

ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ

на оказание услуг по информационно-техническому сопровождению программного обеспечения «Мониторинг оборудования и аудит контрактов»

1. Цель закупки.

Обеспечение постоянного функционирования и непрерывной работы программного обеспечения для удаленного контроля работоспособности оборудования.

2. Наименование программного обеспечения:

2.1. Программное обеспечение «Мониторинг оборудования и аудит контрактов» (далее – ПО).

2.2. Запись в реестре отечественного программного обеспечения от 30.12.2021 № 12440 произведена на основании поручения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 30.12.2021 по протоколу заседания экспертного совета от 27.12.2021 № 1735пр.

3. Назначение программного обеспечения:

3.1. Автоматизация процессов удаленного мониторинга и контроля работоспособности оборудования.

3.2. Контроль исполнения контрактов по обслуживанию устройств.

3.3. Повышение эффективности работоспособности устройств.

3.4. Обеспечение актуальности и достоверности сведений о параметрах работоспособности устройств.

3.5. Подготовка, создание и сопровождение всей документации и статистической отчетности, необходимой для ведения делопроизводства на протяжении всего жизненного цикла оборудования.

4. Технические характеристики сопровождаемого программного обеспечения:

4.1. Осуществление взаимодействия пользователей посредством визуального графического интерфейса.

4.2. Наличие механизма идентификации и проверки подлинности пользователей при входе в программу по идентификатору (логину) и паролю и осуществление их доступа к системе в соответствии с заданными Администратором программного обеспечения ролями (правами доступа к функционалу программного обеспечения).

4.3. Предоставление пользователям доступа к ПО посредством тонкого клиента и веб-клиента через браузер.

4.4. Наличие картографического модуля Сахалинской области.

5. Функции программного обеспечения:

5.1. Наименование и количество метрик (параметров работоспособности) отображаемых в программном обеспечении по каждому типу устройства зависит от производителя оборудования и должны быть предоставлены Заказчиком.

5.2. Мониторинг и классификация проблем в работе оборудования.

5.3. Создание и контроль предписаний направления на ремонт или обслуживание устройств в разрезе контрактов и/или обслуживающих организаций.

5.4. Уведомления о проблемах работоспособности устройств (рабочий стол оператора, почтовый клиент).

5.5. Наличие свободных тегов (текстовых меток) для устройств, отборы по тегам на рабочем столе оператора.

5.6. Визуальное отображение на карте всех зарегистрированных в системе единиц оборудования в режиме реального времени с отображением их текущего статуса в сети.

5.7.Отслеживание исполнения контракта по обслуживанию устройств (учет периодичности технического обслуживания и ремонта узлов оборудования обслуживающей организацией).

5.8.Разделение доступности устройств по группам пользователей.

6. Состав программного обеспечения:

Программа содержит следующие разделы (модули, подсистемы):

- Оперативный контроль;
- Картография;
- Инциденты;
- Аналитика;
- Модуль управленческого учета;
- Модуль администрирования;
- Справочники.

7. Наименование и состав услуг:

Оказание услуг по информационно-техническому сопровождению программного обеспечения «Мониторинг оборудования и аудит контрактов», а именно:

- Консультация пользователей;
- Обновление программного обеспечения;
- Регламентное обслуживание программного обеспечения;
- Сопровождение программного обеспечения;
- Проверка адаптеров загрузки телеметрии с устройств;
- Расширение количества поддерживаемых устройств.

8. Консультация пользователей:

Исполнитель обязан осуществлять консультацию пользователей Заказчика по телефону технической поддержки Исполнителя, электронной почте по вопросам:

- Эксплуатации программного обеспечения, а именно: назначение интерфейсных элементов, настройка оформления отчетов, редактирование справочной информации;
- Разрешения проблемных ситуаций, возникших в ходе эксплуатации программного обеспечения.
- Время доступности технической поддержки с 16:00 до 19:00 по Сахалинскому времени.

9. Обновление программного обеспечения:

9.1.Передача не критичных текущих обновлений по электронной почте в адрес Заказчика для их последующей установки.

9.2.Внесение изменений в алгоритм работы действующего функционала на основании вступивших в действие изменений законодательства РФ.

