вычислительной инфраструктуры | 1. Уровень вычислительной инфраструктуры должен включать:  * **серверы (Тип 1)** — не менее 5 (пяти) шт.; * **серверы (Тип 2)** — не менее 2 (двух) шт.; * **систему хранения данных (СХД)** — не менее 1 (одной) шт.  1. Срок гарантийных обязательств на все поставляемые серверы и СХД — не менее 60 (шестидесяти) месяцев; 2. Все поставляемые Сервера должны комплектоваться серверными ОС, необходимыми для развертывания средств управления и серверных компонент модулей, перечисленных в пункт 4.1 Технического задания; 3. Не менее 4 (четырех) серверов должны комплектоваться средой виртуализации; 4. **Требования к серверам Тип 1:**    1. Сервер должен быть предназначен для монтажа в 19-дюймовый коммуникационный шкаф, в состав поставки должен входить крепежный комплект для установки в коммуникационный шкаф;    2. Высота сервера — не более 1U;    3. Сервер должен иметь в комплекте не менее двух заменяемых независимых блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц (в соответствии с ГОСТ 29322-2014) с поддержкой замены в рабочем режиме (hot-swap);    4. Максимальная потребляемая мощность одного блока питания — не более 750 Ватт;    5. Должно быть обеспечено наличие кнопки включения (выключения) сервера;    6. Количество отсеков для установки дисков с «горячей» заменой — не менее 4 шт.;    7. Количество слотов для оперативной памяти на материнской плате — не менее 12 шт.;    8. Сервер должен комплектоваться процессорами со следующими характеристиками:  * Количество процессоров — не менее 2 шт.; * Количество ядер каждого процессора — не менее 14 шт.; * Количество потоков каждого процессора — не менее 28 шт.; * Базовая тактовая частота процессора — не менее 2,6ГГц; * Объем кэш-памяти процессора — не менее 19 МБ.   1. Сервер должен комплектоваться оперативной памятью со следующими характеристиками: * Общий объем установленной оперативной памяти — не менее 160ГБ; * Частота функционирования оперативной памяти — не менее 2666МГц; * Пропускная способность памяти — не менее 21300Мб/с.   1. Сервер должен комплектоваться твердотельными накопителями со следующими характеристиками: * Количество накопителей — не менее 2 шт.; * Тип накопителей — SSD; * Емкость каждого накопителя — не менее 240ГБ; * Ресурс накопителя — не менее 922 TWB; * Ресурс DWPD — не менее 2 перезаписей всего объема накопителя в день в течение 5 лет; * Скорость чтения — не менее 560Мб/с; * Скорость записи — не менее 280Мб/с.   1. Сервер должен содержать следующие интерфейсы: * Не менее 2 (двух) сетевых интерфейсов Ethernet RJ45 с поддержкой скорости не менее 1Гб/с; * Не менее 2 (двух) оптических сетевых интерфейсов FiberChannel с установленными трансиверами с поддержкой скорости не менее 8Гб/с; * Не менее 1 (одного) интерфейса управления платформой (IPMI); * Не менее 1 (одного) видеоинтерфейса VGA; * Не менее 3 (трех) интерфейсов USB 3.0.  1. **Требования к серверам Тип 2:**    1. Сервер должен быть предназначен для монтажа в 19-ти дюймовый коммуникационный шкаф, в состав поставки должен входить крепежный комплект для установки в коммуникационный шкаф;    2. Высота сервера — не более 1U;    3. Сервер должен иметь в комплекте не менее одного блока электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц в соответствии с ГОСТ 29322-2014;    4. Максимальная потребляемая мощность — не более 350 Ватт;    5. Должно быть обеспечено наличие кнопки включения (выключения) сервера;    6. Количество отсеков для установки дисков с «горячей» заменой — не менее 4 шт.;    7. Количество слотов для оперативной памяти на материнской плате — не менее 4 шт.;    8. Сервер должен комплектоваться процессорами со следующими характеристиками:  * Количество процессоров — не менее 1 шт.; * Количество ядер каждого процессора — не менее 2 шт.; * Количество потоков каждого процессора — не менее 2 шт.; * Базовая тактовая частота процессора — не менее 3,3ГГц; * Объем кэш-памяти процессора — не менее 3 МБ.   1. Сервер должен комплектоваться оперативной памятью со следующими характеристиками: * Общий объем установленной оперативной памяти — не менее 8ГБ; * Частота функционирования оперативной памяти — не менее 2133МГц; * Пропускная способность памяти — не менее 17064Мб/с.   1. Сервер должен комплектоваться твердотельными накопителями со следующими характеристиками: * Количество накопителей — не менее 2 шт.; * Тип накопителей — SSD; * Емкость каждого накопителя — не менее 240ГБ; * Ресурс накопителя — не менее 922 TWB; * Ресурс DWPD — не менее 2 перезаписей всего объема накопителя в день в течение 5 лет; * Скорость чтения — не менее 560Мб/с; * Скорость записи — не менее 280Мб/с.   1. Сервер должен содержать следующие интерфейсы: * Не менее 2 (двух) сетевых интерфейсов Ethernet RJ45 с поддержкой скорости не менее 1Гб/с; * Не менее 2 (двух) оптических сетевых интерфейсов FiberChannel с установленными трансиверами с поддержкой скорости не менее 8Гб/с; * Не менее 1 (одного) интерфейса управления платформой (IPMI); * Не менее 1 (одного) видеоинтерфейса VGA; * Не менее 3 (трех) интерфейсов USB 3.0.  1. **Требования к системе хранения данных (СХД):**    1. СХД должна быть предназначена для монтажа в 19-ти дюймовый коммуникационный шкаф, в состав поставки должен входить крепежный комплект для установки в коммуникационный шкаф;    2. Высота СХД — не более 2U;    3. Количество контроллеров — не менее 2 (двух) шт.;    4. Тип кэш-памяти — DDR3;    5. Объем кэш-памяти на каждый контроллер — не менее 16Гб;    6. СХД должна иметь функционал резервного копирования (защиты) кэш-памяти;    7. СХД должна иметь в комплекте не менее двух блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц в соответствии с ГОСТ 29322-2014, с поддержкой замены в рабочем режиме (hot-swap);    8. Максимальная потребляемая мощность одного блока питания — не более 750 Ватт;    9. СХД должна содержать следующие интерфейсы:  * Не менее 2 (двух) интерфейсов SAS для подключения полок расширения с поддержкой скорости не менее 12Гб/с; * Не менее 8 (восьми) оптических сетевых интерфейсов FiberChannel с установленными трансиверами с поддержкой скорости не менее 8Гб/с; * Не менее 8 (восьми) интерфейсов iSCSI с поддержкой скорости не менее 1Гб/с;   1. Должна иметь поддержку уровней RAID: 0, 1, 5, 6, 10;   2. Количество отсеков для установки дисков — не менее 24 шт.;   3. СХД должна комплектоваться SSD накопителями со следующими характеристиками: * Количество накопителей — не менее 2 шт.; * Емкость каждого накопителя — не менее 800ГБ; * Интерфейс подключения накопителя — SAS с пропускной способностью не менее 12Гб/c; * Ресурс накопителя — не менее 4300 TWB; * Ресурс DWPD — не менее 3 перезаписей всего объема накопителя в день в течение 5 лет; * Скорость чтения — не менее 1100Мб/с; * Скорость записи — не менее 950Мб/с.   1. СХД должна комплектоваться жесткими дисками со следующими характеристиками: * Количество дисков — не менее 8 шт.; * Тип интерфейса подключения — SAS; * Емкость каждого диска — не менее 2,4ТБ; * Скорость вращения шпинделя — не менее 10000 оборотов/мин.; * Кеш-память — не менее 256МБ.   1. СХД должна комплектоваться не менее чем 1 (одной) дисковой полкой с характеристиками: * Высота дисковой полки — не более 4U; * Должна иметь в комплекте не менее двух блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц в соответствии с ГОСТ 29322-2014 с поддержкой замены в рабочем режиме (hot-swap); * Максимальная потребляемая мощность одного блока питания — не более 1600 Ватт; * Должна иметь не менее 6 (шести) интерфейсов SAS с поддержкой скорости не менее 12Гб/с; * Количество отсеков для установки дисков — не менее 60 шт.; * Дисковая полка должна комплектоваться жесткими дисками со следующими характеристиками:   + Количество дисков — не менее 60 шт.;   + Тип интерфейса подключения — SAS;   + Емкость каждого диска — не менее 16ТБ;   + Скорость вращения шпинделя — не менее 7200 оборотов/мин.;   + Кеш-память — не менее 256МБ. |

