Конфиденциально
Экз. №1

УТВЕРЖДАЮ
Директор
Общество с ограниченной ответственностью Центр защиты информации «Север»

_____ Е.П. Попов

«13» ноября 2020 г.

УТВЕРЖДАЮ
Директор
Государственного бюджетного учреждения Республики Саха (Якутия) «Республиканский центр инфокоммуникационных технологий»

_____ И.А. Макаров

«10» ноября 2020 г.

Регламент подключения новых сегментов Государственная информационная система Централизованная облачная система финансово-хозяйственной деятельности государственных учреждений Республики Саха (Якутия)

На 34 листах

РАЗРАБОТАЛ
Главный специалист отдела информационной безопасности Общество с ограниченной ответственностью Центр защиты информации «Север»

_____ А.А. Иванов

«13» ноября 2020 г.

Якутск
2020

Содержание

Перечень сокращений

Сокращение	Определение
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГИС	Государственная информационная система
ИБ	Информационная безопасность
ИОД	Информация ограниченного доступа
ИС	Информационная система
КЗ	Контролируемая зона
СЗИ	Система защиты информации
СКЗИ	Средства криптографической защиты информации
ООО ЦЗИ «Север»	Общество с ограниченной ответственностью Центр защиты информации «Север»
ЛВС	Локальная вычислительная сеть
МНИ	Машинный носитель информации
НСД	Несанкционированный доступ
ТЗ	Техническое задание на создание системы защиты информации

Аннотация

Настоящие технические условия определяют требования, а также устанавливают порядок подключения рабочих мест пользователей к аттестованным по требованиям безопасности информации информационной системе:

- «Централизованная облачная система финансово-хозяйственной деятельности государственных учреждений Республики Саха (Якутия)».

Технические условия разработаны в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и определяет обязательные технические и организационные требования по обеспечению информационной безопасности при подключении рабочих мест к ИС.

1. Общие сведения

1.1. Наименование системы защиты информации

Полное наименование:

- система защиты информации Централизованная облачная система финансово-хозяйственной деятельности государственных учреждений Республики Саха (Якутия);

Краткое наименование: СЗИ ЦОС ФХД, СЗИ ИС.

1.2. Общие сведения об информационных системах

В ЦОС ФХД обрабатывается конфиденциальная информация с использованием средств автоматизации.

ЦОС ФХД имеют клиент-серверную архитектуру.

На серверах ЦОС ФХД производится обработка и хранение поступающей информации. Правила и ограничения автоматизируемых операций ЦОС ФХД реализованы на серверах. Клиентские рабочие места направляют запросы к серверам, полученные от серверов результаты запросов передаются клиенту и отображаются на клиентском рабочем месте в элементах отображения информации в веб-браузере.

Пользователь ЦОС ФХД через клиентские рабочие места соединяются с сервером, идентифицируется и аутентифицируется в системе в рамках предоставленных прав доступа, обрабатывает информацию по закрепленным за специалистом функциональным задачам.

1.3. Цели, назначение и область использования

СЗИ ИС пользовательского сегмента предназначена для автоматизации деятельности в области управления безопасностью персональных данных и обеспечения конфиденциальности, целостности и доступности информации ограниченного доступа обрабатываемых в ЦОС ФХД от актуальных для пользовательского сегмента угроз безопасности информации, не составляющих государственную тайну в соответствии с требованиями документов:

- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» утвержденного приказом ФСТЭК России от 18.02.2013 № 17 для ГИС класса защищенности – К3;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» утвержденного приказом ФСТЭК России от 18.02.2013 № 21 и «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 01.11.2012 №

1119 для защиты персональных данных при их обработке в информационных системах персональных 3 уровня защищенности.

Цели настоящего документа:

- определение порядка подключения рабочих мест пользователей к аттестованным по требованиям безопасности информации ЦОС ФХД;
- выполнение требований Российского законодательства (в том числе руководящих документов ФСТЭК России и ФСБ России) в области защиты информации.

1.4. Характеристики информационной системы

ЦОС ФХД имеет характеристики, представленные в Таблице №1.1.

Таблица №1

№ п/п	Характеристика	Значение
1.	Класс защищенности пользовательского сегмента ГИС	К3
2.	Уровень защищенности ПДн в пользовательском сегменте ГИС	3
3.	Необходимый класс криптографической защиты	КС1 или выше
4.	Использование удаленного доступа к информационным ресурсам через внешние информационно-телекоммуникационные сети	Удаленный доступ к информационным ресурсам производятся через внешние информационно-телекоммуникационные сети.
5.	Использование технологий беспроводного доступа	Технологии беспроводного доступа не используется
6.	Использование в информационной системе мобильных технических средств	Мобильные технические средства в информационной системе не применяются
7.	Наличие взаимодействия с информационными системами сторонних организаций	Взаимодействует с иными информационными системами
8.	Использование машинных носителей	Машинные носители используются
9.	Наличие подключений к сетям международного информационного обмена	Имеет подключение к сетям международного информационного обмена
10.	Использование средств виртуализации	Средства виртуализации не используются в пользовательском сегменте.

2. Условия подключения клиентов

Для организации защищенного взаимодействия, должны быть выполнены следующие требования:

- создать условия для размещения рабочего места с использованием СКЗИ, в соответствии с разделом IV Инструкции «Об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденную приказом ФАПСИ при Президенте РФ №152 от 13.06.2001 года;
- подготовить рабочее место, оборудованный персональный компьютер с наличием подключения к сети Интернет;
- для подключения новых пользователей, в зависимости от места установки, необходимо приобрести, установить и настроить следующие сертифицированные средства защиты информации: СКЗИ ViPNet Client 4.x (КС1 или выше), антивирус Kaspersky Endpoint Security 11 для Windows, средство защиты информации от несанкционированного доступа Dallas Lock 8.0-K;
- на рабочих местах ИС пользователей должна быть установлена операционная система Microsoft, поддерживаемая разработчиком;
- назначить приказом ответственных лиц из числа сотрудников организаций-пользователей, имеющих доступ в ЦОС ФХД;
- произвести приемочные испытания в соответствии с Программой и методикой приемочных испытаний для ЦОС ФХД;
- обеспечить доступ к содержанию информации ограниченного доступа, хранящегося в ИС, был возможен исключительно для должностных лиц (работников) организаций-пользователей ЦОС ФХД, которым сведения, содержащиеся в информационной системе, необходимы для выполнения служебных (трудовых) обязанностей.

После выполнения вышеуказанных требований администратор безопасности организации принимает решение об уровне предоставления доступа и подключает к соответствующей ЦОС ФХД.