9.3.Исполнитель самостоятельно и непрерывно осуществляет мониторинг выхода текущих обновлений, патчей и критических исправлений у разработчика программного обеспечения. Исполнитель обязан в срок не позднее 10 рабочих дней с момента официального выхода обновления направить Заказчику по электронной почте соответствующее уведомление, а также в срок не позднее 10 рабочих дней с момента согласования с Заказчиком провести работы по установке данного обновления в системе

10. Регламентные работы программного обеспечения:

10.1.Проверка работоспособности основного функционала и осуществление регламентных работ в рамках профилактического обслуживания информационных баз с целью предотвращения сбоев и ошибок подсистем программного обеспечения - еженедельно.

10.2.Проведение регламентных работ по очистке – один раз в 2 недели. В нерабочее время Заказчика:

с понедельника по пятницу с 18.00 до 08.00;
суббота (в любое время);
воскресенье (в любое время).

Проверка работоспособности подсистем (еженедельно):

- Оперативный контроль.
- Картография;
- Инциденты;
- Аналитика;
- Модуль управленческого учета;
- Модуль администрирования;
- Справочники.

11. Сопровождение программного обеспечения:

11.1.Внесение изменений в алгоритм работы программного обеспечения. Выполняется по заявке Заказчика в сроки, установленные для категории приоритета "Минимальный" Таблицы № 1 настоящего Технического задания.

11.2.Осуществление работ по оптимизации программного обеспечения для повышения производительности и отзывчивости интерфейсных элементов.

11.3.Осуществление работ по добавлению новых отчетов. По заявкам заказчика с приоритетом минимальный согласно Таблице № 1. Выполняется по заявке Заказчика в сроки, установленные для категории приоритета "Минимальный" Таблицы № 1 настоящего Технического задания.

11.4.Осуществление работ по добавлению новых проверок по запросу пользователей программного обеспечения на основании данных телеметрии, предоставляемых вендоров оборудования. По заявкам заказчика с приоритетом минимальный согласно Таблице № 1.

11.5.Заявки формируются в системе заявок Заказчика.

11.6.Исполнитель предоставляет доступ Заказчику к системе заявок по средствам удаленного доступа после предоставления подписанных документов «Соглашение о конфиденциальности» (Приложение № 3) и «Акт настройки средств защиты на автоматизированном рабочем месте, подключаемом к информационно-телекоммуникационной инфраструктуре ГКУ СО «ЦРЦТ» (Приложение № 4).

11.7.Восстановление работоспособности программного обеспечения в случае возникновения сбоев, а также обновление и настройка программного обеспечения выполняются в соответствии с таблицей № 1.

Таблица №1

Категория	Описание сбоя	Срок восстановления
Высокий	Полная неработоспособность системы, потеря данных, ошибки, блокирующие работу системы	1 рабочий день
Средний	Работа системы сильно затруднена, критичная функция недоступна	2 рабочих дня
Низкий	Некритичные функции работают с ошибками, производительность снижена.	3 рабочих дня
Минимальный	Косметические дефекты, опечатки, добавление новых устройств, добавление новых источников загрузки,	8 рабочих дней

	настройка загрузки телеметрии, добавление новых отчетов, разработка и добавление нового функционала программного обеспечения, не влияющие на функционал.	
--	--	--

12. Обслуживание программного обеспечения загрузки данных с устройств:

Настройка загрузки телеметрии при изменении форматов данных, связанных с обновлением прошивки устройств по заявкам Заказчика (с указанием версии прошивки), с приоритетом минимальный согласно Таблице № 1. Срок выполнения заявок категорий "Низкий" и "Минимальный" на добавление новых типов, моделей или источников данных устройств исчисляется с момента предоставления Заказчиком Исполнителю полного комплекта технической документации (протоколов обмена, документации по API) от производителя (вендора) оборудования.

13. Расширение количества поддерживаемых устройств:

13.1. Добавление новых источников загрузки данных по уже добавленным в ПО устройствам осуществляется по заявкам Заказчика (с приложением технической документации), с приоритетом «минимальный» согласно Таблице № 1.

