_____№_____

УТВЕРЖДАЮ
И.о. Заместителя Генерального директора по техническому обеспечению и качеству-технического директора

_____Е.Г. Скорынин

«___»_____2022г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ОКАЗАНИЕ УСЛУГ

Предмет закупки: Оказание услуги по проведению аттестации рабочего места, подключенного к ФИС ФРДО.

Новоуральск
2022

23.08.2022 12-49/4746-УД

Подписан
простой электронной подписью

Техническое задание на оказание услуг

СОДЕРЖАНИЕ

РАЗДЕЛ 1. НАИМЕНОВАНИЕ ПРЕДМЕТА ЗАКУПКИ

Оказание услуг по проведению аттестации рабочего места, подключенного к ФИС ФРДО (далее по тексту Услуги).

РАЗДЕЛ 2. ОПИСАНИЕ УСЛУГИ

Подраздел 2.1 Состав (перечень) оказываемых услуг

2.1.1 Предоставление неисключительных прав использования программного обеспечения – средств защиты информации, сертифицированных по требованиям информационной безопасности: Secret Net Studio 8 и ViPNet Client 4. x (КС2), сеть 3608 с передачей носителей и комплектом документации (далее – ПО), согласно требованиям, приведенным в приложении № 1 к настоящему Техническому заданию.

2.1.2 Разработка комплекта организационно-распорядительной и технической документации для аттестации рабочего места АО «УЭХК» (далее – Заказчик), подключаемого к ФИС ФРДО. Состав комплекта организационно-распорядительной документации указан в приложении № 2 к настоящему Техническому заданию.

2.1.3 Установка и настройка программного обеспечения и средств защиты информации на рабочем месте Заказчика, подключаемом к ФИС ФРДО (далее – рабочее место).

2.1.4 Аттестационные испытания рабочего места Заказчика по требованиям безопасности информации с выдачей аттестата соответствия требованиям безопасности информации на ИСПДн.

2.1.5 Техническое сопровождение программного обеспечения ViPNet Client 4.x (КС2) сроком на 1 год с предоставлением сертификата активации сервиса прямой технической поддержки.

Подраздел 2.2 Описание оказываемых услуг

2.2.1 Этап 1: Исполнитель предоставляет Заказчику:

- неисключительное право использования Secret Net Studio 8 на один год;
- сертификат активации сервиса прямой технической поддержки ПО ViPNet сеть 3608.

2.2.2 Этап 2: Исполнитель устанавливает и настраивает программное обеспечения и средства защиты информации на рабочем месте Заказчика. Исполнитель совместно с Заказчиком проводит приемо-сдаточные испытания подключения рабочего места Заказчика с оформлением акта готовности рабочего места Заказчика.

2.2.3 Этап 3: Исполнитель . разрабатывает и согласовывает с Заказчиком проекты организационно-распорядительной документации для аттестации рабочего места Заказчика в соответствии с приложением 2 к техническому заданию;

2.2.4 Этап 4: Исполнитель проводит аттестационные испытания ИСПДн и аттестацию объекта информатизации – рабочего места Заказчика.

2.2.5 Этап 5: Исполнитель обеспечивает техническую поддержку установленного программного обеспечения с предоставлением сертификата активации сервиса прямой технической поддержки (по п.2.2.2) и оказывает консультационные услуги по вопросам взаимодействия Заказчика с ФИС ФРДО.

2.2.6 Все услуги по установке, настройке СЗИ, а также по вводу в эксплуатацию СЗПДн ИСПДн производятся с обязательным выездом Исполнителя на объект Заказчика.