3. Обеспечение безопасности взаимодействия

3.1. Основные требования

Реализация требований, указанных в п.2. настоящего документа, достигается путем применения следующих технических и организационных мер по защите информации:

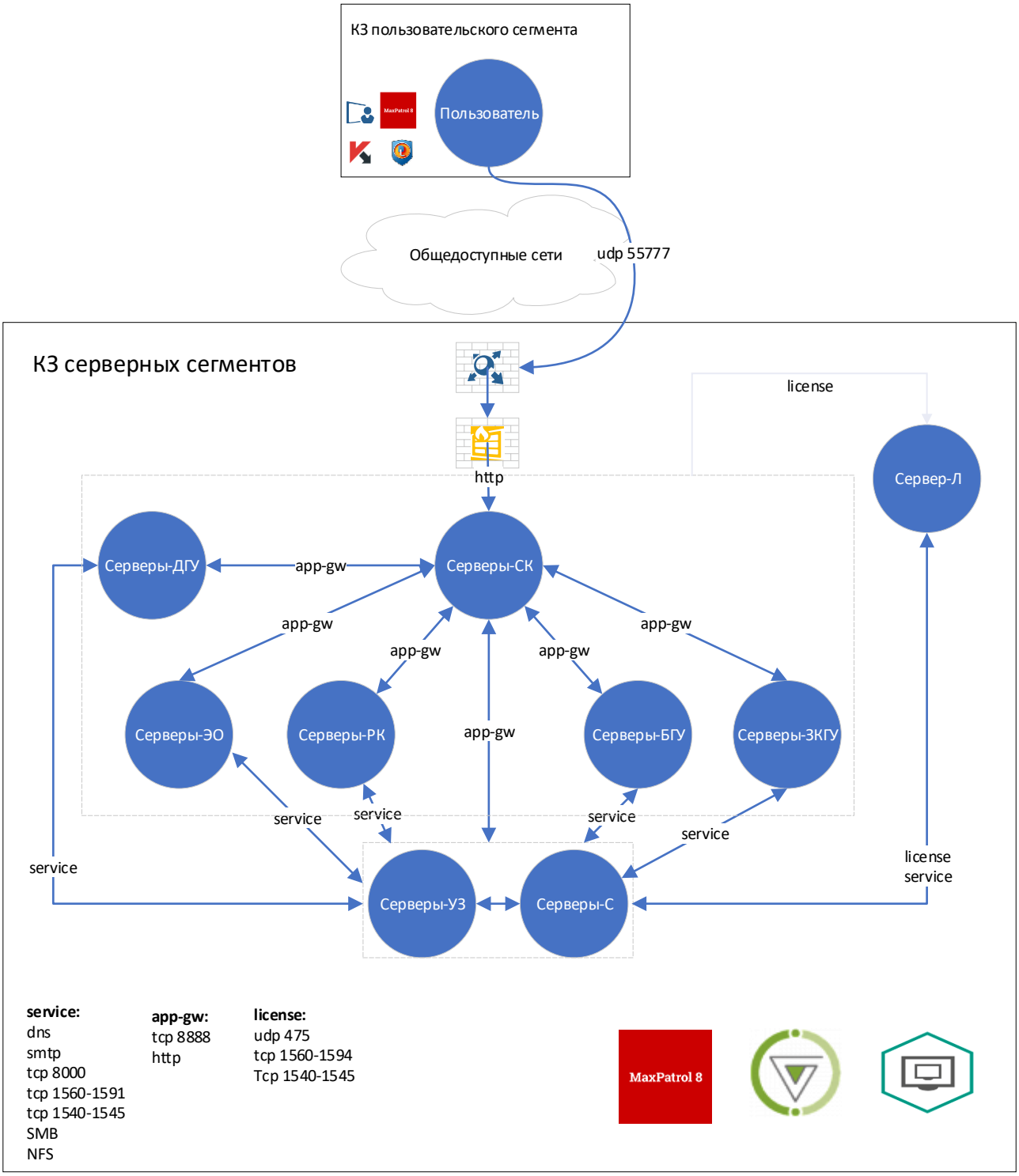
- для организации защищенного электронного взаимодействия с защищенной сетью, необходимо установить и настроить программное обеспечение ViPNet Client 4.x (КС1 или выше);
- установить и настроить средство защиты информации от несанкционированного доступа Dallas Lock 8.0-K;
- установить и настроить антивирусное средство Kaspersky Endpoint Security 11 для Windows;
- выполнение обязательных организационных мероприятий, необходимых при эксплуатации средств криптографической защиты в соответствии с требованиями нормативных документов ФСБ России.

3.2. Схема реализации системы защиты информации

Рабочие места пользователей ЦОС ФХД располагаются в различных КЗ органов государственной власти Республики Саха (Якутия), государственных учреждений Республики Саха (Якутия).

Серверный сегмент ЦОС ФХД располагается в аттестованном по требованиям защиты информации Центре обработки данных электронного правительства Республики Саха (Якутия) по адресу: 677980, Российская Федерация, Республика Саха (Якутия), г. Якутск, ул. Кирова, 12, каб. 3049.

Обобщенная схема взаимодействия сегментов ЦОС ФХД представлена на Рисунке №1.



Kaspersky Endpoint Security 11
Dallas Lock 8.0-K
ViPNet Client 4
vGate R2
Kaspersky Security Для виртуальных сред Легкий агент 5.1
ViPNet xFirewall 5000
ViPNet Coordinator HW 4
MaxPatrol

Рисунок №1. Обобщенная схема взаимодействия

4. Приемочные испытания подключаемых сегментов к информационной системе

В соответствии с п. 17.3 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» утвержденного приказом ФСТЭК России от 18.02.2013 № 17:

- Допускается аттестация ИС на основе результатов аттестационных испытаний выделенного набора сегментов ИС, реализующих полную технологию обработки информации. В этом случае распространение аттестата соответствия на другие сегменты ИС осуществляется при условии их соответствия сегментам ИС, прошедшим аттестационные испытания;
- Сегмент считается соответствующим сегменту ИС, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по ИС и ее системе защиты информации;
- Соответствие сегмента, на который распространяется аттестат соответствия, сегменту ИС, в отношении которого были проведены аттестационные испытания, подтверждается в ходе приемочных испытаний ИС или сегментов ИС.
- В сегментах ИС, на которые распространяется аттестат соответствия, оператором обеспечивается соблюдение эксплуатационной документации на систему защиты информации ИС и организационно-распорядительных документов по защите информации.