13.2. Добавление новых типов устройств или моделей устройств в ПО осуществляется по заявкам Заказчика (с приложением технической документации по API или описания протоколов обмена), с приоритетом «минимальный» согласно Таблице № 1. Срок выполнения заявок категорий "Низкий" и "Минимальный" на добавление новых типов, моделей или источников данных устройств исчисляется с момента предоставления Заказчиком Исполнителю полного комплекта технической документации (протоколов обмена, документации по API) от производителя (вендора) оборудования.

14. Общие требования к Исполнителю:

14.1. Требования, установленные в соответствии с законодательством РФ, к лицам, осуществляющим поставку товара, выполнение работ, оказание услуг, являющихся объектом закупки в соответствии с пунктом 1 части 1 статьи 31 Закона № 44-ФЗ. В соответствии с положениями ст. 1229, 1233 Гражданского кодекса РФ участник закупки должен являться правообладателем исключительного права или обладать правом на использование объекта интеллектуальной собственности.

14.2. По окончании соответствующего этапа оказания услуг Исполнитель должен предоставить Заказчику 2 отчета об оказанных услугах по форме согласно Приложению №1 и Приложению №2 не позднее даты формирования Документа о приемке посредством ЕИС, предварительно согласовав с Заказчиком результаты оказанных услуг по электронной почте.

14.3. Услуги, производятся на центральном объекте системы в режиме удаленного подключения.

Исполнитель, при оказании услуг, обязан принимать организационные и технические меры по обеспечению безопасности информации, обрабатываемой в информационной системе Заказчика, предусмотренные законодательством Российской Федерации, а также установленными Заказчиком требованиями по защите информации, предъявляемые при подключении к сети ПСО и системам Заказчика. Перед получением доступа Исполнитель и Заказчик заключают соглашение о конфиденциальности (Приложение № 3 к ТЗ);

Исполнитель совместно с Заказчиком обеспечивает организацию удаленного доступа к защищенной сети передачи данных Заказчика с рабочих станции Исполнителя с использованием средств технической и криптографической защиты информации. Доступ осуществляется через терминальный сервер или систему контроля удаленного доступа привилегированных пользователей Заказчика. Исполнитель обязуется самостоятельно

приобрести необходимый перечень средств технической (далее – СЗИ) и криптографической защиты информации (далее – СКЗИ) для организации защищенного взаимодействия ViPNet Client КСЗ версии не ниже 4 после согласования данного мероприятия с Заказчиком. Использование эквивалента не допустимо в связи с имеющейся сетью криптографической защиты информации ViPNet КСЗ № 3220. Для установки и настройки СЗИ и СКЗИ Исполнитель за свой счет может привлечь организацию, имеющую действующую лицензию ФСБ, ФСТЭК России на осуществление данного вида деятельности или выполняет работы самостоятельно.

По требованию заказчика Исполнитель должен предоставить Заказчику копию документа, подтверждающего соответствие системы защиты информации подключаемых автоматизированных рабочих мест Исполнителя, установленным требованиям защиты информации для систем Заказчика.

14.4. Исполнитель для оказания услуг должен документально подтвердить наличие прав на модификацию и иное использование программного обеспечения «Мониторинг оборудования и аудит контрактов» являющимся автором, иным правообладателем, что должно быть подтверждено одним из перечисленных документов:

- документ, подтверждающий наличие у Исполнителя исключительных прав на программное обеспечение «Мониторинг оборудования и аудит контрактов»;
- лицензионный договор (лицензионное соглашение) с правообладателем, предоставляющим Исполнителю полномочия, необходимыми и достаточными для оказания услуг;
- сублицензионный договор с лицом, с которым правообладатель программного обеспечения «Мониторинг оборудования и аудит контрактов», заключил лицензионный договор и предоставил этому лицу права на использование программного обеспечения «Мониторинг оборудования и аудит контрактов» и которое, в свою очередь, предоставило соответствующие права Исполнителю в объеме, необходимом и достаточном для оказания услуг.

Соответствие требованию подтверждается предоставлением копий вышеуказанных документов.