**Таблица А.2 — Требования к оборудованию и программному обеспечению уровня сетевой инфраструктуры**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование** | **Характеристики** |
| 1. | Уровень сетевой инфраструктуры | 1. Уровень сетевой инфраструктуры должен включать:  * **коммутаторы (Тип 1)** для балансировки сетевого трафика для модуля межсетевого экранирования и обнаружения вторжений — не менее 8 (восьми) шт.; * **коммутаторы (Тип 2)** для агрегации соединений с элементами уровня вычислительной инфраструктуры АПК «ВИФИД» и соединений интерфейсов управления — не менее 4 (четырех) шт.  1. Срок гарантийных обязательств на все поставляемые коммутаторы — не менее 60 (шестидесяти) месяцев; 2. Срок технической поддержки 8x5 от производителя как на аппаратную, так и на программную составляющую коммутатора — не менее 60 (шестидесяти) месяцев; 3. **Требования к коммутаторам Типа 1:**  * Коммутатор должен содержать не менее 16 портов типа QSFP28 с поддержкой скорости до 100Гб/с и форматов кабелей как медных (DAC) так и оптических. Каждый порт должен поддерживать следующие скорости: 10/25/40/50/100Гб/с.; * Коммутатор должен обеспечивать полную пропускную способность всех портов на максимальной их скорости — производительность матрицы коммутации не менее 3.2Тб/с и не менее 2.38 Миллиардов пакетов в сек., при размере пакетов 64Байт; * Направление воздушного потока — от портов к блокам питания; * Коммутатор должен иметь в комплекте не менее двух заменяемых независимых блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц (в соответствии с ГОСТ 29322-2014) с поддержкой замены в рабочем режиме (hot-swap); * Максимальная потребляемая мощность — не более 350Вт.; * Высота коммутатора — не более 1U; * Коммутатор должен быть предназначен для монтажа в 19-ти дюймовый коммуникационный шкаф, в состав поставки должен входить крепежный комплект для установки в коммуникационный шкаф; * Коммутатор должен иметь не менее 1 порта внешнего управления типа Ethernet RJ45; * Коммутаторы должны комплектоваться трансиверами и соединительными шнурами в количестве, необходимом для обеспечения балансировки сетевого трафика поставляемого Подрядчиком модуля межсетевого экранирования и обнаружения вторжений. Заказчик обеспечивает наличие свободных портов (интерфейсов) на пограничных маршрутизаторах (не менее 12 портов с поддержкой скорости до 40Гб/с либо 4 порта с поддержкой скорости до 100Гб/с на каждом из двух устройств) и коммутаторах ядра (не менее 12 портов с поддержкой скорости до 40Гб/с). Трансиверы и соединительные шнуры для портов (интерфейсов), предоставляемых Заказчиком на пограничных маршрутизаторах и коммутаторах ядра предоставляются Подрядчиком; * Должна быть обеспечена поддержка нижеследующих протоколов и функций уровня 2 модели OSI:   + Мульти шасси LAG (MLAG), MLAG с поддержкой STP;   + IGMPv2/v3, Snooping;   + VLAN 802.1Q (до 4000 VLANs одновременно);   + 802.1W Rapid Spanning Tree;   + 802.1Q Multiple STP;   + RSTP и PVRST;   + Агрегация каналов 802.3ad (LAG) и LACP. * Должна быть обеспечена поддержка нижеследующих протоколов и функций уровня 3 модели OSI:   + поддержка User/Management VRFs — до 64 VRF;   + IPv4 и IPv6 маршрутизация, включая route-maps;   + Статическая маршрутизация, BGP4, OSPFv2;   + BFD (BGP, OSPF, static routes);   + VRRP;   + DHCPv4/v6 Relay;   + Router Port, interface VLAN;   + ECMP, 64-way;   + IGMPv2/v3 Snooping Querier. * Должна быть обеспечена поддержка протоколов NTP, OpenFlow, FTP/TFTP, SNMP v2,3, DHCP, SSHv2, SYSLOG; * Должна быть обеспечена поддержка зеркалирования портов (SPAN и ERSPAN); * Должна быть обеспечена поддержка агрегации линков LACP (IEEE 802.3ad); * Должны быть обеспечены следующие функции безопасности:   + Контроль шторма на 2-ом уровне модели OSI;   + Контроль списков доступа на 2-4 уровнях модели OSI (ACLs L2-L4 & user defined).  1. **Требования к коммутаторам Тип 2:**  * Должен содержать не менее 48 портов типа 10/100/1000Base-T RJ-45 с поддержкой скорости до 1Гб/c и не менее 4 портов 10GBase-X для установки SFP+ модулей с поддержкой скорости до 10Гб/с; * Коммутатор должен обеспечивать производительность матрицы коммутации не менее 128Гб/с и не менее 131 миллионов пакетов в сек.; * Направление воздушного потока — от портов к блокам питания; * Коммутатор должен иметь в комплекте не менее двух заменяемых независимых блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц (в соответствии с ГОСТ 29322-2014) с поддержкой замены в рабочем режиме (hot-swap); * Максимальная потребляемая мощность — не более 350Вт.; * Высота коммутатора — не более 1U; * Коммутатор должен быть предназначен для монтажа в 19-ти дюймовый коммуникационный шкаф, в состав поставки должен входить крепежный комплект для установки в коммуникационный шкаф; * Коммутатор должен иметь не менее 1 порта внешнего управления типа Ethernet RJ45; * Коммутаторы должны комплектоваться трансиверами и соединительными шнурами в количестве, необходимом для обеспечения агрегации соединений с элементами уровня вычислительной инфраструктуры, поставляемыми Поставщиком и агрегации соединений интерфейсов управления. * Коммутатор должен иметь поддержку технологии Multi-Chassis Link Aggregation (MLAG); * Коммутатор должен иметь поддержку протоколов защиты от петель 802.1w; * Коммутатор должен иметь возможность поддержки протоколов маршрутизации OSPF, BGP; * Должна быть обеспечена поддержка протоколов NTP, SNMP v2,3, DHCP, SSHv2,. SYSLOG; * Должна быть обеспечена поддержка агрегации линков LACP (IEEE 802.3ad);   Должна быть обеспечена поддержка протокола VRRP или аналога; |