Программа и методика приемочных испытаний для пользовательских сегментов ЦОС ФХД представлена в Приложении №1 к данному Регламенту. Приемочные испытания проводятся комиссией (приемочной комиссией).

По результатам приемочных испытаний составляется Протокол приемочных испытаний и Акт по результатам приемочных испытаний.

Пример Протокола приемочных испытаний представлен в Приложении №2 к данному Регламенту.

Пример Акта по результатам приемочных испытаний представлен в Приложении №3 к данному Регламенту.

При выполнении всех вышеуказанных требований, приемочные испытания подключаемого пользовательского сегмента ЦОС ФХД считается успешными.

Приложение №1
к Регламенту подключения новых пользователей

Таблица №1 — номера пунктов Частного технического задания на создание системы защиты информации

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
1.	4.1.1.1	Проверка подсистем СЗИ	Подсистемы, выбранные для реализации в СЗИ, должны соответствовать минимально необходимым для реализации в соответствующем классе, если иное не указано в данном пункте.
2.	4.1.1.2	Проверка способов и средств связи для информационного обмена между компонентами системы	Взаимодействие технических средств, участвующих в обработке защищаемой информации, должно производится в пределах контролируемой зоны и по протоколу TCP/IP. Коммутационное оборудование должно быть совместимо между собой при передаче/приеме информации.
3.	4.1.1.3	Проверка характеристик взаимосвязей создаваемой системой со смежными системами	Если передача информации производится по линиям связи, выходящим за пределы контролируемой зоны, то должны использоваться сертифицированные ФСБ России средства криптографической защиты информации.
4.	4.1.1.4	Проверка режимов функционирования	Система должна иметь возможность производить технологические перерывы на профилактические работы и/или устранение сбоев.
5.	4.1.1.5	Проверка диагностирования системы	СрЗИ должны иметь возможность журналирования процессов, происходящих в системе. Также должны иметь инструменты для диагностирования основных процессов и оборудования СЗИ.
6.	4.1.1.6	Проверка способности системы на модернизацию	При подключении новых рабочих мест пользователей к ИС, не должны происходить сбои СЗИ. Обновление программного обеспечения, используемых в автоматизированных рабочих местах, должно производится автоматически. Функции обновления программного обеспечения СрЗИ должны быть прописаны в инструкциях администратора информационной безопасности.
7.	4.1.2.1	Проверка численности персонала	В системе должны быть пользователи и администраторы. Функции администратора информационной безопасности и администратора информационной системы могут быть совмещены.
8.	4.1.2.2	Проверка квалификации персонала	Пользователи системы должны иметь общую подготовку, которая включает: — Навыки работы с офисным программным обеспечением; — Навыки работы с операционной системой; — Навыки работы с веб-браузерами. Администраторы должны иметь общую подготовку и специальную подготовку для работы с системой. Специальная подготовка включает: — Навыки работы с СрЗИ;

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
			— Навыки работы с администраторскими полномочиями в операционной системе; — Навыки работы со средством криптографической защиты информации.
9.	4.1.2.3	Проверка режима работы персонала	Пользователи и администраторы должны иметь 8 часовой рабочий день, если иное не прописано в трудовом договоре.
10.	4.1.3	Проверка возможности модернизации системы при изменении нормативно-правовой базы Российской Федерации	Документация на систему и настройки СрЗИ должны иметь возможность при изменении нормативно-правовой базы Российской Федерации.
11.	4.1.4	Проверка надежности системы	Технические меры по обеспечению надежности должны предусматривать: — резервирование критически важных компонентов и данных системы и отсутствие единой точки отказа. — использование технических средств с избыточными компонентами и возможностью их горячей замены. — конфигурирование используемых средств и применение специализированного ПО, обеспечивающего высокую доступность. Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок обслуживающего персонала, минимизацию времени ремонта или замены вышедших из строя компонентов системы за счет: — квалификации обслуживающего персонала; — регламентации и нормативного обеспечения выполнения работ обслуживающего персонала и пользователей системы; — регламентации проведения работ и процедур по обслуживанию и восстановлению системы; — своевременной диагностики неисправностей; — наличия запасных инструментов и принадлежностей; — наличия договоров на сервисное обслуживание и поддержку компонентов системы.
12.	4.1.5	Проверка безопасности системы	СЗИ должна отвечать требованиям по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств системы (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и т.п.), по допустимым уровням освещенности, вибрационных и шумовых нагрузок.
13.	4.1.6	Проверка эргономичности и технической эстетики	Качество взаимодействия персонала со средствами защиты информации, входящими в состав СЗИ, и комфортность условий его работы должно по эргономическим и гигиеническим требованиям соответствовать:

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
			– ГОСТ Р 50948–2001 «Дисплеи. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности»; – «Гигиенические требования к видео дисплейным терминалам, персональным электронно–вычислительным машинам. Санитарные правила и нормы СанПиН 2.2.2/2.4.1340–03». Конфигурация средств защиты информации должна обеспечивать удобный для персонала интерфейс, при этом рабочие АРМ, на которых установлены средства защиты, должны обеспечивать возможность непрерывной работы за счет: – правильного и удобного расположения монитора; – удобного расположения и формы клавиатуры; – удобной формы манипуляторов.
14.	4.1.7	Проверка транспортабельности	Требований нет.
15.	4.1.8	Проверка эксплуатационных мероприятий	В системе должны быть предусмотрены следующие виды диагностирования и технического обслуживания: – Оперативное обслуживание; – Профилактически работы.
16.	4.1.9	Проверка защиты информации от несанкционированного доступа	Получение аттестата.
17.	4.1.10	Проверка сохранности информации при авариях	При авариях СЗИ должно обеспечивать сохранность защищаемой информации.
18.	4.1.11	Проверка защиты системы от внешних воздействий	В рамках СЗИ должны использоваться средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации и требованиям Госкомсвязи России «Автоматизированные системы управления аппаратурой электросвязи», 1998 года по электромагнитной совместимости и помехозащищенности.
19.	4.1.12	Проверка патентной чистоты	Все используемые СрЗИ должны иметь лицензию на использование.
20.	4.1.13	Проверка стандартизации и унификации в системе	Все оборудование, входящие в состав подсистем СЗИ, должно соответствовать стандартам Российской Федерации. Должна обеспечиваться совместимость технических средств и ПО СрЗИ с техническими средствами и ПО, используемыми в ИС.
21.	4.1.14	Проверка поставляемых технических средств и средств защиты информации	–
22.	4.2.1.1	Проверка выбора базового набора мер защиты информации	Базовый набор мер защиты информации должен соответствовать выбранному классу защищенности информационной системы.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
23.	4.2.1.2	Проверка адаптированного базового набора мер защиты информации	Адаптация базового набора мер защиты информации должна быть реализована на основе структурно-функциональных характеристик системы и исключать меры защиты информации, не используемые в информационной системе структурно-функциональных характеристик.
24.	4.2.1.3	Проверка уточненного адаптированного базового набора мер защиты информации	Уточнение адаптированного базового набора ер защиты информации в системе не проводилась.
25.	4.2.1.4	Проверка дополненного уточненного адаптированного базового набора мер защиты информации	При проверке дополненного уточненного адаптированного базового набора мер защиты информации в системе должны быть реализованы следующие меры защиты информации: — организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; — обеспечение сохранности носителей персональных данных; — утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей; — использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз; — назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.
26.	4.2.2	Проверка регламента реализации функций обеспечения безопасности информации	На момент проведения приемочных испытаний все функции и подсистемы защиты информации должны быть реализованы в системе.
27.	4.2.3	Проверка качества реализации каждой функции обеспечения безопасности информации	При выполнении всех функций данной таблицы, пункт считается выполненным.
28.	4.3.1	Проверка математического обеспечения системы	Используемые для шифрования информации средства должны реализовывать шифрование по ГОСТ и иметь сертификат соответствия ФСБ России.
29.	4.3.2.1	Проверка информационного обеспечения системы	В СЗИ должны обрабатываться технологические и административные данные.
30.	4.3.2.2	Проверка информационного обмена между компонентами системы	Информационный обмен должен производится в сервера системы на клиентское рабочее место и с клиентского рабочего места на сервер в двухстороннем режиме.
31.	4.3.2.3	Проверка информационной совместимости со смежными системами	По информационной совместимости СЗИ не должна конфликтовать со смежными подсистемами, используемыми в информационной системе.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
32.	4.3.2.4	Проверка функций защиты данных от разрушений при авариях и сбоях в электропитании системы	СрЗИ должны обеспечивать восстановление СЗИ и защищаемой информации после аварий и сбоев в электропитании системы
33.	4.3.2.5	Проверка контроля, хранения, обновления и восстановления данных	При обновлении программного обеспечения СрЗИ должны быть сверены контрольные суммы дистрибутива и обновившегося программного обеспечения СрЗИ.
34.	4.3.2.6	Проверка придания документам юридической силы	Требований нет.
35.	4.3.3	Проверка лингвистического обеспечения	Ввод пароля и других данных для обеспечения защиты информации в СЗИ, должны производится с использованием кириллицы или латиницы.
36.	4.3.4.1	Проверка независимости программных средств от СВТ и ОС	СрЗИ должны быть совместимы (установлены и корректно работать) с используемыми в системе автоматическими рабочими местами.
37.	4.3.4.2	Проверка качества программных средств	Программное обеспечение СрЗИ должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных. Также должны иметь действующий сертификат соответствия ФСТЭК России и ФСБ России.
38.	4.3.5.1	Проверка вида технических средств	Аппаратные платформы должны использоваться, по возможности, разработанные и произведенные в Российской Федерации.
39.	4.3.6	Проверка метрологического обеспечения	Требований нет.
40.	4.3.7.1	Проверка структуры и функций персонала, участвующих в функционировании системы	Инструкция и администратор информационной безопасности должны быть утверждены руководителем организации.
41.	4.3.7.2	Проверка организации функционирования системы	В СЗИ должны быть установлены и настроены все СрЗИ и проведен анализу уязвимости.
42.	4.4	Проверка защиты информации от утечки по техническим каналам	Устройства вывода информации (мониторы), должны предотвращать перехват информации ограниченного доступа по видовым техническим каналам утечки информации. Предывание в контролируемой зоне не допущенных лиц должно быть запрещено во избежание прослушивания переговоров. Окна при работе должны быть закрыты и предотвращать прослушивание информации по акустическому каналу утечки информации.
43.	4.5	Проверка физической защиты информации	Средства физической защиты должны осуществлять: – предотвращение несанкционированного проникновения нарушителей в КЗ, помещения, где размещены компоненты информационной системы; – воспрепятствование насильственному разрушению дверей, окон, вентиляционных люков и других мест возможного проникновения в помещения, где размещены компоненты информационной системы; – регулирование потока входящих лиц (сотрудников и посетителей) и ограничения доступа в конкретные помещения лиц, не имеющих специального разрешения;

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
			— постоянный контроль помещений, в которых размещены компоненты информационной системы; — обеспечение пожарной безопасности.
44.	4.6	Проверка защиты информации при информационном взаимодействии с иными информационными системами	При информационном взаимодействии с иными информационными системами, иная информационная система должна подтвердить защищенность своей системы в виде аттестата или ином виде.

Таблица №2 – ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ИНФОРМАЦИИ Приложение №1 и Приложение №2 Частного технического задания на создание системы защиты информации ИС

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		Идентификация и аутентификация субъектов доступа и объектов доступа	
1.	ИАФ.1	Проверка наличия идентификационной и аутентификационной информации у работников оператора и однозначное сопоставление идентификатора пользователя с запускаемым от его имени процессам.	Пользователи СЗИ должны иметь логины, которые однозначно идентифицируют пользователя. Пользователь СЗИ для входа в систему должен ввести логин и пароль.
2.	ИАФ.3	Проверка: — Наличия администратора безопасности, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств; — Наличия формированного идентификатора, который однозначно идентифицирует пользователя и (или) устройство.	В СЗИ ОИ должен быть назначен администратор безопасности. Пользователи СЗИ должны иметь логины, которые однозначно идентифицируют пользователя.
3.	ИАФ.4	Проверка: — Наличия администратора безопасности ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации; — Функций выдачи начальной аутентификационной информации;	В СЗИ ОИ должен быть назначен администратор безопасности. СрЗИ должна иметь функцию выдачи начальных паролей для пользователей. СрЗИ должна иметь функцию обновления паролей с периодичностью, указанной в документации оператора. СрЗИ должна выдавать пароль определённой сложности, указанной в документации оператора. СрЗИ должна препятствовать неправомерному доступу и модификации паролей пользователей и администраторов.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		– Функций обновления аутентификационной информации с периодичностью, установленной оператором; – сложности выдаваемой аутентификационной информации; – Мер по защите аутентификационной информации от неправомерного доступа к ней и модифицирования.	
4.	ИАФ.5	Проверка защиты обратной связи в процессе аутентификации.	Вводимые символы пароля должны отображаться условными знаками «*», «×» или иными знаками.
5.	ИАФ.6	Проверка наличия идентификационной и аутентификационной информации у пользователей, не являющихся работниками оператора, и однозначное сопоставление идентификатора пользователя с запускаемым от его имени процессам.	Пользователи, не являющиеся работниками оператора, должны иметь логины, которые однозначно идентифицируют пользователя. Пользователь СЗИ для входа в систему должен ввести логин и пароль.
Управление доступом субъектов доступа к объектам доступа			
6.	УПД.1	Проверка функций управления учетными записями пользователей, в том числе внешних пользователей: – определения типа учетной записи; – объединения учетных записей в группы; – верификации пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; – заведения, активация, блокирование и уничтожение учетных записей пользователей; – периодичность пересмотра учетных записей пользователей; – оповещения администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;	СрЗИ в СЗИ ОИ должна выполнять следующие функции управления учетными записями пользователей, в том числе внешних пользователей: – определять типы учетных записей; – создавать группы учетных записей; – оповещение администратора безопасности о изменении сведений о пользователе. Наличие администратора безопасности, который проводит верификацию пользователя, активацию, блокирование, уничтожение учетных записей, периодичный пересмотр учетных записей, уничтожение временных учетных записей, предоставление прав доступа пользователям,