Подраздел 2.3 Объем оказываемых услуг, либо доля оказываемых услуг в общем объеме закупки

№	Описание	Единица измерения	Кол-во	
1.	Неисключительное право использования модулей средства	лицензия	1	

	защиты информации Secret Net Studio 8 для MS Windows, лицензия на 12 месяцев.		
2.	Проектная документация	комплект	1
3.	Установка средств защиты информации на рабочем месте Заказчика	рабочее место	1
4.	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client 4.x(КС2, ViPNet-сеть 3608) уровень – расширенный на 12 месяцев	штука	1
5.	Аттестация с выдачей аттестата соответствия по требованиям информационной безопасности	аттестат	1
6.	Носители ПО:		
6.1	Установочный комплект Secret Net Studio 8 для MS Windows с комплектом документации (сертификат соответствия ФСТЭК России, формуляр и др. в печатном виде).	комплект	1
6.2	Дистрибутив ViPNet Client 4.x актуальная версия (КС2, ViPNet-сеть 3608) для MS Windows с комплектом документации (сертификат соответствия ФСТЭК России, формуляр и др. в печатном виде).	комплект	1

Изготовителем ПО Secret Net Studio 8 является ООО «Код безопасности». Изготовителем ПО ViPNet Client 4.x является ООО «ИнфоТеКС». Предоставление права использования аналогов ПО Secret Net Studio 8 и технической поддержки ПО ViPNet Client 4.x не допускается на основании пункта а) части 5 статьи 3.2.1 ЕОСЗ, так как приобретаемая продукция будет взаимодействовать с ПО ViPNet Client 4.x на аттестованном по требованиям безопасности АРМ АО «УЭХК».

Код	Вид услуги
58.29.50.000	Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение
62.01.11.000	Услуги по проектированию и разработке информационных технологий для прикладных систем
74.90.20.149	Услуги (работы) в области защиты информации прочие
62.02.30.000	Услуги по технической поддержке информационных технологий

РАЗДЕЛ 3. ТРЕБОВАНИЯ К УСЛУГАМ

Подраздел 3.1 Общие требования

3.1.1 Исполнитель оказывает Услуги в объеме, обеспечивающим получение аттестата соответствия по требованиям информационной безопасности для рабочего места Заказчика.

3.1.2 Все услуги по установке, настройке СЗИ, а также по вводу в эксплуатацию СЗПДн ИСПДн производятся с обязательным выездом Исполнителя на объект Заказчика по адресу г. Новоуральск ул.Дзержинского д.4.

3.1.3 Исполнитель самостоятельно и за свой счет, без дальнейшего предъявления затрат Заказчику осуществляет доставку своего персонала и оборудования к месту оказания услуг и обратно.

Подраздел 3.2 Требования к качеству оказываемых услуг
3.2.1 Исполнитель оказывает Услуги с качеством, обеспечивающим полнофункциональное функционирование рабочего места Заказчика, подключенного к ФИС ФРДО и аттестованного по требованиям информационной безопасности. 3.2.2 Услуги должны оказываться с соблюдением требований Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и принятыми в соответствии с ним нормативно-методическими документами, устанавливающими требования к защите персональных данных. 3.2.3 Качество и комплектность СЗИ и ПО должны соответствовать требованиям, предъявляемым к техническим характеристикам товара в стране производителя, а также действующим в РФ стандартам и техническим условиям. Упаковка, в которой поставляется ПО, должна обеспечивать ее сохранность при транспортировке и хранении. Маркировка на упаковке должна соответствовать действующим стандартам. 3.2.4 Все организационно-распорядительные документы, разрабатываемые Исполнителем в процессе оказания услуг, должны соответствовать технологии обработки информации в ИСПДн. 3.2.5 Организационно-распорядительные документы должны создавать условия для обеспечения защиты ПДн от угроз несанкционированного доступа, инсайдерских угроз, угроз хищения носителей информации.
Подраздел 3.3 Требования к гарантийным обязательствам оказываемых услуг
3.3.1 Исполнитель гарантирует полнофункциональное функционирование рабочего места Заказчика, подключенного к ФИС ФРДО в течение 12 календарных месяцев с даты подписания сторонами Акта сдачи-приемки оказанных Услуг.
Подраздел 3.4 Требования к конфиденциальности
3.4.1 При доступе к персональным данным работников Заказчика в период оказания услуг Исполнитель обязан соблюдать конфиденциальность и обеспечивать безопасность персональных данных, с соблюдением требований к их защите в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»..
Подраздел 3.5 Требования к безопасности оказания услуг и безопасности результата оказанных услуг
3.5.1. Исполнитель обязуется выполнять требования Заказчика в области охраны труда, ядерной, радиационной, пожарной безопасности и требования в части допуска и доступа персонала Исполнителя в ЗАТО г. Новоуральск в соответствии с условиями заключенного договора на оказание Услуг.
Подраздел 3.6 Специальные требования
3.6.1 Заказчик вправе передавать сведения, касающиеся оказания Услуг по договору в АО «Гринатом» (ИНН 7706729736) с гарантиями сохранения конфиденциальности и обеспечения режима защиты от несанкционированного доступа на основании соглашения о конфиденциальности между Сублицензиатом и АО «Гринатом», без дополнительного согласования с Правообладателем. 3.6.2 Исполнитель устанавливает и настраивает СЗИ в соответствии с требованиями законодательства по защите информации, а также в соответствии с эксплуатационной документацией на СЗИ.
Подраздел 3.7. Требования к сроку оказания услуг
3.7.1. Услуги оказываются Исполнителем в течение 14 (четырнадцати) календарных месяцев с момента заключения договора, с учетом промежуточных сроков оказания услуг по этапам:

Этап 1: в течение не более 45 календарных дней с даты подписания Договора обеими сторонами.

Этап 2: в течение не более 30 календарных дней с момента завершения оказания Услуг по этапу 1.

Этап 3: в течение не более 60 календарных дней с даты подписания Договора обеими сторонами.

Этап 4: в течение 30 календарных дней с момента завершения оказания Услуг по этапу 3, но не позднее 06.02.2023.

Этап 5: в течение 12 месяцев с момента завершения оказания Услуг по этапу 1.

РАЗДЕЛ 4. РЕЗУЛЬТАТ ОКАЗАННЫХ УСЛУГ

Подраздел 4.1 Описание конечного результата оказанных услуг

4.1.1 Конечным результатом оказания Услуг является:

- по Этапу 1– предоставленные Заказчику неисключительные права на Secret Net Studio 8 и ViPNet Client 4. x (КС2), сеть 3608 и комплект носителей ПО;
- по Этапу 2 – установленное и настроенное ПО, необходимое для подключения рабочего места Заказчика к ФИС ФРДО, утвержденный Заказчиком и Исполнителем акт готовности рабочего места Заказчика, подключенного к ФИС ФРДО;
- по Этапу 3 – утвержденная Заказчиком документация для аттестации рабочего места;
- по Этапу 4 – аттестат соответствия требованиям информационной безопасности рабочего места Заказчика, подключенного к ФИС ФРДО;
- по Этапу 5 - функционирующее у Заказчика рабочее место.

Подраздел 4.2 Требования по приемке услуг

4.2.1 Требования по передаче прав:

1) Исполнитель оформляет и направляет Заказчику Акт приема передачи прав на ПО Secret Net Studio 8 в 2 (двух) экземплярах и носители ПО.

2) Заказчик подписывает Акт приема-передачи прав в течение 5 (пяти) рабочих дней с момента его получения и направляет один подписанный экземпляр Исполнителю.

3) Права использования ПО считаются предоставленными Заказчику с даты подписания обеими Сторонами Акта приема-передачи прав.

4.2.2 Требования по приемке носителей ПО:

1) Исполнитель передает Заказчику Носитель с Сопроводительным документом одним из способов, определенных в подразделе 4.3 Технического задания по адресу 624130, Свердловская обл., г. Новоуральск, ул. Дзержинского, д. 2.

2) Заказчик в течение 5 (пяти) рабочих дней, рассматривает Носитель на соответствие условиям договора:

- в случае соответствия Носителя Заказчик отправляет Исполнителю по факсу Сопроводительный документ, подписанный доверенным представителем Закзачика, с печатью Заказчика с одновременным направлением подлинника Сопроводительного документа Исполнителю под роспись или заказным письмом;
- в случае несоответствия наименования и состава Носителя Заказчик составляет Акт о несоответствии, в котором фиксируются обнаруженные недостатки и направляет его Исполнителю на рассмотрение.