**Таблица А.3 — Требования к оборудованию и программному обеспечению уровня защиты информации**

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование** | **Характеристики** |
|  | Модуль (система) антивирусной защиты (САЗ) | 1. САЗ должна включать:  * **программные средства антивирусной защиты для рабочих станций Windows;** * **программные средства антивирусной защиты для серверов Windows;** * **программные средства антивирусной защиты для серверов Linux;** * **программные средства централизованного управления, мониторинга и обновления.**  1. Срок действия простой (неисключительной) лицензии на использование программных средств: не менее 60 месяцев; 2. САЗ должна представлять собой программное обеспечение с возможностью единовременной эксплуатации на АРМ и серверах в количестве не менее 272; 3. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке; 4. Программные средства антивирусной защиты должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 5. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке; 6. САЗ должна иметь возможность интеграции с модулем мониторинга событий информационной безопасности (экспорт событий); 7. Требования к программным компонентам антивирусной защиты:    1. **Требования к программным средствам антивирусной защиты для рабочих станций Windows:**       1. Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:  * Microsoft Windows 10.   + 1. Программные средства антивирусной защиты для рабочих станций Windows должны иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к средствам антивирусной защиты (ФСТЭК России, 2012) и Профиле защиты средств антивирусной защиты типа «В» 4 класса защиты или выше;     2. Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: * антивирусного сканирования в режиме реального времени и по запросу из контекстного меню объекта; * антивирусного сканирования по расписанию; * антивирусного сканирования подключаемых устройств; * эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; * нейтрализации действий активного заражения; * анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; * анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; * блокировки действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; * отката действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; * ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; * антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; * защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP; * фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; * проверки сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; * блокировки баннеров и всплывающих окон на загружаемых Web-страницах; * распознавания и блокировки фишинговых и небезопасных сайтов; * защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; * контроля сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений; * создания специальных правил, запрещающих или разрешающих установку или запуск программ для всех или для определенных групп пользователей (локальных пользователей или групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; * контроля работы пользователя с внешними устройствами ввода-вывода по типу устройства или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору; * записи в журнал событий о записи или удалении файлов на съемных дисках; * контроля работы пользователя с сетью «Интернет», в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля; * защиты от атак типа BadUSB; * запуска специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. * защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля; * установки только выбранных компонентов программного средства антивирусной защиты; * централизованного управления всеми вышеуказанными компонентами с помощью единой системы управления; * запуска задач по расписанию или сразу после запуска приложения; * ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; * проверки целостности антивирусной программы; * добавления исключений из антивирусной проверки по контрольной сумме файла, маске имени (директории) или по наличию у файла доверенной цифровой подписи; * наличия у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; * наличия защищенного хранилища для отчетов о работе антивируса; * включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей; * защиты паролем восстановление объектов из резервного хранилища.   1. **Требования к программным средствам антивирусной защиты для серверов Windows:**      1. Программные средства антивирусной защиты для серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: * Microsoft Windows Server 2016; * Microsoft Windows Server 2019.   + 1. Программные средства антивирусной защиты для серверов Windows должны иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к средствам антивирусной защиты (ФСТЭК России, 2012) и Профиле защиты средств антивирусной защиты типа «Б» 4 класса защиты или выше;     2. Программные средства антивирусной защиты для серверов Windows должны обеспечивать реализацию следующих функциональных возможностей: * антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; * антивирусное сканирование по расписанию; * антивирусное сканирование подключаемых устройств; * эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; * нейтрализации действий активного заражения; * анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; * анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; * блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; * откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; * ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; * антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; * возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; * создания специальных правил, запрещающих или разрешающих установку или запуск программ для всех или же для определенных групп пользователей (локальных пользователей или групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; * запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям; * защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; * установки только выбранных компонентов программного средства антивирусной защиты; * централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; * запуск задач по расписанию или сразу после загрузки операционной системы; * гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; * ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; * возможность проверки целостности антивирусной программы; * возможность добавления исключений из антивирусной проверки по контрольной сумме файла, маске имени (директории) или по наличию у файла доверенной цифровой подписи; * наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; * наличие защищенного хранилища для отчетов о работе антивируса; * возможность включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей; * возможность защитить паролем восстановление объектов из резервного хранилища.   1. **Требования к программным средствам антивирусной защиты для серверов Linux:**      1. Программные средства антивирусной защиты для серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: * Ubuntu 18.04; * CentOS 7.7.   + 1. Программные средства антивирусной защиты для серверов Linux должны иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к средствам антивирусной защиты (ФСТЭК России, 2012) и Профиле защиты средств антивирусной защиты типа «Б» 4 класса защиты или выше;     2. Программные средства антивирусной защиты для серверов Linux должны обеспечивать реализацию следующих функциональных возможностей: * резидентного антивирусного мониторинга; * проверку ресурсов доступных по SMB/NFS; * эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; * антивирусное сканирование по команде пользователя или администратора и по расписанию; * антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz; .tgz; .arj.; * наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); * защиту файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования; * помещение подозрительных и поврежденных объектов на карантин; * возможность перехвата и проверки файловых операций на уровне SAMBA; * управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; * запуск задач по расписанию или сразу после загрузки операционной системы; * возможность экспортировать и сохранять отчеты в форматах HTML и CSV; * гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; * сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию; * возможность управления через пользовательский графический интерфейс без root прав; * централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.   1. **Требования к программным средствам централизованного управления, мониторинга и обновления:**      1. Программные средства управления, мониторинга и обновления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей: * Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС; * Централизованные установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе; * Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; * Наличие различных методов установки антивирусных агентов: для удаленной установки — RPC, GPO, агент администрирования, для локальной установки — возможность создать автономный пакет установки; * Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз; * Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; * Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения; * Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; * Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; * Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; * Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; * Автоматическое распространение лицензии на клиентские компьютеры; * Возможность подключения по RDP или штатными средствами из консоли управления; * Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; * Поддержка функциональности управления шифрованием данных; * Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; * Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления; * Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и т.д.; * Экспорт отчетов в файлы форматов PDF и XML; * Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; * Создание внутренних учетных записей для аутентификации на сервере управления; * Создание резервной копии системы управления встроенными средствами системы управления; * Наличие веб-консоли управления приложением; * Наличие системы контроля возникновения вирусных эпидемий.   + 1. Программные средства управления, мониторинга и обновления должны иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к средствам антивирусной защиты (ФСТЭК России, 2012) и Профиле защиты средств антивирусной защиты типа «А» 4 класса защиты или выше;   1. Требования к обновлению антивирусных баз:      1. Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: * Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток; * Множественность путей обновления, в том числе — по каналам связи и на отчуждаемых электронных носителях информации; * Проверку целостности и подлинности обновлений средствами электронной цифровой подписи. |