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		— уничтожения временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в ОИ; — предоставления пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС.	
7.	УПД.2	Проверка метода, тип и правила разграничения доступа.	СрЗИ должны реализовывать дискреционный метод доступа.
8.	УПД.3	Проверка следующих функций: — фильтрация информационных потоков; — разрешение передачи информации в ОИ только по определенному маршруту.	СрЗИ должна производить фильтрацию информационных потоков и определять маршруты, пот которым разрешена передача информации.
9.	УПД.4	Проверка обеспечения разделение полномочий (ролей) пользователей, администраторов безопасности и администраторов ИС.	СрЗИ должна разделять полномочия пользователей и администраторов.
10.	УПД.5	Проверка минимально необходимых прав и привилегий пользователям, администраторам безопасности и администраторам ИС.	СрЗИ должна ограничивать действия пользователей и администраторов.
11.	УПД.6	Проверка настроек СрЗИ, которая регламентирует количество неуспешных попыток входа в ОИ.	СрЗИ должна ограничивать количество неуспешных попыток ввода пароля.
12.	УПД.10	Проверка блокирования СрЗИ сеанса доступа к ОИ пользователю.	СрЗИ должна блокировать сеанс доступа к ОИ по истечению времени, указанной в документации оператора.
13.	УПД.11	Проверка перечня действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.	СрЗИ должна обеспечивать только те действия, которые указаны в документации оператора.
14.	УПД.13	Проверка: — установления (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа ИС;	СрЗИ должны отказать пользователю произвести удаленный доступ к серверам и другим рабочим местам пользователей. Действия по удаленному доступу должны быть отражены документации оператора. СрЗИ должны фиксировать и отключать несанкционированный удаленный доступ к рабочим местам пользователей и серверам ОИ.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		– ограничения на использование удаленного доступа, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа; – предоставления удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); – мониторинга и контроля удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС.	
15.	УПД.16	Проверка каналов связи с иными информационными системами	Соединение с иными информационными системами должна производится по защищенным СКЗИ каналам.
Ограничение программной среды			
16.	ОПС.3	Проверка пользователей на наличие прав на установку ПО	СЗИ не должны давать пользователю установить ПО.
Защита машинных носителей информации			
17.	ЗНИ.1	Проверка наличия журнала учета МНИ.	Оператор должен иметь журнал учета МНИ.
18.	ЗНИ.2	Проверка наличия документа, где определены лица, имеющие физический доступ к МНИ.	Оператор должен иметь приказ/перечень либо другой документ, определяющий перечень лиц, которым разрешен физический доступ к МНИ.
19.	ЗНИ.8	Проверка гарантированного уничтожения информации на МНИ.	СрЗИ должна иметь функцию затирания данных и(или) перезапись данных случайными/заранее выбранными последовательностями данных.
Регистрация событий безопасности			
20.	РСБ.1	Проверка у оператора документа, где отражены события безопасности регистрируемые СрЗИ.	СрЗИ должны вести журналы событий безопасности.
21.	РСБ.2	Проверка наличия документа, где отражены состав и содержание информации о событиях безопасности, подлежащих регистрации. Проверялись: – регистрация входа (выхода) пользователя в ИС; – регистрации подключения МНИ и вывода информации на носители информации;	СрЗИ должны регистрировать событий безопасности указанные в документе.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		– регистрация запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации; – регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав; – регистрация попыток доступа программных средств к защищаемым объектам доступа; – регистрации попыток удаленного доступа к ИС.	
22.	РСБ.3	Проверка сбора, записи и хранения информации о событиях безопасности.	Сбор, запись и хранение информации о событиях безопасности должен предусматривать: – возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени; – генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту); – хранение информации о событиях безопасности в течение установленного времени.
23.	РСБ.4	Проверка наличия регламента реагирования на сбои при регистрации событий безопасности	Регламент реагирования на сбои при регистрации событий должно предусматривать: – предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности; – реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности.
24.	РСБ.5	Проверка наличия средств мониторинга (просмотра и анализа) записей регистрации.	СрЗИ должны предусматривать наличие функций средств мониторинга записей регистрации.
25.	РСБ.6	Поверка генерации надежных меток времени и синхронизации системного времени.	ОИ должны синхронизировать системное время с NTP-сервера.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
26.	РСБ.7	Проверка получения меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС.	Зарегистрированные события безопасности должны иметь корректные временные метки.
		Антивирусная защита	
27.	АВЗ.1	Проверка наличия на АРМ пользователей антивирусного СрЗИ. Также проверялись: — сроки действия лицензии; — проведение периодических проверок компонентов ОИ на наличие вирусов.	На АРМ ОИ должны быть установлены антивирусные СрЗИ. Сроки действия лицензий должны быть действующими. Должны быть выставлены параметры периодического контроля компонентов ОИ на наличие вирусов.
28.	АВЗ.2	Проверка обновления базы данных признаков вирусов.	Антивирусное СрЗИ должно производить обновление базы данных признаков вирусов, которая должна предусматривать: — получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вирусов; — получение из доверенных источников и установку обновлений базы данных вирусов.
		Контроль (анализ) защищенности информации	
29.	АНЗ.1	Проверка наличия регламентов по выявлению (поиске), анализу и устранению уязвимостей и обновления базы признаков уязвимостей	Оператор должен иметь документ, регламентирующий по выявлению, анализу и устранению уязвимостей. Базы признаков уязвимостей СрЗИ должны обновляться.
30.	АНЗ.2	Проверка наличия регламента установки обновлений ПО, включая обновление ПО СрЗИ и наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.	Оператор должен иметь документ, регламентирующий установку обновлений ПО, включая По СрЗИ. Также должны весить отметки в эксплуатационных документах СЗИ, СрЗИ и ПО.
31.	АНЗ.3	Проверка контроля соответствия настроек ПО и СрЗИ параметрам настройки, приведенным в эксплуатационной документации на СЗИ и СрЗИ.	СрЗИ должны иметь настройки, соответствующие требованиям по защите информации.
32.	АНЗ.4	Проверка соответствия состава технических средств, ПО и СрЗИ приведенному в эксплуатационной документации, выполнение условий и сроков действия сертификатов соответствия на СрЗИ и наличие не санкционированно установленных технических средств, ПО и СрЗИ.	Технические средства, ПО и СрЗИ должны соответствовать эксплуатационной документации. Должны использоваться только СрЗИ с действующими сертификатами соответствия ФСТЭК России и(или) ФСБ России
33.	АНЗ.5	Проверка контроля правил генерации и смены паролей пользователей, заведение и удаление учетных записей пользователей, реализация правил разграничения доступом, полномочий пользователей.	СрЗИ должно осуществляться: — контроль правил генерации и смены паролей пользователей; — контроль заведения и удаления учетных записей пользователей; — контроль реализации правил разграничения доступом;