3) Исполнитель в течение 10 (десяти) календарных дней со дня получения Акта согласует с Заказчиком сроки устранения выявленных несоответствий Носителя, либо в указанный срок письменно сообщить о своем несогласии с Актом о несоответствиях.

4) Услуги по передаче Носителя (пункт 5 подраздела 2.3.) считаются принятыми Заказчиком в полном объеме на основании подписанного сторонами Сопроводительного документа.

4.2.3 Требования по сдаче-приемке Услуг.

1) Приемку функционирования рабочего места АО «УЭХК», подключенного к ФИС ФРДО Заказчик проводит проверкой подключения к ФИС ФРДО. Положительный результат – это наличие подключения и вход на портал.

2) После проверки работоспособности и оформления Протокола аттестационных испытаний и Заключения о соответствии Исполнитель оформляет Акт сдачи-приемки оказанных Услуг и направляет Заказчику на рассмотрение.

3) Заказчик, в течение 5 (пяти) рабочих дней, рассматривает и согласовывает представленный Исполнителем Акт сдачи-приемки оказанных Услуг, либо предоставляет мотивированный отказ от приёмки Услуг, с описанием выявленных недостатков.

4) Услуги считаются принятыми Заказчиком в полном объеме на основании подписанного сторонами Акта сдачи-приемки оказанных Услуг.

4.2.4 Требования по передаче сертификата технической поддержки ПО ViPNet:

1) Исполнитель предоставляет Заказчику Сертификат с Сопроводительным документом одним из способов, определенных в разделе 4.3 Технического задания.

2) Заказчик в течение 2 (двух) рабочих дней, рассматривает Сертификат на соответствие условиям договора:

- в случае соответствия Сертификата Заказчик отправляет Исполнителю по факсу Сопроводительный документ, подписанный доверенным представителем Заказчика, с печатью Заказчика с одновременным направлением подлинника Сопроводительного документа Исполнителю под роспись или заказным письмом;

- в случае несоответствия наименования и состава Сертификата Заказчик составляет Акт о несоответствии, в котором фиксируются обнаруженные недостатки и направляет его Исполнителю на рассмотрение.

3) Исполнитель в течение 10 (десяти) календарных дней со дня получения Акта согласует с Заказчиком сроки устранения выявленных несоответствий Сертификата, либо в указанный срок письменно сообщить о своем несогласии с Актом о несоответствиях.

4) Услуги по передаче Сертификата считаются принятыми Заказчиком в полном объеме на основании подписанного сторонами Сопроводительного документа.

Подраздел 4.3 Требования по передаче Заказчику технических и иных документов (оформление результатов оказанных услуг)

4.3.1 Исполнитель и Заказчик согласуют форму Сопроводительного документа и один из способов передачи Носителей ПО, Сертификата технической поддержки ПО ViPNet, Протокола аттестационных испытаний и Заключения о соответствии рабочего места Заказчика:

- либо представителем Исполнителя доверенному представителю Заказчика, при этом датой передачи Сертификата считается дата подписания доверенным представителем Заказчика сопроводительного документа;

- либо организацией связи (курьерской службой, почтовым отправлением), при этом датой поставки считается дата проставления штемпеля (штампа и/или подписи представителя Заказчика) на соответствующей почтовой квитанции.

4.3.2 Право собственности на предоставленные Носители ПО и Сертификат переходит от Исполнителя к Заказчику с даты подписания Сторонами Сопроводительного документа. Риски случайной гибели и/или порчи Носителей ПО и Сертификата переходят к Заказчику с даты предоставления Носителей ПО и Сертификата.

4.3.3 Все документы должны быть выполнены на русском языке и предоставляются Исполнителем Заказчику в печатном виде после исполнения услуг по п.2.1.5. Ксерокопии документов не допускаются.