15. Требования, предъявляемые к защите АРМ Исполнителя при проведении работ в инфраструктуре Заказчика:

15.1 Требования к защите информации АРМ, используемых при доработке/разработке функциональных возможностей компонентов ИС, а также АРМ, применяемых для организации удаленных подключений к ресурсам Заказчика, включают:

- определение правил и процедур защиты АРМ;
- реализацию мер контроля физического доступа к техническим средствам АРМ;
- обеспечение безопасной настройки системного и прикладного ПО АРМ;
- реализацию парольной защиты и авторизации;
- применение средств защиты информации.

15.2 Детальные требования по защите АРМ пользователей могут быть уточнены (усилены) по результатам определения угроз безопасности информации и проектирования систем/подсистем защиты информации конкретной ИС.

15.3 Защита АРМ должна предусматривать контроль эффективности мер и средств защиты информации. Такой контроль должен быть периодическим (не реже одного раза в год). Исполнитель должен назначить администратора безопасности, на которого должны быть возложены задачи организации работ по защите АРМ, а также контроль за соблюдением предъявляемых требований.

15.4 Минимальные общие обязанности, предъявляемые к пользователям АРМ, должны предусматривать обязанности по:

- осуществлению выполнения требований парольной защиты;
- блокированию сеансов удаленного доступа и сеансов локального использования при покидании своего АРМ;
- выполнению требований эксплуатационной документации на используемые им средства защиты информации;
- оказанию содействия в расследовании инцидентов информационной безопасности в ИС в рамках своей компетенции;
- информированию администратора безопасности в случае аппаратных или программных ошибок, сбоев в механизмах защиты информации АРМ;
- уведомлению администратора безопасности об обнаружении попыток или фактов несанкционированного доступа к информации, обнаружения инцидентов информационной безопасности.

15.5 Реализация мер контроля физического доступа к техническим средствам АРМ должна предусматривать:

- организацию контролируемой зоны, в пределах которой постоянно размещаются АРМ, обрабатывающие информацию, средства защиты информации, а также средства обеспечения функционирования АРМ;
- определение лиц, допущенных к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- размещение устройств вывода (отображения) информации (мониторов, принтеров) АРМ, исключающее ее несанкционированный просмотр;
- принятие мер, исключающих возможность несанкционированного изменения аппаратной части технических средств АРМ (например, путем опечатывания системного блока АРМ пользователя);
- применение средств доверенной загрузки (при необходимости).
- Требования по настройке системного и прикладного программного обеспечения АРМ должны предусматривать соблюдение следующих минимальных требований:
- использование только лицензионного ПО фирм-изготовителей;
- установку ПО на АРМ только с официального дистрибутива, доверенного внутреннего репозитория или репозитория в российском сегменте «Интернет»;
- установку на АРМ сертифицированных средств антивирусной защиты и средств защиты от НСД, а также реализацию запрета на возможность их отключения.

15.6 Администратор безопасности должен сконфигурировать ОС, средство защиты от НСД и средство антивирусной защиты, а также прикладное ПО и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные версии ОС и прикладного ПО;
- исключить возможность загрузки и использования ОС, отличной от штатной;

- исключить возможность неконтролируемого Администратором безопасности удаленного управления, администрирования и модификации ОС и её настроек;
- режимы безопасности, реализованные в ОС и прикладном ПО, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для выполнения должностных обязанностей права;
- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные пользователю привилегии;
- необходимо регулярно устанавливать пакеты обновлений безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС и прикладное ПО;
- необходимо использовать средство обнаружения уязвимостей, организовать регулярный анализ результатов аудита;
- организовать постоянный мониторинг и анализ событий безопасности, а также реагирование и предотвращение компьютерных атак.

15.7 На АРМ должны применяться следующие виды паролей:

- пароли BIOS/UEFI;
- пароли для входа в операционную систему и доступа к ресурсам информационных систем.

15.8 На АРМ привилегированных пользователей должны быть реализованы механизмы личной идентификации сотрудника.

15.9 Изменение аутентификационной информации (средств аутентификации), заданных их производителями или используемых при настройке ПО, должно обеспечиваться администратором безопасности.