|  | Модуль (система) защиты от несанкционированного доступа (СЗИ НСД) | 1. Система защиты от НСД должна включать:  * программный комплекс средств защиты информации в операционных системах семейства Linux **(СЗИ НСД Тип 1)** с возможностью единовременной эксплуатации на серверах в количестве не менее 174 шт.; * программный комплекс средств защиты информации в операционных системах семейства Windows **(СЗИ НСД Тип 2)** с возможностью единовременной эксплуатации на АРМ и серверах в количестве не менее 4 шт.  1. Срок действия простой (неисключительной) лицензии на использование программных средств защиты информации: не менее 60 месяцев; 2. Программные средства СЗИ НСД должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СЗИ от НСД должно иметь действующий сертификат ФСТЭК России, подтверждающий соответствие:  * требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — не ниже 5 класса защищенности или требованиям, указанным в технических условиях (заданиях безопасности); * требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4-го.  1. **СЗИ НСД Тип 1** должно быть предназначено для работы на серверах под управлением следующих операционных систем:  * Ubuntu 18.04.  1. **СЗИ НСД Тип 2** должно быть предназначено для работы на АРМ и серверах под управлением следующих операционных систем:  * Microsoft Windows 10; * Microsoft Windows Server 2016; * Microsoft Windows Server 2019.  1. **СЗИ НСД Тип 1 и Тип 2** должны обеспечивать:  * контроль входа пользователей в систему как по логину и паролю, так и с использованием аппаратных средств аутентификации; * разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) сервера; * возможность контроля целостности аппаратной конфигурации сервера; * возможность контроля целостности критических объектов операционной системы и ресурсов файловой системы компьютера; * регистрация событий безопасности в журнале безопасности, контроль действий пользователей: доступ к защищаемым файлам и устройствам; * возможность локального и удаленного централизованного администрирования. |
|  | Модуль (система) межсетевого экранирования и обнаружения вторжений (СМЭ) | 1. Система межсетевого экранирования и обнаружения вторжений должна включать:  * программно-аппаратный комплекс межсетевого экранирования (**СМЭ Тип 1**) — комплект, с количеством устройств, достаточным для обработки сетевого трафика в объеме не менее 160Гб/с; * программно-аппаратный комплекс межсетевого экранирования с функционалом обнаружения вторжений (**СМЭ Тип 2**) — комплект, с количеством устройств, достаточным для обработки сетевого трафика в объеме не менее 20Гб/с; * программно-аппаратный **комплекс управления СМЭ —** не менее 2-х шт.  1. Срок гарантийных обязательств на все поставляемые устройства комплексов СМЭ — не менее 60 (шестидесяти) месяцев; 2. **СМЭ Тип 1** должна иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к межсетевым экранам (ФСТЭК России, 2016) и Профиле защиты межсетевого экрана типа «А» четвертого класса защиты или выше; 3. **СМЭ Тип 2** должна иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к межсетевым экранам (ФСТЭК России, 2016), Профиле защиты межсетевого экрана типа «А» четвертого класса защиты или выше, Требованиях к системам обнаружения вторжений (ФСТЭК России, 2011) и Профиле защиты систем обнаружения вторжений уровня сети четвертого класса защиты или выше; 4. Программно-аппаратные комплексы СМЭ должны быть предназначены для установки в 19-ти дюймовую монтажную стойку; 5. Программно-аппаратные комплексы СМЭ должны комплектоваться трансиверами и соединительными шнурами в количестве, необходимом для обеспечения совместной работы с Коммутаторами Типа 1, поставляемых Подрядчиком; 6. Комплект программно-аппаратных комплексов **СМЭ Тип 1,** обеспечивающий обработку сетевого трафика в объеме не менее 160Гб/с должен соответствовать следующим требованиям:  * наличие горячего резервирования по схеме не хуже N+1; * высота комплекта устройств — не более 20U; * наличие возможности горизонтального масштабирования системы; * наличие возможности осуществления межсетевого экранирования на уровнях L2 и L3 модели OSI.  1. Каждый программно-аппаратный комплекс **СМЭ Тип 1** должен соответствовать следующим требованиям:  * наличие в комплекте не менее двух заменяемых независимых блоков электропитания от переменного электрического тока (типа AC) напряжением 230 Вольт, частотой 50Гц (в соответствии с ГОСТ 29322-2014); * поддержка объединения в кластер с возможностью создания типов кластеров: active/passive; * количество выделенных интерфейсов управления — не менее 1 шт.; * количество интерфейсов пропускной способностью не менее 10Гб/с — не менее 16 шт.; * возможность осуществления межсетевого экранирования: создание правил фильтрации сетевого трафика на основе IP адресов, портов и протоколов; * возможность фильтрации пакетов на прикладных уровнях; * поддержка протоколов динамической маршрутизации OSPF и BGP; * возможность управления полосой пропускания трафика; * поддержка VLAN (802.1Q); * поддержка функций NAT, PAT;  1. Комплект программно-аппаратных комплексов **СМЭ Тип 2,** обеспечивающий обработку сетевого трафика в объеме не менее 20Гб/с должен соответствовать следующим требованиям:  * наличие горячего резервирования по схеме не хуже N+1; * высота комплекта устройств — не более 20U; * наличие возможности горизонтального масштабирования системы;  1. Каждый программно-аппаратный комплекс **СМЭ Тип 2** должен соответствовать требованиям, предъявляемым к СМЭ Тип 1, а так же следующим требованиям:  * Функционал обнаружения и предотвращения вторжений (IDS);  1. Программно-аппаратные **комплексы управления СМЭ** должны соответствовать следующим требованиям:  * полная совместимость с СМЭ Тип 1 и СМЭ Тип 2, входящими в комплект поставки; * наличие функционала построения отказоустойчивой конфигурации; * количество управляемых программно-аппаратных комплексов СМЭ Тип 1 и СМЭ Тип 2 — не менее количества всех устройств СМЭ Тип 1 и СМЭ Тип 2, входящие в комплекты поставки; * возможность управления через WEB-интерфейс по протоколу HTTP; * регистрация в системных журналах различных событий, в том числе протоколирование работы фильтров и действий администраторов; |
|  | Модуль (система) криптографической защиты (СКЗИ) | 1. Система криптографической защиты должна включать:  * программно-аппаратный комплекс, реализующий функции криптографического шлюза для взаимодействия с внешними информационными системами **(СКЗИ Тип 1)** в количестве не менее 4 шт.; * программно-аппаратный комплекс, реализующий функции криптографического шлюза для взаимодействия между площадками АПК «ВИФИД» **(СКЗИ Тип 2)** в количестве не менее 4 шт.; * программный комплекс защиты информации для АРМ **(СКЗИ Тип 3)** в количестве не менее 50 шт.; * программный **комплекс управления защищенной сетью СКЗИ** в количестве не менее 1 шт.  1. Срок действия простой (неисключительной) лицензии на использование программных комплексов: не менее 60 месяцев; 2. Программные комплексы СКЗИ должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. Срок гарантийных обязательств на программно-аппаратные комплексы СКЗИ всех типов — не менее 60 (шестидесяти) месяцев; 4. Каждый программно-аппаратный комплекс **СКЗИ Тип 1** должен обеспечивать:  * возможность монтажа в стандартную 19-ти дюймовую монтажную стойку; * производительность шифрования — не менее 5 Гб/с; * осуществление функции прокси-сервера защищенных соединений; * предоставление функции туннелирующего сервера без ограничений на число лицензий для туннелируемых IP-адресов; * предоставление функции сервера IP-адресов; * поддержка режима горячего резервирования (failover); * шифрование каждого IP-пакета на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищенной сетью.   1. Высота СКЗИ Тип 1 — не более 1U;   2. Максимальная потребляемая мощность СКЗИ Тип 1 — не более 500Вт.;   3. Каждый программно-аппаратный комплекс СКЗИ Тип 1 должен иметь не менее 4 (четырех) сетевых интерфейса 10/100/1000 Мбит/с и не менее 4 (четырех) сетевых интерфейса 10G SPF+ Ethernet 10 Гбит/с;   4. СКЗИ Тип 1 должен иметь действующий сертификат ФСБ России, подтверждающий соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации;  1. Каждый программно-аппаратный комплекс **СКЗИ Тип 2** должен обеспечивать:  * возможность монтажа в стандартную 19-ти дюймовую монтажную стойку; * производительность шифрования — не менее 800Мб/с; * предоставление функции туннелирующего сервера без ограничений на число лицензий для туннелируемых IP-адресов; * предоставление функции сервера IP-адресов; * поддержка режима горячего резервирования (failover); * шифрование каждого IP-пакета на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищенной сетью.   1. Высота СКЗИ Тип 2 — не более 1U;   2. Максимальная потребляемая мощность СКЗИ Тип 1 — не более 500Вт.;   3. Каждый программно-аппаратный комплекс СКЗИ Тип 1 должен иметь не менее 4 (четырех) сетевых интерфейса 10/100/1000 Мбит/с и не менее 2 (двух) сетевых интерфейса 1G SPF Ethernet 1 Гбит/с;   4. СКЗИ Тип 2 должен иметь действующий сертификат ФСБ России, подтверждающий соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации;  1. Каждый программный комплекс **СКЗИ Тип 3** должен обеспечивать:  * поддержку прозрачной работы через различные NAT-устройства; * безопасную передачу (прием) данных VPN-шлюзам и VPN-клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования; * наличие драйвера сетевой защиты, непосредственно взаимодействующего с драйвером сетевого интерфейса и осуществляющего контроль и фильтрацию сетевого трафика; * наличие сервиса управления драйвером сетевой защиты, обеспечивающего функционирование узла в защищенной сети, а именно загрузку в драйвер защиты правил фильтрации, справочной информации о структуре защищенной сети и ключей шифрования, сведений о сетевых параметрах доступа для узлов защищенной сети, передачу в ПО VPN-клиента результатов обработки IP-пакетов; * наличие драйвера шифрования IP-пакетов, осуществляющего шифрование и имитозащиту сетевого трафика на ключах, созданных с использованием программного комплекса управления защищенной сетью СКЗИ; * конфиденциальность, целостность и аутентификацию каждого IP-пакета; * настройки сетевых фильтров, параметров доступа к VPN-узлам и аудита событий; * возможность обновления ключевой и справочной информации, а также программного обеспечения СКЗИ Тип 3; * сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя; * наличие службы контроля приложений, осуществляющей контроль сетевой активности приложений и позволяющей реализовывать политики доступа приложений в сеть; * возможность реализации дополнительных сервисов: защищенный чат, защищенная конференция, защищенный обмен файлами. * СКЗИ Тип 3 должна функционировать на АРМ под управлением операционной системы Microsoft Windows 10;   1. СКЗИ Тип 3 должен иметь действующий сертификат ФСБ России, подтверждающий соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 или выше и возможности использования для криптографической защиты (шифрования и имитозащиты IP-трафика) информации;  1. Программный **комплекс управления защищенной сетью СКЗИ** должен обеспечивать:  * функционал формирования и управления топологией VPN-сети, а также обеспечения ключевой информацией узлы и пользователей VPN-сети; * возможностью их установки на разные автоматизированные рабочие места компонент, отвечающих за управление топологией VPN-сети и управление ключевой информацией VPN сети; * механизмы создания резервной копии и восстановления структуры VPN-сети с сохранением всех настроек; * прозрачную работу через различные NAT-устройства.   1. Программный комплекс управления защищенной сетью СКЗИ должен иметь действующий сертификат ФСБ России, подтверждающий соответствие требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 или выше и возможности использования для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функций для файлов и данных, содержащихся в областях оперативной памяти, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. №63 «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации. |