4.3.4 Право собственности на комплект документов по этапу 3 и аттестат соответствия переходит от Исполнителя к Заказчику с даты согласования и подписания документов Сторонами.

4.3.5 Исполнитель направляет Заказчику следующие документы:

- Акт приема-передачи права использования ПО Secret Net Studio 8 в 2 (двух) экземплярах;
- Сопроводительный документ и Акт приема-передачи Носителей ПО;
- Сопроводительный документ и Акт приема-передачи Сертификата технической поддержки ПО ViPNet;
- Счет (счет-фактура), оформленные в соответствии с требованиями действующего законодательства Российской Федерации.

РАЗДЕЛ 5. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1	АРМ	Автоматизированное рабочее место
2	ИС	Информационная система
3	ИСПДн	Информационная (-ых) система (-х) персональных данных
4	НСД	Несанкционированный доступ к информации
5	ПДн	Персональные данные
6	ПО	Программное обеспечение
7	РФ	Российская Федерация
8	СЗИ	Средство (-а) защиты информации
9	СЗПДн	Система защиты персональных данных
10	ФСТЭК России	Федеральная служба по техническому и экспортному контролю
11	ФИС ФРДО	Федеральная информационная система - Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении

РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

Номер приложения	Наименование приложения
1	Требования к поставляемым ПО и СЗИ
2	Состав комплекта организационно-распорядительной документации

Начальник отдела 50 _____ К.Н. Носырев

Инженер-программист отдела 50 _____ Т.Ю. Островская

Эксперт
(специалист, отвечающий за
экспертизу технической
части заявок участников) _____ Н.В. Белослудцев

СОГЛАСОВАНО:

Заместитель Генерального директора по управлению персоналом	_____	Е.Ю. Рогова
Начальник отдела 39	_____	И.В. Цветков
Начальник отдела 91	_____	Ю.В. Воронцов

Приложение №1

Требования к поставляемым ПО и СЗИ

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
1.	Средство защиты информации от несанкционированного доступа с модулями межсетевого экрана, обнаружения вторжений и антивирусной защиты информации	Средство защиты информации от несанкционированного доступа (далее – НСД) должно осуществлять: – защиту рабочих станций от НСД; – контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; – разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации; – разграничение доступа пользователей к информации; – контроль утечек информации; – регистрацию событий безопасности и аудит. Требования к сертификации и применению в информационных системах: СЗИ должно соответствовать требованиям документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) не ниже 4 класса защиты, «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. Требования к операционной платформе и аппаратной части: – СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы): • Windows 10; • Windows 8/8.1; • Windows 7 SP1. – СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. – Требования к функциональности СЗИ: – СЗИ должно выполнять следующие функции по защите информации: – Контроль входа пользователей в систему и работа пользователей в системе: • проверка пароля пользователя при входе в систему; • поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭЦП, Рутокен Lite,

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ; • возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; • возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); • однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); • возможность блокирования входа в систему локальных пользователей; • возможность блокирования операций вторичного входа в систему в процессе работы пользователей; • возможность блокировки сеанса работы пользователя по истечении интервала неактивности; • возможность управления политикой сложности паролей; • поддержка возможности входа в систему по сертификатам; • возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей. – Избирательное (дискреционное) управление доступом: • возможность назначения прав доступа на файлы, каталоги, принтеры, устройства; • возможность наследования прав доступа для файлов, каталогов и устройств; • возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту. o Полномочное (мандатное) управление доступом: • возможность выбора уровня конфиденциальности сессии для пользователя; • возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам; • возможность изменения количества мандатных меток в системе и их названий; • контроль потоков конфиденциальной информации в системе; • возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP. o Контроль вывода конфиденциальных данных на печать: • возможность ограничить перечень мандатных меток информации для печати на заданном принтере; • теневое копирование информации, выводимой на печать;