15.10 Администратор безопасности должен организовывать или осуществлять генерацию (назначение) паролей пользователя АРМ и присвоение им персональных идентификаторов.

15.11 Для паролей пользователей АРМ (в т.ч. привилегированных) и технологических учетных записей должны быть предустановлены требования:

- длина пароля для пользователей – не менее 12 символов; для привилегированных пользователей – не менее 12 символов; для технологических учетных записей – не менее 16 символов. Для паролей должны быть реализованы механизмы проверки сложности и повторяемости, использования специальных символов, строчных и заглавных букв;
- максимальное количество неудачных попыток аутентификации (ввода неправильного пароля) до блокировки не более 15 попыток;
- в качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов;
- в качестве пароля не может быть использована комбинация символов, набираемых в закономерном порядке на клавиатуре (например, 123456, qwerty и т. П.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- в качестве пароля не должны использоваться ранее использовавшиеся пароли.

15.12 Для защищаемых АРМ должно обеспечиваться:

- применение сертифицированных средств антивирусной защиты;
- применение сертифицированных средств защиты от НСД;
- применение средств межсетевого экранирования;

- применение средств (сервисов) анализа защищенности;
- применение средств мониторинга событий информационной безопасности или альтернативные меры мониторинга информационной безопасности и реагирования на инциденты;
- применение сертифицированных средств криптографической защиты информации.

15.13 Настройка и эксплуатация средств защиты информации должна осуществляться в соответствии с эксплуатационной документацией, достаточной для выполнения требуемого класса защищенности и уровня защищенности персональных данных ИС.

15.14 Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

15.15 Средства защиты информации должны применяться с соблюдением запретов, установленных пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

15.16 Вышеуказанные требования могут быть скорректированы в соответствии с техническими условиями подключения внешних пользователей и конкретной ИС Заказчика.

15.17 По требованию Заказчика Исполнитель должен предоставить Заказчику копию документа, подтверждающего соответствие системы защиты информации подключаемых АРМ Исполнителя, установленным требованиям защиты информации для ИС Заказчика (Приложение № 4 к ТЗ).

Отчет по заявкам

к Государственному контракту № ____ от ____ г. на услуги по информационно-техническому сопровождению программного обеспечения
«Мониторинг оборудования и аудит контрактов» за период ____ 202__ г.

Номер заявки	Дата заявки	Дата закрытия заявки	Описание содержания заявки	Статус заявки (в работе, выполнена, отменена)	Комментарии к заявке

Отчет о проведении регламентных работ

к Государственному контракту № ____ от _____ г. на услуги по информационно-техническому сопровождению программного обеспечения
«Мониторинг оборудования и аудит контрактов» за период _____ 202_ г.

№	Описание	Дата выполнения				Подпись исполнителя	Примечание
1	Проверка работоспособности основного функционала и осуществление регламентных работ в рамках профилактического обслуживания информационных баз с целью предотвращения сбоев и ошибок подсистем программного обеспечения (еженедельно)						
2	Проведение регламентных работ по очистке диска (1 раз в 2 недели)						
3	Проверка работоспособности подсистем: Оперативный контроль; Картография; Инциденты; Аналитика; Модуль управленческого учета; Модуль администрирования; Справочники. (еженедельно)						

СОГЛАШЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ

№ _____

(типовая форма)

г. Южно-Сахалинск

«___» _____ 20__ г.

Государственное казенное учреждение Сахалинской области «Центр региональной цифровой трансформации» именуемое Сторона-1, руководителя учреждения Брюханова Анатолия Андреевича, действующего на основании Устава, с одной стороны, и _____, именуемое в дальнейшем Сторона-2, в лице _____, действующего на основании _____, вместе именуемые «Стороны», заключили настоящее Соглашение о конфиденциальности (далее – Соглашение) о нижеследующем:

1. Предмет соглашения:

- 1.1. Соглашение регулирует отношения, связанные с передачей и охраной конфиденциальности информации ограниченного доступа, которой Стороны будут обмениваться на всех этапах _____ (договорных отношений по государственному контракту № _____ от _____, пилотного проектам _____).
- 1.2. В рамках настоящего Соглашения Сторона, передающая информацию, именуется в дальнейшем «Передающая сторона», а Сторона, принимающая информацию, именуется в дальнейшем «Принимающая Сторона». Обе Стороны настоящего соглашения могут быть, как Передающей стороной, так и Принимающей стороной.
- 1.3. Передающая Сторона обязуется передавать по запросу Принимающей стороны в пользование Принимающей стороне информацию ограниченного доступа, а Принимающая Сторона обязуется принимать, обеспечивать её сохранность и неразглашение.