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
			— контроль реализации полномочий пользователей; — контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей; — устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.
Обеспечение целостности информационной системы и информации			
34.	ОЦЛ.3	Проверка наличия регламента восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций.	Документ, регламентирующий восстановление ПО, включая ПО СрЗИ должна предусматривать: — восстановление ПО, включая ПО СрЗИ, из резервных копий (дистрибутивов) ПО; — восстановление и проверка работоспособности СЗИ, обеспечивающие необходимый уровень защищенности информации; — возврат ОИ в начальное состояние, обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ОИ, определенных оператором, позволяющих решать задачи по обработке информации.
Защита технических средств			
35.	ЗТС.2	Проверка принятия режима контролируемой зоны.	Должен быть принят приказ об определении границ контролируемой зоны.
36.	ЗТС.3	Проверка наличия перечня (списка) лиц, допущенных к техническим средствам, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.	Оператор должен определить перечень лиц, допущенных имеющих доступ в контролируемую зону.
37.	ЗТС.4	Проверка расположения устройств вывода (отображения) информации, которая должна исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.	Устройства вывода (отображения, печати) информации должны располагаться так, чтобы исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.
Защита информационной системы, ее средств, систем связи и передачи данных			
38.	ЗИС.3	Проверка защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при	Защита информации должна обеспечиваться путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации СКЗИ.

№	Пункты ТЗ	Наименование проверок	Ожидаемый результат проверки
		ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.	

Приложение №2
к Регламенту подключения новых пользователей

начало формы протокола

Конфиденциально
Экз. №1

УТВЕРЖДАЮ
[должность руководителя]
[наименование организации]

_____ [ФИО]

« » _____ 2020 г.

Система защиты информации
сегмента [название сегмента]
[название информационной системы]

ПРИЕМОЧНЫЕ ИСПЫТАНИЯ

Протокол приемочных испытаний

На XX листах

[наименование населенного пункта]
[год]

Оглавление

Перечень сокращений

Сокращение	Определение
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГИС	Государственная информационная система
ИБ	Информационная безопасность
СЗИ	Система защиты информации
СрЗИ	Средство защиты информации
ОИ	Объект информатизации
НПА	

1. Наименование объекта информатизации

1.1. Для приемочных испытаний был представлены ОИ (Таблице №1).

Таблица №1

№	Название организации	Адрес
1.	[полное название организации 1]	[адрес организации 1]
2.	[полное название организации 2]	[адрес организации 2]
3.	...	...
4.	[полное название организации N]	[адрес организации N]

1.2. Приемочные испытания проводятся для ИС:

а. [название ИС 1];
б. [название ИС 2];
в. [название ИС ...];
г. [название ИС N].

1.3. Приемочные испытания проводились комиссией:

Руководитель комиссии:

[ФИО] [наименование организации], [должность]

Члены комиссии:

[ФИО] [наименование организации], [должность]

[ФИО] [наименование организации], [должность]

2. Цель приемочных испытаний

2.1. Целью приемочных испытаний является определение соответствия ОИ (сегмента ИС) требованиям по обеспечению безопасности информации, не составляющей государственную тайну (далее О защищаемой информации), и распространение аттестата соответствия ИС на ОИ (сегмент), на который проводятся приемочные испытания.

2.2. Приемочные испытания проводились в объеме предусмотренном в «Регламенте подключения новых пользователей» и включали в свой состав:

- проверка технологии обработки информации;
- проверку соответствия класса защищенности ОИ, на которые проводятся приемочные испытания, классу защищенности сегмента аттестованной ИС;
- проверку соответствия проектных решений ОИ, на которые проводятся приемочные испытания, проектным решениям сегмента аттестованной ИС;
- проверку соответствия проектных решений СЗИ ОИ, на которые проводятся приемочные испытания, проектным решениям СЗИ сегмента аттестованной ИС;
- проверку угроз безопасности информации ОИ, на которые проводятся приемочные испытания, угрозам безопасности информации сегмента аттестованной ИС.

3. Перечень используемых нормативных документов и методик

3.1. При проведении приемочных испытаний комиссия должна руководствоваться требованиями следующих НПА и методических документов в области защиты информации:

[1] Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[3] Постановление Правительства РФ от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

[4] Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[5] ГОСТ 34.603–92 Виды испытаний автоматизированных систем;

[6] ГОСТ 34.003–90 Автоматизированные системы. Термины и определения.

4. Перечень средств контроля защищённости информации

4.1. Перечень используемых средств контроля защищенности информации представлен в Таблице №2.