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		• автоматическая маркировка документов, выводимых на печать; • управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать: • отдельный вид грифа для каждой мандатной метки; • отдельный вид маркировки для первой страницы документа; • отдельный вид маркировки для последней страницы документа; • вид маркировки для оборота последнего листа; • поддержка функции печати в файл; • поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях. ○ Контроль аппаратной конфигурации компьютера и подключаемых устройств: • Должны контролироваться следующие устройства: • последовательные и параллельные порты; • локальные устройства; • сменные, физические и оптические диски; • программно реализованные диски; • USB-устройства; • PCMCIA-устройства; • EEE1394 (FireWire)- устройства; • устройства, подключаемые по шине Secure Digital. • Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства. • Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации. • Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться. • Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации. • В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя. • При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств. – Контроль сетевых интерфейсов: • Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		• Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя. – Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии Active Scripts. – Список модулей, разрешенных для запуска, должен строиться: • с помощью явного указания модулей; • по информации об установленных на компьютере программах; • по зависимостям исполняемых модулей; • по ярлыкам в главном меню; • по событиям журнала безопасности. – Контроль целостности файлов, каталогов, элементов системного реестра: • Должна быть возможность проведения контроля целостности, в процессе загрузки ОС, в фоновом режиме при работе пользователя. • Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. • Должна быть возможность восстановления исходного состояния контролируемого объекта. • Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. • При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. – Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей. – Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации. – Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. – Функциональный контроль ключевых компонентов системы. – Регистрация событий безопасности в журнале. • Должна быть возможность формирования отчетов по результатам аудита. • Должна быть возможность поиска и фильтрации при работе с данными аудита. – Получение отчета по параметрам системы защиты.

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		Требования к централизованному управлению в доменной сети: СЗИ должно предоставлять следующие возможности по управлению системой: – Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров. – Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты. – Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности. – Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров. – Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер). – Выполнение команд, специфичных для защитных подсистем. – Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера. – Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров. – Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования. – Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз. – Централизованное управление в сложной доменной сети должно функционировать по иерархическому принципу, при этом система должна позволять: • распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов); • посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов). – Создавать отчеты по ресурсам и параметрам защищаемых компьютеров, используемых в системе. Требования к сертификации и применению в информационных системах: СЗИ должны соответствовать требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации.

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – не ниже 5 класса защищенности. Требования к функциональности СЗИ: • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети; • фильтрацию сетевых пакетов; • защиту установленных сетевых соединений; • регистрацию событий безопасности и аудит. Модуль средства обнаружения вторжений должен осуществлять: – обнаружение и предотвращение вторжений; – регистрацию событий безопасности и аудит. Требования к сертификации и применению в информационных системах: СЗИ должно соответствовать требованиям документов: «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011)» не ниже 4 класса защиты, «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2011). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. Требования к функциональности СЗИ: СЗИ должно выполнять следующие функции по защите информации: – Обнаружение и предотвращение вторжений: • Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов. • Сигнатурные механизмы должны обеспечивать проверку HTTP-трафика на наличие заданных конструкций как для входящего, так и для исходящего сетевого трафика. При обнаружении признаков атаки прохождение подозрительных сетевых пакетов должно быть заблокировано. • Эвристические механизмы должны распознавать и фиксировать следующие типы атак:

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		▪ сканирование портов; ▪ подделка ARP (ARP-spoofing); ▪ SYN-флуд; ▪ атаки, направленные на отказ в обслуживании (DoS); ▪ распределенные атаки, направленные на отказ в обслуживании (DDoS). При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера. • Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов. – Функциональный контроль ключевых компонентов системы. – Регистрация событий безопасности в журнале. • Должна быть возможность формирования отчетов по результатам аудита. • Должна быть возможность поиска и фильтрации при работе с данными аудита. Модуль антивирусной защиты информации должен осуществлять: – антивирусную защиту от вредоносного программного обеспечения; – регистрацию событий безопасности и аудит. Требования к сертификации и применению в информационных системах: СЗИ должно соответствовать требованиям документов: «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012)» не ниже 4 класса защиты, «Профиль защиты средств антивирусной защиты типа «А» четвертого класса защиты» ИТ.САВЗ.А4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «Б» четвертого класса защиты» ИТ.САВЗ.Б4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «В» четвертого класса защиты» ИТ.САВЗ.В4.ПЗ (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа «Г» четвертого класса защиты» ИТ.САВЗ.Г4.ПЗ (ФСТЭК России, 2012). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. Требования к функциональности СЗИ: СЗИ должно выполнять следующие функции по защите информации: – Антивирусная защита:

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		• Должна обеспечиваться автоматическая проверка наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа. • Должно обеспечиваться сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию. • Должна быть возможность указать расписание запуска антивирусных проверок с возможностью выбора ежечасного запуска, запуска в заданное время ежедневно, запуска в заданный день недели и время еженедельно или по событиям запуска СЗИ и событию успешного обновления баз. • Профили антивирусного сканирования должны поддерживать настройку следующих параметров: ▪ название и описание; ▪ уровень эвристического анализа; ▪ проверка или пропуск архивов; ▪ пропуск файлов больше заданного размера; ▪ проверка файлов только с заданным перечнем расширений; ▪ действия с обнаруженными вредоносными объектами – лечение, удаление, помещение в карантин; ▪ объекты сканирования, включая возможность указать проверку исполняемых процессов в оперативной памяти, проверку загрузочных секторов, проверку локальных, съемных и сетевых дисков и перечень проверяемых директорий. • Должно обеспечиваться удаление вредоносного программного обеспечения и его блокировка (перемещение в карантин). • Должно обеспечиваться восстановление файлов из карантина по команде администратора. • Должен поддерживаться список файлов и директорий, исключаемых из проверки (белый список). • Должна обеспечиваться возможность обновления баз данных признаков компьютерных вирусов (антивирусных баз), в том числе с доступом к серверу обновлений через прокси-сервер. • Должен обеспечиваться контроль целостности антивирусных баз и защита от их подмены при загрузке с сервера обновлений. • Должна обеспечиваться возможность развертывания зеркала сервера обновлений в локальной сети. • Должна быть реализована возможность обновления антивирусных баз со съемных носителей и по локальной сети, без доступа к серверу обновлений. – Функциональный контроль ключевых компонентов системы. – Регистрация событий безопасности в журнале. • Должна быть возможность формирования отчетов по результатам аудита.

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		• Должна быть возможность поиска и фильтрации при работе с данными аудита. Комплект поставки должен содержать: – Неисключительное право на программное обеспечение средство защиты информации от несанкционированного доступа с модулями межсетевого экрана, обнаружения вторжений и антивирусной защиты информации, сроком действия не менее 1 года.
2.	Дистрибутив средства защиты информации от несанкционированного доступа	Комплект поставки дистрибутива средства защиты информации от несанкционированного доступа должен быть совместим с поставляемым ПО в соответствии с настоящим Техническим заданием и должен включать в себя: - CD в конверте с записанными сертифицированными приложениями; - формуляр; - заверенные копии сертификатов ФСТЭК России.
3.	Средство криптографической защиты информации, реализующее функции клиента	Средство криптографической защиты информации должно быть совместимым с средствами криптографической защиты информации, указанными в технических условиях на подключение информационных систем персональных данных образовательных организаций высшего образования к ИСПДн ЦОД ФБУ «Федеральный центр тестирования». Средство криптографической защиты информации должно функционировать под управлением ОС Microsoft Windows 7 (32/64bit), Windows 8.1 (32/64-разрядная), Windows 10 (32/64-разрядная) и обладать следующими функциями: - защита (конфиденциальность, подлинность и целостность) IP-трафика (приложений, систем управления и служебного трафика ОС), передаваемого между защищаемыми рабочими станциями пользователей посредством шифрования, а также между рабочими станциями; – персонального межсетевого экрана – осуществлять фильтрацию IP-пакетов по заданным правилам зашифрованного и открытого трафиков (списки IP-адресов, протоколы, порты), реализовывать режим инициативных соединений; – поддержка прозрачной работы через устройства статической и динамической NAT/PAT маршрутизации; – зашифрованное взаимодействие между защищаемыми узлами по протоколу TCP/IP на основе заданной политики безопасности и связям; – передача файлов между участниками защищенного взаимодействия с подтверждением доставки без установки дополнительного ПО;