2. Термины и определения:

- 2.1. В соответствии с нормативно-правовыми актами Российской Федерации в рамках настоящего Соглашения применяются следующие термины и определения:
 - информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;
 - конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
 - персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);
 - служебная информация ограниченного распространения – один из видов информации ограниченного доступа – несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;
 - контрагент – сторона гражданско-правового договора, которой обладатель информации ограниченного доступа передал такую информацию;

- режим служебной тайны – правовые, организационные, технические и иные меры, принимаемые Стороной для обеспечения ограничения на распространение служебной информации ограниченного доступа, и на доступ к этой информации.

3. Право на отнесение сведений к информации ограниченного доступа

- 3.1. Право на отнесение сведений к информации ограниченного доступа принадлежит обладателю такой информации.
- 3.2. Не является информацией ограниченного доступа следующая информация:
 - информация, сведения или данные, носящие общеизвестный характер и являющиеся публично доступными;
 - информация, которая на дату заключения настоящего Соглашения использовалась Принимающей стороной на законном основании;
 - информация, которая на момент ее передачи Принимающей стороне не была определена Передающей стороной как информация ограниченного доступа;
 - информация, подпадающая под действие пункта 4 статьи 8 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Охрана конфиденциальности информации ограниченного доступа

- 4.1. Обладателем информации ограниченного доступа принимаются следующие меры по охране ее конфиденциальности:
 - 4.1.1. Определение перечня информации ограниченного доступа.
 - 4.1.2. Ограничение доступа к информации ограниченного доступа путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.
 - 4.1.3. Учет лиц, получивших доступ к информации ограниченного доступа и (или) лиц, которым такая информация была предоставлена или передана.
 - 4.1.4. Регулирование отношений по использованию информации ограниченного доступа работниками на основании трудовых договоров, контрагентами на основании гражданско-правовых договоров и иными организациями на основании контрактов (договоров).
- 4.2. Принимающая Сторона обязуется с момента получения информации ограниченного доступа:
 - 4.2.1. Не использовать ее полностью или частично в иных, непредусмотренных Соглашением, целях, кроме указанных в пункте 1.1. Соглашения, без получения предварительного письменного согласия Передающей Стороны.
 - 4.2.2. Сохранять и защищать полученную информации ограниченного доступа, с соблюдением требований законодательства в области защиты информации.
 - 4.2.3. Не разглашать и не способствовать прямо или косвенно разглашению третьим лицам информации ограниченного доступа.
 - 4.2.4. Не копировать информацию ограниченного доступа, не размножать, не воспроизводить, не дублировать полностью или частично, пока такое копирование, размножение, воспроизведение или дублирование не будет разрешено в письменной форме Передающей стороной.
- 4.3. После получения письменного требования Передающей Стороны, а также после окончания срока действия договорных обязательств, и в случае собственной реорганизации или ликвидации, Принимающая сторона обязана за свой счет возвратить Передающей Стороне в течение 10 (десяти) календарных дней на основании соответствующего акта приема-передачи все полученные оригиналы и копии носителей информации ограниченного доступа или уничтожить по акту все оригиналы

и копии информации ограниченного доступа, включая размноженные экземпляры, в любой форме, находящиеся в распоряжении Принимающей стороны. Один экземпляр акта об уничтожении предоставить Передающей Стороне.