|  | Модуль (система) контроля (анализа) защищенности (СКАЗ) | 1. Система контроля (анализа) защищенности должна включать:  * программный комплекс контроля (анализа) защищенности, предназначенный для сканирования, просмотра результатов и контроля не менее 350 элементов IT-инфраструктуры Заказчика (IP-адресов).  1. Срок действия простой (неисключительной) лицензии на использование программного комплекса: не менее 60 месяцев; 2. Программный комплекс контроля (анализа) защищенности должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СКАЗ должна иметь действующий сертификат ФСТЭК России, подтверждающий соответствие:  * требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — не ниже 5 класса защищенности или требованиям, указанным в технических условиях (заданиях безопасности); * требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4-го.  1. СКАЗ должна обеспечивать:  * аудит уязвимостей системного и прикладного программного обеспечения:   + сигнатурный анализ данных, собранных при сканировании сетевого узла и предоставление информации об обнаруженных уязвимостях;   + сканирование группы сетевых узлов;   + сканирование платформ Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Ubuntu 18.04, CentOS 7.7; * выявление недостающих обновлений безопасности; * аудит конфигурации безопасности согласно указанному профилю; * инвентаризацию аппаратного и программного обеспечения сканируемых систем; * идентификация открытых сетевых портов и сервисов; * формирование отчетов по результатам сканирования.  1. Управление СКАЗ должно осуществляться с помощью графической консоли; 2. СКАЗ должна реализовывать хранение решающих правил (сигнатур), сканируемых объектов ИТ-инфраструктуры и настроек подключения с использованием системы управления реляционными базами данных; 3. СКАЗ должна реализовывать обновление базы данных уязвимостей; 4. СКАЗ должна поддерживать и иметь возможность проверки сетевого туннеля в безагентном режиме сканирования, с использованием привилегированных учетных записей и соответствующих стандартизованных протоколов. |
|  | Модуль (система) мониторинга событий информационной безопасности (СМСИБ) | 1. Система мониторинга событий информационной безопасности должна включать:  * программный комплекс мониторинга событий информационной безопасности производительностью не менее 30 000 событий в секунду, обеспечивающий единовременную работу с источниками событий информационной безопасности в объеме не менее 500 шт.;  1. Срок действия простой (неисключительной) лицензии на использование программного комплекса: не менее 60 месяцев; 2. Программный комплекс системы мониторинга событий информационной безопасности должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. Подрядчик должен обеспечить разработку не менее 30 специфичных правил корреляции событий; 4. СМСИБ должна обеспечивать решение следующих общих задач:  * сбор, обработка, отображение и долгосрочное хранение информации о событиях и подозрениях на инциденты информационной безопасности, выявляемых в инфраструктуре Заказчика; * предоставление инструментов для анализа событий и расследования инцидентов информационной безопасности; * предоставление исходной информации для определения влияния события или подозрения на инцидент информационной безопасности (ИБ) на сервисы Заказчика.  1. СМСИБ должна представлять собой единую систему с иерархической функциональной структурой и централизованным пунктом управления; 2. СМСИБ должна включать следующие функциональные подсистемы:  * подсистема сбора и обработки событий ИБ; * подсистема хранения событий ИБ; * подсистема корреляции событий ИБ; * подсистема поиска событий и подозрений на инциденты ИБ; * подсистема регистрации инцидентов; * подсистема обеспечения ИБ самой системы; * подсистемы управления.  1. СМСИБ должна обеспечить выполнение следующих функций:  * консолидация и хранение информации о инцидентах ИБ, регистрируемых СМСИБ с целью выявления подозрений на инциденты ИБ; * анализ информации о подозрениях на инциденты ИБ с целью их подтверждения и назначения для последующего реагирования; * сбор и систематизация данных для проведения специалистами по ИБ последующего анализа причин и источников инцидентов информационной безопасности для определения корректирующих действий по снижению вероятности наступления аналогичных инцидентов информационной безопасности в будущем; * обобщенное представление информации о выявленных подозрениях на инциденты ИБ на единой консоли; * уведомление ответственных сотрудников ИБ об обнаружении инцидентов (подозрений на инцидент); * администрирование; * мониторинг состояния, устранение сбоев и отказов программного обеспечения.  1. Требования к функциональным подсистемам СМСИБ:    1. Подсистема сбора и обработки событий ИБ должна обеспечивать реализацию следующего набора типовых действий:  * автоматизированный сбор и нормализация событий ИБ, включая:   + присвоение событиям категорий в соответствии с типом зарегистрированного события;   + присвоение событию степени критичности;   + приведение событий ИБ к единому формату;   + сохранение исходного события и нормализованного;   + нормализация объединенного потока событий от различных источников;   + передача информации о событиях ИБ и сетевых потоках в подсистему управления инцидентами ИБ, подсистему хранения событий ИБ. * поддержка передачи событий в другие системы; * события должны содержать как минимум следующую информацию:   + дата и время возникновения события;   + источник (адрес или хост);   + уникальный идентификатор события;   + тип (категория) события;   + описание события;   + критичность (приоритет) события;   + время получения события от источника.   1. Подсистема хранения событий ИБ должна быть реализована в виде единого распределенного хранилища и обеспечивать реализацию следующего набора типовых действий: * долгосрочное хранение событий ИБ как в нормализованном, так и в исходном виде; * хранение событий ИБ в сжатом виде для экономии объема требуемого места в хранилище; * адаптация системы хранения событий ИБ под разные часовые пояса (отображение всех событий в едином временном пространстве); * распределенное хранение событий без консолидации в единое хранилище с возможностью оперативного доступа ко всем событиям из единой консоли; * возможность распределенного поиска по всем событиям в едином запросе без передачи события в единое хранилище; * долгосрочное хранение событий с оперативным доступом к любым событиям на всем интервале хранения; * сокращение объемов хранения за счет автоматической очистки несущественных и информационных данных на основе заданной и управляемой администраторами критичности событий; * автоматическая очистка хранилища от неинформативных событий; * возможность раздельной установки глубины хранения пользователем для важных и информативных событий.   1. Подсистема корреляции событий должна обеспечивать: * агрегацию инцидентов. Агрегация должна осуществляться при совпадении значений любых заданных администратором полей событий. При регистрации большого количества однотипных событий, превышающего количественные значения правила корреляции, должен быть создан только один инцидент; * функционал поведенческого анализа, осуществляющий сбор количественной статистики по значениям различных полей событий и генерацию инцидентов при обнаружении отклонений от собранной статистики; * функционал отслеживания аутентификации, предоставляющий возможность генерации инцидентов при входе любого пользователя в любую систему-источник с IP-адреса, вход с которого ранее не осуществлялся данным пользователем, либо на хост, вход на который ранее не осуществлялся данным пользователем.   1. Подсистема корреляции событий ИБ должна обеспечивать реализацию следующего набора типовых действий: * выявление подозрений на инциденты ИБ посредством корреляции событий ИБ по заданным правилам. В базовом функционале должны выявляться подозрения на следующие инциденты, включая, но не ограничиваясь:   + превышение числа указанного числа попыток неуспешного доступа;   + успешных вход под учетной записью после многочисленных неуспешных попыток;   + попытки подбора пароля к сервисам удаленного управления серверов и сетевого оборудования, а также для критичных учетных записей;   + блокирование учетной записи после многочисленных неуспешных попыток;   + блокирование критичной (сервисной) учетной записи по превышению лимита неудачных входов;   + интерактивный вход под служебной (сервисной) учетной записью;   + попытки входа под несуществующей учетной записью;   + попытки входа под заблокированной учетной записью;   + удаленный (интерактивный) вход на критичные ресурсы под учетными записями, не перечисленными в указанном списке   + изменение или создание учетных записей пользователями, не входящими в доверенную группу;   + изменение учетных записей и групп вне рабочего времени;   + изменение сервисных учетных записей;   + вход с использованием привилегированных или сервисных учетных записей, в том числе в нерабочие часы;   + массовое изменение учетных записей и групп;   + включение опции Password Never Expires;   + очистка журналов событий;   + превышение допустимого числа запрещенных межсетевым экраном соединений;   + превышение допустимого числа сброшенных соединений;   + превышение допустимого числа неустановленных соединений;   + многочисленные ошибки доступа к источнику (нет прав доступа);   + ошибка загрузки и применения обновлений;   + запуск службы или приложений под привилегированными учетными записями. * создание и корректировка правил корреляции событий ИБ в графическом конструкторе без знания языков программирования; * установка приоритета инцидента, регистрируемого в результате срабатывания правила корреляции; * установки зоны видимости инцидента на основе ролевой модели применительно к каждому правилу корреляции; * возможность использования в правилах корреляции внешних изменяемых пользователем списков; * установка временных ограничительных параметров срабатывания правила корреляции; * автоматическая регистрация выявленных подозрений на инциденты ИБ, оповещение об их выявлении ответственных лиц и передача их в подсистему хранения; * создание новых правил корреляции событий ИБ на основе выбранной группы событий или отдельных событий; * приоритезация выявленных подозрений на инциденты ИБ с учетом критичности событий ИБ, вызвавших данный инцидент и критичности ресурсов, затронутых им; * проактивные сценарии при срабатывании правила корреляции; * передача в проактивные сценарии одиночных значений или массивов имен пользователей, исходных IP адресов, прочих переменных, фигурирующих в инциденте; * отправка уведомления о регистрации инцидента по электронной почте сотрудникам, не имеющих доступа к системе.   1. Подсистема корреляции событий ИБ должна обеспечивать корреляцию: * по отдельным событиям; * по количеству событий за интервал времени; * по последовательности действий.   1. Подсистема поиска событий и подозрений на инциденты ИБ должна обеспечивать реализацию следующего набора типовых действий: * формирование графических представлений и визуализаций данных в событиях; * сортировка и группировка событий; * отображение нормализованных событий с выводом указанной последовательности и набора полей; * изменение очередности и количества выводимых полей при детальном просмотре событий; * создание сохраненных фильтров просмотра событий пользователями и администраторами; * использование составных поисковых запросов; * поиск событий без знания текста события, по категориям и критериям; * возможность использования логических операторов и операторов сравнения (AND, OR, NOT ,=); * выгрузка событий по фильтрам с указанными полями и их очередностью; * гибкое формирование отчетов по событиям и подозрениям на инциденты ИБ на базе поисковых запросов; * поиск событий ИБ, связанных с конкретным подозрением на инцидент ИБ; * сортировка событий по каждому из возможных полей; * сортировка уязвимостей по различным критериям, в т.ч. по критичности.   