Таблица №2

№	Наименование	Модель[1]	Зав. номер	Сведения о сертификации, поверке (калибровке)
1.	Программа поиска и гарантированного уничтожения информации на дисках	«TERRIER», версия 3.0	Копия № XXXX СЗЗ XXXXXX	Сертификат ФСТЭК России №1193 от 16.05.2006, продлен до 16.05.2021
2.	Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС», версия 2.0.2	Копия № XXXX СЗЗ XXXXXX	Сертификат ФСТЭК России №1548 от 15.01.2008, действителен до 15.01.2020. Окончание срока технической поддержки 15.01.2025
3.	Средство создания модели системы разграничения доступа	«Ревизор 1 XP»	Копия № XXXX СЗЗ XXXXXX	Сертификат ФСТЭК России №989 от 08.02.2005, продлен до 08.02.2020. Окончание срока технической поддержки 08.02.2025
4.	Программа контроля полномочий доступа к информационным ресурсам	«Ревизор 2 XP»	Копия № XXXX СЗЗ XXXXXX	Сертификат ФСТЭК России №990 от 08.02.2005, продлен до 08.02.2020. Окончание срока технической поддержки 08.02.2025
5.	Сетевой сканер	Сетевой сканер Ревизор Сети 3.0	Копия № XXXX СЗЗ XXXXXX	Сертификат ФСТЭК России №3413 от 02.06.2015, продлен до 02.06.2023. Окончание срока технической поддержки 02.06.2026

5. Описание проверок

5.1. В ходе проведения приемочных испытаний ОИ на соответствие требованиям по обеспечению безопасности защищаемой информации и распространению аттестата соответствия ИС, были проведены следующие мероприятия:

- проверка технологии обработки информации;
- проверку соответствия класса защищенности ОИ, на которые проводятся приемочные испытания, классу защищенности сегмента аттестованной ИС;
- проверку соответствия проектных решений ОИ, на которые проводятся приемочные испытания, проектным решениям сегмента аттестованной ИС;
- проверку соответствия проектных решений СЗИ ОИ, на которые проводятся приемочные испытания, проектным решениям СЗИ сегмента аттестованной ИС;
- проверку угроз безопасности информации ОИ, на которые проводятся приемочные испытания, угрозам безопасности информации сегмента аттестованной ИС.

5.2. Меры по защите информации, описанные далее, реализованы во всех ОИ (сегментах).

[1] Модели предоставлены для примера

5.3. В случае если меры по защите информации в сегментах отличаются от общих принятых мер, то они описаны отдельно применительно к этому сегменту.

5.4. В ходе проведения приемочных испытаний был проведен анализ технологии обработки информации, включающая полноту исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации ОИ, исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков, определение состава использованных для обработки, хранения и передачи информации ОТСС.

5.4.1. Проверка состава и содержания представленных документов показала их достаточность для проведения приемочных испытаний заявленных ОИ.

5.4.2. В ходе проведения приемочных испытаний представленной документации комиссией была проанализирована система доступа пользователей ОИ к защищаемым информационным ресурсам и данные по технологии обработки и передачи защищаемой информации, также были проанализированы обобщенные технологические схемы ОИ.

Проверка показала наличие правильно организованной системы доступа пользователей ОИ к защищаемым информационным ресурсам.

5.5. В ходе проведения приемочных испытаний был выявлен и проанализирован перечень сертифицированных СрЗИ, функционирующих в ОИ.

Перечень СрЗИ, функционирующих в ОИ, приведен в Таблице №3.

Таблица №3

№ п/п	Наименование СрЗИ	Заводской (серийный) номер	Сведения о сертификате/ Специальный защитный знак	Место установки СрЗИ
1.	Dallas Lock 8.0-K	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №2720 от 25.09.2012, действителен до 25.09.2021 / xxxxxx	г. Якутск, ул. Халтурина, д. 243, помещение «Бухгалтерия»
2.	Kaspersky Endpoint Security 11 для Windows	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №4068 от 22.01.2019, действителен до 22.01.2024 / xxxxxx	
3.	ViPNet Client 4	XXXXXXXXXXXX	Сертификат соответствия ФСБ России № СФ/124-3787 от 17.12.2021, действителен до 28.02.2021 / СКЗИ xxx-xxxxxx	
4.	Dallas Lock 8.0-K	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №2720 от 25.09.2012, действителен до 25.09.2021 / xxxxxx	г. Якутск, ул. Халтурина, д. 243, помещение «Бухгалтерия»
5.	Kaspersky Endpoint Security 11 для Windows	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №4068 от 22.01.2019, действителен до 22.01.2024 / xxxxxx	
6.	ViPNet Client 4	XXXXXXXXXXXX	Сертификат соответствия ФСБ России № СФ/124-3787 от 17.12.2021, действителен до 28.02.2021 / СКЗИ xxx-xxxxxx	
7.	Dallas Lock 8.0-K	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №2720 от 25.09.2012, действителен до 25.09.2021 / xxxxxx	г. Якутск, ул. Халтурина, д. 243, помещение «Бухгалтерия»

№ п/п	Наименование СрЗИ	Заводской (серийный) номер	Сведения о сертификате/ Специальный защитный знак	Место установки СрЗИ
8.	Kaspersky Endpoint Security 11 для Windows	XXXXXXXXXXXX	Сертификат соответствия ФСТЭК России №4068 от 22.01.2019, действителен до 22.01.2024 / xxxxxx	
9.	ViPNet Client 4	XXXXXXXXXXXX	Сертификат соответствия ФСБ России № СФ/124-3787 от 17.12.2021, действителен до 28.02.2021 / СКЗИ xxx-xxxxxx	

5.6. Комиссией была проведена проверка правильности определения класса защищенности ОИ (сегмента).

5.6.1. Сегменту ИС, на соответствие которому проводятся приемочные испытания, присвоен класс защищенности К3.

5.6.2. С учётом того, что в ОИ обрабатывается информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, ОИ имеет 3 итоговый уровень значимости, ОИ имеет объектовый масштаб, в соответствии с нормативным актом [4] комиссией установлен класс защищенности К3, что соответствует представленному Акту определения класса защищенности ОИ.

5.7. Комиссией проведена проверка соответствия проектных решений в ОИ (сегмента), на которые проводятся приемочные испытания, проектным решениям сегмента аттестованного по требованиям безопасности информации ИС.

5.7.1. В ходе проверки комиссия установила, что в ОИ и сегменте аттестованного по требованиям безопасности информации ИС реализованы идентичные проектные решения ОИ. ОИ, на которое проводятся приемочные испытания, может работать с аттестованной по требованиям безопасности информации ИС.

5.8. Комиссией проведена проверка соответствия проектных решений СЗИ ОИ (сегмента), на которые проводятся приемочные испытания, проектным решениям СЗИ сегмента аттестованного по требованиям безопасности информации ИС.

5.8.1. В ходе проверки комиссия установила, что СЗИ ОИ и СЗИ сегмента аттестованного по требованиям безопасности информации ИС реализованы идентичные проектные решения СЗИ. СЗИ ОИ, на которое проводятся приемочные испытания, может работать с СЗИ аттестованной по требованиям безопасности информации ИС (Таблица №4).