№ п/п	Наименование средств защиты информации	Функциональные характеристики средств защиты информации
		– предоставление дополнительных сервисных функций для оперативного защищенного обмена циркулярными сообщениями, проведения текстовых конференций; –шифрование каждого IP-пакет на симметричном ключе связи с другим клиентом, выработанном в программном обеспечении, реализующем функции управления защищённой сетью; - обеспечение удаленного централизованного обновления адресной и ключевой информации комплекса с контролем прохождения обновления; – взаимодействие с другими рабочими станциями с установленным СПО с использованием технологии «клиент-клиент». ПО должно включать встроенный почтовый клиент с поддержкой квитирования (доставлено, прочитано) и механизмов электронной цифровой подписи. ПО должно соответствовать требованиям ФСБ России к средствам криптографической защиты информации класса не ниже КС2. Поставка должна быть в виде передачи неисключительного права на средство криптографической защиты информации, реализующее функции клиента.
4.	Дистрибутив средства криптографической защиты информации	Комплект поставки дистрибутива сертифицированного средства криптографической защиты информации должен быть совместим с средством криптографической защиты информации, реализующим функции клиента, поставляемым в соответствии с настоящим Техническим заданием, и должен включать в себя: - CD в конверте с записанными сертифицированными приложениями; - формуляр на средство криптографической защиты информации; - заверенные копии сертификатов ФСТЭК России.
5.	Сертификат технического сопровождения средства криптографической защиты информации	Комплект поставки сертификата технического сопровождения сертифицированного средства криптографической защиты информации должен быть совместим со средством криптографической защиты информации, реализующим функции клиента, поставляемым в соответствии с настоящим Техническим заданием, и должен включать в себя: - сертификат прямой расширенной технической поддержки на срок не менее одного года, на количество средств криптографической защиты информации, реализующим функции клиента, поставляемых в рамках настоящего Технического задания.

Начальник отдела 50 _____ К.Н. Носырев

Инженер-программист отдела 50 _____ Т.Ю. Островская

Приложение 2

Состав комплекта организационно-распорядительной документации

1 Модель угроз. Разработка модели угроз производится в соответствие с требованиями ФСТЭК России.

2 Приказ «О создании комиссии по защите персональных данных».

3 Приказ «О защите персональных данных».

4 Перечень лиц, доступ которым к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (приложение к приказу «О защите персональных данных»).

5 Перечень лиц, имеющих право доступа в помещения с элементами ИСПДн (приложение к приказу «О защите персональных данных»).

6 Технический паспорт ИСПДн.

7 Инструкция администратора ИСПДн.

8 Инструкция администратора безопасности ИСПДн.

9 Инструкция пользователя ИСПДн.

10 Инструкция по управлению доступом.

11 Инструкция по защите от воздействия вредоносных программ.

12 Инструкция по порядку обращения с машинными носителями персональных данных.

13 Инструкция о действиях лиц, допущенных к работе в ИСПДн, в случае возникновения нештатных ситуаций.

14 Инструкция о порядке контроля за выполнением мероприятий по обеспечению безопасности персональных данных и работой пользователей в ИСПДн.

15 Инструкция по порядку доступа в режимные помещения.

16 Инструкция по внутреннему контролю в сфере обработки и защиты персональных данных.

17 Инструкция по порядку эксплуатации хранилищ.

18 Инструкция по порядку обращения с криптосредствами, применяемыми в информационных системах персональных данных.

19 Перечень информационных систем персональных данных.

20 Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

21 Формы журналов учета (лиц, допущенных к информационной системе персональных данных ключей от режимных помещений, личных печатей, карт для доступа в режимные помещения, ключей от хранилищ и др.).

Начальник отдела 50 _____ К.Н. Носырев

Инженер-программист отдела 50 _____ Т.Ю. Островская

Подписан
простой электронной подписью