1. Подсистема регистрации инцидентов безопасности СМСИБ должна быть выполнена в виде единого решения с остальными подсистемами в единой консоли управления и обеспечивать реализацию следующих типовых действий: * ведение процессов инцидент-менеджмента согласно стандарту ITIL; * регистрация инцидентов в результате срабатывания по правилам корреляции; * ролевое разделение доступа к инцидентам; * разделение доступа по группам и пользователям системы на основе условий, задаваемых в правилах корреляции; * постановка задач сотрудникам и группам в рамках инцидентов; * оповещение посредством электронной почты о назначенных инцидентах; * оповещение посредством электронной почты о поставленных задачах в рамках инцидентов; * постановка задач сотрудникам, не имеющим доступа к инциденту с изменением зоны видимости инцидента; * эскалация инцидентов с изменением зоны видимости инцидентов; * поиск и навигация по событиям, попавшим под инцидент; * повторное открытие ранее закрытого инцидента при его повторном возникновении; * навигация по закрытым инцидентам; * просмотр решения инцидентов.   1. Подсистема информационной безопасности должна обеспечивать реализацию следующих типовых действий: * аутентификация пользователей посредством встроенных механизмов; * разграничение доступа к функциям и информации, обрабатываемой посредством ролевой модели; * логирование входов и действий обслуживающего персонала; * защита от несанкционированного доступа к обрабатываемой информации; * регистрация и предотвращение попыток несанкционированного доступа к средствам контроля и контролируемой информации.   1. Управление осуществляется посредством графического веб-интерфейса, обеспечивающего:   отображение текущего состояния всех компонентов системы;  создание и формирование отчеты с возможностью визуализации данных с помощью таблиц и диаграмм;  готовые пакеты панелей визуализации;  возможность управления настройками и правилами корреляции на всех серверах из единой консоли.   1. Источники событий должны интегрироваться с СМСИБ одним из следующих способов:  * использование унифицированных (на базе IP) процедур (протоколы syslog, RPC или др.) для реализации информационного обмена средств источников событий со средствами СМСИБ; * использование специализированных коллекторов, осуществляющих:   + сбор событий по протоколу syslog, netflow;   + сбор событий, хранящихся в лог-файлах локально и на сетевых ресурсах;   + сбор событий, хранящихся в журналах Windows Event Log;   + сбор событий, хранящихся в БД;   + сбор информации об установленном ПО и патчах на ОС Windows;   + сбор событий посредством проприетарных протоколов, используемых соответствующими источниками.   1. При передаче событий должна обеспечиваться их целостность и гарантированная доставка в хранилище;   2. В случае избыточной нагрузки, СМСИБ должна уметь буферизовать поступающий поток во избежание потерь событий и распределения оптимальной нагрузки;   3. Для источников событий, которые не могут быть интегрированы в СМСИБ на основании типовых (унифицированных) решений, проблемы обеспечения информационно-технического взаимодействия должны решаться в каждом конкретном случае отдельно при взаимодействии и по согласованию с Заказчиком.   4. СМСИБ должна содержать инструментарий подключения новых источников событий, доступный через интерфейс пользователя. |
|  | Модуль (система) контроля привилегированных пользователей (СКПП) | 1. Система контроля привилегированных пользователей должна включать:  * программный комплекс контроля привилегированных пользователей с лицензией на 50 конкурентных сессий без ограничения по количеству пользователей и серверов, к которым осуществляется доступ.  1. Срок действия простой (неисключительной) лицензии на использование программного комплекса: не менее 60 месяцев; 2. Программный комплекс контроля привилегированных пользователей должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СКПП должна иметь действующий сертификат ФСТЭК России, подтверждающий соответствие:  * требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4-го.  1. СКПП должна обеспечивать работу в отказоустойчивом режиме; 2. СКПП должна работать в режиме шлюза (прокси-сервера) без установки агентов на серверы и рабочие станции; 3. СКПП должна обеспечивать мониторинг и регистрацию действий пользователей на целевых системах; 4. СКПП должна поддерживать следующие протоколы:  * RDP; * SSH; * Telnet; * SFTP;  1. СКПП должна обеспечивать:  * функционал просмотра завершенной сессии с возможностью текстового поиска; * функционал просмотра в режиме реального времени активной сессии с возможностью ее прерывания; * функционал просмотра видеозаписи сессии с возможностью быстрого поиска фрагмента видеозаписи; * функционал создания политик (правил), определяющих, следует ли разрешить (запретить) пользователю установить сессию, следует ли записать сессию пользователя; * возможность контроля и управления направлением передачи информации через буфер обмена (протокола RDP); * функционал предоставления доступа к целевым системам по расписанию; * предоставление доступа привилегированному пользователю к целевым системам через веб-портал; * встроенные средства мониторинга основных показателей своей работы, в том числе с показом показателей в табличном или графическом виде за последние несколько часов работы и оповещение о возникновении ошибок и нештатных ситуаций в работе сервисов; * функционал ведения журнала аудита доступа с возможностью выгрузки журнала; * возможность создания списков запрещенных и разрешенных команд передаваемых команд в текстовых протоколах ( SSH , Telnet); |
|  | Модуль (средство) доверенной загрузки (СДЗ) | 1. Средство доверенной загрузки должно включать:  * Программно-аппаратный комплекс, обеспечивающий доверенную загрузку АРМ в количестве не менее 4 шт.; * Персональные идентификаторы, не менее 12 шт.;  1. Срок гарантийных обязательств на СДЗ — не менее 60 (шестидесяти) месяцев; 2. Программные средства СДЗ должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СЗД должно иметь действующий сертификат ФСТЭК России, подтверждающий соответствие требованиям по безопасности информации, установленных в Требованиях к средствам доверенной загрузки (ФСТЭК России, 2013) и Профиле защиты средства доверенной загрузки уровня платы расширения 4 класса защиты или выше; 4. СЗД должно обеспечивать:  * идентификацию и аутентификацию пользователей при их входе в систему с помощью персональных идентификаторов:   + должна быть обеспечена возможность работы нескольких пользователей на одном компьютере;   + пользователю должна быть предоставлена возможность работы на нескольких компьютерах при предъявлении одного и того же персонального идентификатора; * защиту от несанкционированной загрузки операционной системы со съемных носителей информации; * контроль целостности программного и аппаратного обеспечения защищаемого компьютера до загрузки операционной системы:   + файлов и физических секторов жесткого диска;   + элементов системного реестра компьютера;   + журнала транзакций файловых систем;   + PCI-устройств;   + структур SMBIOS. * регистрацию событий, связанных с безопасностью системы в журнале безопасности.  1. СЗД должно быть предназначено для работы на АРМ под управлением ОС Microsoft Windows 10 с интерфейсом PCI Express M.2. |
|  | Модуль (система) резервного копирования (СРК) | 1. Система резервного копирования должна включать:  * программный комплекс средств резервного копирования с возможностью единовременной эксплуатации на серверах в количестве не менее 7 шт.;  1. Срок действия простой (неисключительной) лицензии на использование программных средств: не менее 60 месяцев; 2. Программные средства резервного копирования должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СРК должна иметь возможность резервного копирования и аварийного восстановления данных на компьютерах, работающих под управлением ОС, используемых Подрядчиком на уровне вычислительной инфраструктуры; 4. СРК должна обеспечивать:  * поддержку среды виртуализации, используемой Подрядчиком на уровне вычислительной инфраструктуры; * резервное копирование и аварийное восстановление папок и файлов; * поддержка следующих функции и возможностей резервного копирования:   + создание полных, дифференциальных и инкрементных резервных копий;   + автоматическое удаление устаревших резервных копий;   + сжатие;   + исключение файлов;   + автоматическое или ручное разбиение резервных копий;   + дедупликацию. * поддержка следующих функций и возможностей управления резервными копиями:   + восстановление при загрузке;   + восстановление файлов, сохраняя настройки безопасности;   + копирование отдельных файлов или папок из резервной копии с помощью браузера. * поддержка следующих функций и возможностей управления резервными копиями:   + шаблоны схем резервного копирования;   + Pre и Post команды;   + настраиваемая схема резервного копирования;   + защита резервной копии с помощью пароля;   + условия удаления резервных копий — количество копий, возраст копии;   + создание резервной копии вместе с загрузочными компонентами на съемный загрузочный носитель для возможности аварийного восстановления. * ограничение доступа к управлению резервным копированием и восстановлением данных для пользователя и групп пользователей путем авторизации. |
|  | Модуль (система) защиты среды виртуализации (СЗСВ) | 1. Система защиты среды виртуализации должна включать:  * программный комплекс защиты среды виртуализации для эксплуатации на серверах Тип 2 в количестве не менее 4 шт., с возможностью единовременной эксплуатации на серверах уровня вычислительной инфраструктуры, поставляемых Подрядчиком;  1. Срок действия простой (неисключительной) лицензии на использование программных средств: не менее 60 месяцев; 2. Программные средства системы защиты среды виртуализации должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных; 3. СЗСВ должно иметь действующий сертификат ФСТЭК России, подтверждающий соответствие:  * требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — не ниже 5 класса защищенности или требованиям, указанным в технических условиях (заданиях безопасности); * требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4-го.  1. СЗСВ должно обеспечивать:  * аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности:   + реализация модели разделения прав на управление виртуальной инфраструктурой и на управление безопасностью. * защиту средств управления виртуальной инфраструктурой от НСД:   + наличие функционала мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра;   + наличие механизма блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой;   + наличие механизма оповещения администратора виртуальной инфраструктуры о том, что действие заблокировано СЗСВ. * защиту гипервизоров от НСД:   + возможность создания списка разрешенных программ;   + возможность контроля разграничения сети управления и сети виртуальных машин;   + возможность настройки параметров логирования виртуальных машин;   + возможность создания списков запрещенных устройств;   + возможность запрета коммуникаций между виртуальными машинами;   + возможность проверки использования стандартных SSL сертификатов;   + возможность создания списка пользователей, которым разрешен локальный вход на гипервизор;   + возможность очистки внешней и оперативной памяти при окончании работы с виртуальной машиной;   + возможность ограничения доступа к конфигурационным файлам служб;   + возможность контроля использования протокола SSH;   + возможность запрета операций с буфером обмена для каждой виртуальной машины;   + возможность создания парольных политик;   + возможность отключения неиспользуемых протоколов, портов и функций;   + возможность настройки безопасности виртуального коммутатора;   + возможность настройки синхронизации времени;   + возможность на запрет доступа консоли виртуальной машины. * контроль целостности конфигурации виртуальных машин и их доверенную загрузку:   + контроль целостности настроек виртуальной машины перед ее загрузкой;   + контроль образа BIOS виртуальной машины;   + доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска. * мандатный принцип контроля доступа; * регистрацию событий, связанных с информационной безопасностью;  1. СЗСВ должно иметь возможность отключения механизмов защиты в аварийных ситуациях; 2. СЗСВ должно иметь возможность экспорта\импорта настроек конфигурации. |