Таблица №4

№	Пункт ТЗ[2]	Результат[3]	Примечание[4]
1.	4.1.1.1		
2.	4.1.1.2		
3.	4.1.1.3		
4.	4.1.1.4		
5.	4.1.1.5		
6.	4.1.1.6		
7.	4.1.2.1		

[2] Пункт Частного технического задания на создание системы защиты информации ИС

[3] Результат Соответствия/Несоответствия/Частичного соответствия пунктам Частного технического задания на создание системы защиты информации ИС

[4] Примечание, заполняется опционально

№	Пункт ТЗ[2]	Результат[3]	Примечание[4]
8.	4.1.2.2		
9.	4.1.2.3		
10.	4.1.3		
11.	4.1.4		
12.	4.1.5		
13.	4.1.6		
14.	4.1.7		
15.	4.1.8		
16.	4.1.9		
17.	4.1.10		
18.	4.1.11		
19.	4.1.12		
20.	4.1.13		
21.	4.1.14		
22.	4.2.1.1		
23.	4.2.1.2		
24.	4.2.1.3		
25.	4.2.1.4		
26.	4.2.2		
27.	4.2.3		
28.	4.3.1		
29.	4.3.2.1		
30.	4.3.2.2		
31.	4.3.2.3		
32.	4.3.2.4		
33.	4.3.2.5		
34.	4.3.2.6		
35.	4.3.3		
36.	4.3.4.1		
37.	4.3.4.2		
38.	4.3.5.1		
39.	4.3.7.1		
40.	4.3.7.2		
41.	4.4		
42.	4.5		
43.	4.6		
Требования к мерам защиты информации Приложение №1 и Приложение №2[5]			
44.	ИАФ.1		
45.	ИАФ.2		
46.	ИАФ.3		

[5] Меры защиты информации берутся с Частного технического задания на создание системы защиты информации для конкретного сегмента на который проводится приемочные испытания

№	Пункт ТЗ[2]	Результат[3]	Примечание[4]
47.	ИАФ.4		
48.	ИАФ.5		
49.	ИАФ.6		
50.	УПД.1		
51.	УПД.2		
52.	УПД.3		
53.	УПД.4		
54.	УПД.5		
55.	УПД.6		
56.	УПД.10		
57.	УПД.11		
58.	УПД.13		
59.	УПД.16		
60.	ОПС.2		
61.	ОПС.3		
62.	ЗНИ.1		
63.	ЗНИ.2		
64.	ЗНИ.5		
65.	ЗНИ.8		
66.	РСБ.1		
67.	РСБ.2		
68.	РСБ.3		
69.	РСБ.4		
70.	РСБ.5		
71.	РСБ.6		
72.	РСБ.7		
73.	АВЗ.1		
74.	АВЗ.2		
75.	АНЗ.1		
76.	АНЗ.2		
77.	АНЗ.3		
78.	АНЗ.4		
79.	АНЗ.5		
80.	ОЦЛ.3		
81.	ЗТС.2		
82.	ЗТС.3		
83.	ЗТС.4		
84.	ЗИС.3		

5.9. В аттестованном по требованиям безопасности информации ИС актуальными угрозами безопасности информации являются угрозы безопасности информации, представленные в Таблице №5.

Таблица №5[6]

№ п/п	Код УБИ ФСТЭК	Наименование УБИ
1	УБИ.006	Угроза внедрения кода или данных
2	УБИ.014	Угроза длительного удержания вычислительных ресурсов пользователями
3	УБИ.015	Угроза доступа к защищаемым файлам с использованием обходного пути
4	УБИ.022	Угроза избыточного выделения оперативной памяти
5	УБИ.026	Угроза искажения XML-схемы
6	УБИ.028	Угроза использования альтернативных путей доступа к ресурсам
7	УБИ.031	Угроза использования механизмов авторизации для повышения привилегий
8	УБИ.033	Угроза использования слабостей кодирования входных данных

5.9.1. В ОИ, на которое проводится приемочные испытания, реализована идентичная с аттестованной ИС технология обработки информации, класс защищенности информации, проектные решения сегмента, проектные решения СЗИ.

5.9.2. На основе этого в ОИ (сегменте) угрозы безопасности информации идентичны с угрозами безопасности информации, которые были установлены для сегмента аттестованного по требованиям безопасности информации ИС.

6. Результат испытаний

Результаты приемочных испытаний объекта информатизации [название организации] расположенного по адресам:

г. Якутск, [адрес с указанием кабинета],
г. Якутск, [адрес с указанием кабинета],
г. Якутск, [адрес с указанием кабинета],
г. Якутск, [адрес с указанием кабинета],

установили соответствие аттестованному по требованиям безопасности информации сегменту [название сегмента] [наименование ИС]. Комиссия установила, что объектам информатизации возможно распространение аттестата соответствия № [номер аттестата соответствия] от [дата аттестата соответствия].

Руководитель комиссии:

[Должность] _____ [ФИО]

Состав комиссии:

[Должность] _____ [ФИО]

[Должность] _____ [ФИО]

конец формы протокола

[6] Таблица заполнять в соответствии с угрозами безопасности информации, выявленными в модели угроз безопасности информации ИС.

начало формы

АКТ

по результатам приемочных испытаний системы защиты информации сегмента
[название сегмента]
[название информационной системы]

[наименование населенного пункта] [дата]

Приемочная комиссия объектов информатизации (далее – Комиссия[7]) в составе:

Председатель комиссии:

[ФИО] [наименование организации], [должность]

Члены комиссии:

[ФИО] [наименование организации], [должность]

[ФИО] [наименование организации], [должность]

провели приемочные испытания (далее - Испытания) сегмента [название сегмента] [название информационной системы] расположенного по адресу [адрес расположения испытуемого сегмента[8]]. Испытания проведены [дата проведения приемочных испытаний].

Результаты Испытаний приведены в Протоколе приемочных испытаний.

По результатам проведения Испытаний [название сегмента] [название информационной системы] Комиссия

РЕШИЛА

допустить [название сегмента] [название информационной системы] в постоянную эксплуатацию с [дата]

Подпись **Ф.И.О.**

Руководитель комиссии:

_____ [ФИО]

Члены комиссии:

_____ [ФИО]

_____ [ФИО]

конец формы

[7] Комиссия должна состоять минимум из 3 человек, включая председателя комиссии.
[8] Возможно произвести испытания на нескольких объектах информатизации.