- 4.4. Работниками, допускаемыми к информации ограниченного доступа и привлекаемыми к выполнению договорных обязательств, должны быть приняты обязательства о неразглашении информации ограниченного доступа (подписано соглашение о неразглашении информации ограниченного доступа). Сторона, получающая в соответствии с настоящим Соглашением информацию ограниченного доступа, гарантирует, что ее работники, получившие доступ к этой информации, приняли обязательства о неразглашении информации ограниченного доступа (подписано соглашение о неразглашении информации ограниченного доступа).
- 4.5. Не передавать третьей стороне информацию ограниченного доступа, без письменного разрешения обладателя данной информации. Стороны при передаче информации ограниченного доступа третьей стороне должны убедиться, что последней приняты меры по охране её конфиденциальности не ниже мер, установленных настоящим Соглашением.
- 4.6. Информация ограниченного доступа может быть раскрыта Принимающей стороной без согласия Передающей стороны в следующих случаях:
 - по запросу государственных органов, уполномоченных запрашивать такую информацию в соответствии с применимым законодательством, на основании должным образом оформленного запроса на предоставление указанной информации;
 - по запросу судебных органов для целей защиты и исполнения прав по настоящему Соглашению и/или иным соглашениям, заключенным между Сторонами.
- 4.6.1. Если какая-либо из Сторон получит надлежащим образом выданное административное или судебное требование предоставить Информацию другой Стороны, получатель такого требования обязан незамедлительно уведомить вторую Сторону и предложить ей защитить свои интересы от такого требования.
- 4.6.2. В случае получения надлежаще оформленного мотивированного запроса уполномоченного государственного органа, на основании которого у Принимающей стороны возникнет обязанность раскрыть информацию ограниченного доступа без получения прямо выраженного письменного согласия Передающей стороны, Принимающая сторона обязуется раскрыть исключительно ту часть информации ограниченного доступа, раскрытие которой необходимо в силу законного требования государственного органа, в пределах, допустимых в соответствии с действующим законодательством Российской Федерации.
- 4.7. Стороны обязуются не использовать для обработки и передачи информации ограниченного доступа каналы связи, не соответствующие установленным требованиям по защите информации.
5. **Особенности регулирования отношений, связанных с защитой служебной информации ограниченного распространения**
- 5.1. На материальные носители, содержащие служебную информацию ограниченного распространения, передаваемые одной Стороной другой Стороне, должна быть нанесена пометка «Для служебного пользования».
- 5.2. Каждая Сторона считает полученную от другой Стороны или иной организации служебную информацию – информацией ограниченного распространения, если на носителях информации проставлена пометка «Для служебного пользования».

- 5.3. В случае устной передачи служебной информации ограниченного распространения (с применением средств защиты информации, позволяющих обеспечить конфиденциальность передаваемой информации в соответствии с требованиями защиты информации) передающая сторона делает соответствующее сообщение.
- 5.4. Сторона, получившая служебную информацию ограниченного распространения от другой Стороны, обязуется:
- 5.4.1. Принять меры по охране ее конфиденциальности, указанные в разделе 4 настоящего Соглашения.
- 5.4.2. Сообщать ее исключительно работникам из числа граждан Российской Федерации, принявших согласно п. 4.4 Соглашения обязательства о неразглашении информации ограниченного доступа (подписавших соглашение о неразглашении информации ограниченного доступа), которым она необходима для достижения целей, определяемых договорными отношениями Сторон.
- 5.4.3. По окончании срока действия настоящего Соглашения обеспечить возврат служебной информации ограниченного распространения и зафиксированной на материальных носителях, Стороне, предоставившей указанную информацию.
- 5.5. В отношении информации с пометкой «Для служебного пользования», ее материальных носителей и устной передачи такой информации от одной Стороны другой Стороне действует режим служебной тайны.
- 5.6. Обязательства Сторон о неразглашении служебной информации ограниченного распространения, действуют в течение срока ее нахождения в режиме служебной тайны.
- 5.7. В случае своей реорганизации Стороны примут меры по охране служебной информации ограниченного распространения не ниже мер, установленных настоящим Соглашением.
- 5.8. В случае ликвидации Стороны, она обязана в согласованный Сторонами срок до своей ликвидации обеспечить возврат служебной информации ограниченного распространения, зафиксированной на материальных носителях, Стороне, предоставившей указанную информацию.