**Приложение Б**

**Структурная схема АПК «ВИФИД»**



**Приложение В**

**Форма Сублицензионного договора**

**Сублицензионный договор № \_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| г. Москва | «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2020 г. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (наименование получателя), именуемый в дальнейшем «Сублицензиат», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Лицензиат», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_, с другой стороны, именуемые вместе «Стороны», заключили настоящий Договор о нижеследующем:

**1. Предмет Договора**

1.1. По настоящему Договору Лицензиат (Лицензионный договор от »\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_) в рамках Договора от »\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_ обязуется предоставить Сублицензиату право использования программного обеспечения — простую (неисключительную) лицензию (далее также — программное обеспечение, программа для ЭВМ). Перечень программного обеспечения, право использования которого предоставляется по настоящему Договору, установлены в Приложении № 1 к настоящему Договору. Территория действия простой (неисключительной) лицензии, передаваемой по настоящему Договору, ограничена пределами Российской Федерации. Программное обеспечение передается на материальном носителе или по электронным каналам связи с ключами, кодами и иными сведениями, необходимыми для использования программного обеспечения.

1.2. Содержание права использования программного обеспечения, предоставляемого по настоящему Договору Сублицензиату, определено пунктами 1.2.1-1.2.2 настоящего Договора. По настоящему Договору Лицензиат передает Сублицензиату следующие правомочия в отношении программного обеспечения:

* + 1. право на воспроизведение программного обеспечения, ограниченное установкой (инсталляцией) и запуском данного программного обеспечения на ЭВМ (электронно-вычислительной машине) в соответствии с типовым лицензионным соглашением с конечным пользователем, и использование функционала программного обеспечения в соответствии с его прямым назначением. При этом:

- лицензионное соглашение с конечным пользователем — соглашение, декларируемое правообладателем программы для ЭВМ в одностороннем порядке и принимаемое конечным пользователем в момент начала использования программы для ЭВМ способом, предусмотренным правообладателем программы для ЭВМ. Лицензионное соглашение с конечным пользователем включено в программу для ЭВМ (появляется при инсталляции) и (или) опубликовано на официальном сайте соответствующего правообладателя и (или) передается Сублицензиату в виде отдельного документа;

- конечный пользователь обязуется самостоятельно ознакомиться с типовым лицензионным соглашением Правообладателя и несет риск последствий не ознакомления с ним.

* + 1. право на изготовление копии программного обеспечения при условии, что эта копия предназначена только для архивных целей или для восстановления работоспособности программного обеспечения. При этом копия программного обеспечения не может быть использована в иных целях.
  1. Сублицензиату предоставляются все права использования программного обеспечения, которые указаны в настоящем Договоре. Сублицензиату также принадлежат права, предусмотренные ст. 1280 Гражданского кодекса Российской Федерации. Лицензиат гарантирует Сублицензиату возможность беспрепятственного использования этих прав.
  2. Сублицензиат обязуется в течение 2 (двух) рабочих дней со дня получения от Лицензиата соответствующего запроса предоставлять Лицензиату письменные отчеты об использовании программного обеспечения.
  3. Сублицензиат является конечным пользователем программного обеспечения и не имеет права передавать каким-либо способом программное обеспечение, права на его использование иным лицам.
  4. Лицензиат подтверждает и гарантирует, что он действует в пределах прав и полномочий, установленных правообладателем программного обеспечения, и на момент предоставления Сублицензиату прав на программное обеспечение он является их законным и правомерным обладателем, а указанные права не заложены, не арестованы, не являются предметом претензий и исков третьих лиц.
  5. Ни одно из положений настоящего Договора не является и не может рассматриваться как отчуждение исключительных прав на интеллектуальную собственность (интеллектуальные права) правообладателя и (или) лицензиара.
  6. Сублицензиат соглашается и обязуется не осуществлять следующие действия:
     1. Использовать программное обеспечение или соответствующую документацию к нему в каких-либо иных целях, кроме тех, что разрешены настоящим Договором, в том числе передавать программное обеспечение, права на него на возмездной и безвозмездной основе третьим лицам (если такая передача не предусмотрена настоящим Договором), сдавать в пользование, распространять (тиражировать) программное обеспечение с целью получения коммерческой выгоды.
     2. Модифицировать программное обеспечение и производить его обратное проектирование, под которым подразумевается декомпилирование программного обеспечения с целью определения структуры, конструкции, концепции и методологии программного обеспечения для включения последних в какой-либо разрабатываемый конечным пользователем или третьим лицом программный продукт или для каких-либо иных целей.
     3. Осуществлять действия по обходу технических средств защиты, встроенных в программное обеспечение, адаптировать, вносить изменения в исходный код, восстанавливать исходный код программного обеспечения, за исключением случаев, явно определенных в правом пользования в соответствии с действующим законодательством Российской Федерации.
  7. В случае, когда передача прав на программное обеспечение сопровождается передачей сопроводительной документации или дополнительной информации, Лицензиат осуществляет передачу такой документации и информации по каналам электронной связи или иным способом, согласованным Сторонами. В случае если Стороны договорились о передаче документации или информации, или копий программного обеспечения на материальных носителях, Лицензиат за свой счет организует передачу таких материальных носителей Сублицензиату, если Стороны не оговорили иной порядок (например, передачу материальных носителей в месте, обозначенном Лицензиатом).

**2. Условия предоставления простых (неисключительных) лицензий**

2.1. Лицензиат (согласно Договору от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_) предоставляет Сублицензиату простые (неисключительные) лицензии на использование программного обеспечения в течение срока, установленного Договором от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_.

2.2. Простые (неисключительные) лицензии считаются предоставленными с момента подписания Лицензиатом и Сублицензиатом Акта приема-передачи прав использования программного обеспечения (далее — Акт приема-передачи прав).

2.3. Сторона настоящего Договора вправе мотивированно отказаться от подписания Акта приема-передачи прав по настоящему Договору с направлением соответствующего письменного уведомления в адрес другой Стороны в случае если представленный для подписания Акт приема-передачи прав не соответствует по наименованиям, количеству и объему передаваемых прав условиям настоящего Договора, в том числе Приложению №1 (Спецификация прав использования программного обеспечения).

1. **Цена Договора**
   1. Стоимость предоставляемых прав по настоящему Договору, под которой Сторонами понимается вознаграждение Лицензиата за предоставляемое Сублицензиату право использования программного обеспечения, включена в стоимость поставляемого программного обеспечения по Договору от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_ и уплачивается Лицензиату Заказчиком. В соответствии с пп. 26 п. 2 ст. 149 НК РФ предоставление прав на использование программ для ЭВМ не подлежит обложению НДС.

**4. Срок действия предоставляемых прав**

4.1. Срок действия прав на использование программного обеспечения составляет не менее 60 месяцев и указан в Приложении № 1 к Договору.

**5. Ответственность Сторон**

5.1. За неисполнение или ненадлежащее исполнение своих обязательств по настоящему Договору Стороны несут гражданско-правовую ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. В случае предъявления к Сублицензиату третьими лицами претензий или исков, связанных с предоставляемыми по настоящему Договору правами, Сублицензиат, при условии что такие претензии или иски не связаны с нарушением последним предоставляемых по настоящему Договору прав, вправе потребовать от Лицензиата возмещения всех убытков, причиненных в связи с несоблюдением Лицензиатом гарантий, указанных в пункте 1.3 настоящего Договора или в связи с любыми иными обстоятельствами, возникшими по вине Лицензиата и послужившими основаниями для беспрепятственного использования Сублицензитом предоставленных ему по настоящему Договору прав, а Лицензиат обязуется самостоятельно и без участия Сублицензиата урегулировать все такие возможные претензии и (или) иски третьих лиц, а также возместить Сублицензиату все причиненные в связи с такими претензиями и или исками убытки в полном объеме (включая, но не ограничиваясь, расходы на оплату вознаграждения адвокатов, расходы на оплату любых сумм в пользу третьих лиц на основании решения суда и иные расходы любого характера).

Лицензиат не несет ответственности и не возмещает убытки за проблемы, возникающие в процессе использования программного обеспечения (проблемы совместимости с другими программными продуктами (пакетами, драйверами и др.), проблемы, возникающие из-за неоднозначного толкования сопроводительной документации, несоответствия результатов использования программного обеспечения ожиданиям конечного пользователя и т.п.). За все возможные негативные последствия, вызванные несовместимостью или конфликтами программного обеспечения с другими программными продуктами, установленными на ЭВМ конечного пользователя, полную ответственность несет конечный пользователь.

Конечный пользователь обязуется соблюдать все авторские права, лицензионные соглашения и установленные ограничения.

**6. Изменение и расторжение настоящего Договора**

6.1. Любые изменения и дополнения, вносимые в настоящий Договор, оформляются дополнительными соглашениями, подписываемыми Лицензиатом и Сублицензиатом, и являющимися его неотъемлемыми частями.

6.2. Настоящий Договор может быть расторгнут по основаниям и в порядке, установленным действующим законодательством. Любые изменения и (или) дополнения к настоящему Договору действительны только в том случае, если они совершены в письменной форме и подписаны уполномоченными представителями обеих Сторон.

6.3. Стороны обязуются в течение 3 (трех) календарных дней с момента изменения уведомлять друг друга об изменении своих реквизитов (адреса местонахождения, банковских реквизитов, телефонных номеров и пр.). В противном случае документы (либо иная информация), переданные по указанным в настоящем Договоре реквизитам, считаются полученными (т.е. надлежащим образом переданными).

1. **Порядок разрешения споров**
   1. Все споры и разногласия, возникшие в связи с исполнением настоящего Договора, его изменением, расторжением или признанием недействительным, Стороны будут стремиться решить путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями.
   2. В случае недостижения взаимного согласия, споры по настоящему Договору разрешаются в Арбитражном суде города Москвы с соблюдением претензионного порядка разрешения спора со сроком ответа на претензию — 10 (десять) дней.

**8. Прочие условия**

8.1. Настоящий Договор заключен на срок предоставления прав, указанный в пункте 4.1 настоящего Договора.

8.2. Все вопросы, не урегулированные в настоящем Договоре, разрешаются в соответствии с действующим законодательством Российской Федерации.

8.3. Настоящий Договор составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

8.4. К настоящему Договору прилагается и является его неотъемлемой частью:

Приложение 1 — Спецификация прав использования программного обеспечения;

Приложение 2 — Форма Акта приема-передачи прав использования программного обеспечения.

1. **Подписи Сторон**

|  |  |
| --- | --- |
| **Сублицензиат:** | **Лицензиат:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_)**  М.П. | **\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_)**  М.П. |

Приложение № 1

к Договору № от

**СПЕЦИФИКАЦИЯ**

**Перечень программного обеспечения,**

**право использования которого предоставляется по Договору**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Срок действия предоставляемых прав** | **Объем, кол-во, (ед.)** | **Цена, (руб.)** | **Сумма, (руб.)** |
| **1.** |  |  |  |  |  |
| **2.** |  |  |  |  |  |
| **3.** |  |  |  |  |  |
| **…** |  |  |  |  |  |
| **ИТОГО** | | | | |  |

|  |  |
| --- | --- |
| **Сублицензиат:** | **Лицензиат:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_)**  М.П. | **\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_)**  М.П. |

Приложение № 2

к Договору № от

**АКТ**

**ПРИЕМА — ПЕРЕДАЧИ ПРАВ НА ИСПОЛЬЗОВАНИЕ**

**ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

город \_\_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в лице \_\_\_\_\_\_\_\_\_\_\_ действующего на основании Устава, именуемый в дальнейшем «Лицензиат», с одной стороны и

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующий на основании \_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, именуемый в дальнейшем «Сублицензиат», вместе именуемые Стороны, составили и подписали настоящий Акт о приеме-передаче права на использование программного обеспечения (именуемый в дальнейшем — Акт) к Сублицензионному договору № \_\_\_\_ от «\_\_» \_\_\_\_\_ 202 г. (именуемый в дальнейшем — Договор) о нижеследующем:

В соответствии условиям Договора Лицензиат передал, а Сублицензиат принял права на использование следующего программного обеспечения:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование программного обеспечения** | **Кол-во, (шт)** | **Цена, (руб.)** | **Сумма, (руб.)** | **Срок использования** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |
| **ИТОГО** | |  |  |  |  |

Права предоставлены Лицензиатом согласно условиям Договора в полном объеме и в установленный Договором срок.

Предоставленные права приняты Сублицензиатом в полном объеме.

Каких-либо претензий по объему, наименованию, срокам предоставления права на использование программного обеспечения, Сублицензиат к Лицензиату не имеет.

Акт составлен на русском языке в 2-х (двух) подлинных идентичных экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

|  |  |
| --- | --- |
| Лицензиат: | Сублицензиат: |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| М.П. | М.П. |