6. Передача информации ограниченного доступа

- 6.1. Передача информации ограниченного доступа осуществляется:
- почтовыми отправлениями с уведомлением о вручении;
 - нарочным;
 - посредством защищенного удаленного подключения с использованием ViPNet Client;
 - в устной форме.
- 6.1.1. При передаче информации ограниченного доступа почтовыми отправлениями с уведомлением о вручении с вложением вышеуказанной Информации, зафиксированной на машинном и/или бумажном носителе, Передающая Сторона включает в почтовое отправление опись вложения, в которой указывается тип носителя и состав передаваемой информации ограниченного доступа. Если Принимающая Сторона не направит Передающей стороне уведомление об отсутствии в почтовом отправлении вложения или несоответствии вложения описи, Информация считается полученной почтовым отправлением с момента получения Передающей Стороной уведомления о вручении почтового отправления.
- 6.1.2. При передаче информации ограниченного доступа на машинном и/или бумажном носителе посредством почтового отправления, фельдъегерской связью, либо с нарочным, Передающая Сторона оформляет в своей части Акт приема-передачи по

форме соответствующего приложения к Соглашению (Приложение № 1). Принимающая Сторона при получении информации ограниченного доступа заполняет и подписывает Акт приема-передачи в своей части и отправляет его Передающей Стороне (почтовым отправлением с уведомлением о вручении, либо с нарочным) не позднее 5 календарных дней с даты получения. В случае неполучения Передающей Стороной подписанного Акта приема-передачи от Принимающей Стороны в течение вышеуказанного срока, Акт считается подписанным Принимающей Стороной.

- 6.1.3. При передаче информации ограниченного доступа в устной форме (с применением средств защиты информации, позволяющих обеспечить конфиденциальность передаваемой информации в соответствии с требованиями защиты информации) Передающая Сторона уведомляет Принимающую Сторону о том, что передаваемые в устной форме сведения и/или данные являются информацией ограниченного доступа. Передающая Сторона обеспечивает подготовку документа по переданной в устной форме информации ограниченного доступа в форме протокола совещания, переговоров, записи бесед, памятной записки и т.п., который подписывают обе Стороны. Передающая Сторона устанавливает в отношении данного документа требование об отнесении сведений к информации ограниченного доступа и осуществляет передачу документа в кратчайшие сроки Принимающей Стороне. Информация ограниченного доступа считается полученной с момента передачи ее в устной форме (при условии наличия подписанного с двустороннего подтверждения получения информации в устной форме).
- 6.2. Передача информации ограниченного доступа по открытым каналам телефонной, телеграфной и факсимильной связи, а также с использованием сети «Интернет» без соответствующих средств защиты (ViPNet Client) в соответствии с действующим законодательством, запрещена.
- 6.3. Раскрытие и/или передача информации ограниченного доступа в соответствии с Соглашением **не означает** предоставление Принимающей Стороне каких-либо прав (полностью или в их части) в отношении раскрытой/переданной информации ограниченного доступа, в том числе, прав на изобретения, открытия в ноу-хау, авторских прав, прав на товарные знаки, словесные обозначения, торговые и технологические секреты, принадлежащие Передающей Стороне.
- 6.4. Относительно любого обмена информацией ограниченного доступа, который может происходить между Сторонами в рамках Соглашения, Сторонами принято и согласовано, что нижеперечисленные сотрудники каждой из Сторон являются уполномоченными лицами, которым разрешено принимать и/или передавать информацию ограниченного доступа от имени соответствующей Стороны:

От имени организации _____

- ФИО, электронная почта;
- ФИО, электронная почта.

От имени организации _____

- ФИО, электронная почта;
- ФИО, электронная почта.

- 6.5. Вся корреспонденция и переписка между Сторонами в соответствии с Соглашением, либо в связи с ним, а также все сопутствующие документы, в том числе Акты приема-передачи, направляемые Сторонами друг другу, должны быть совершены в письменной

форме и переданы почтовым отправлением с уведомлением о вручении, либо доставлены нарочным по следующим адресам:

ГКУ СО «ЦРЦТ»

Место нахождения: 693020, г. Южно-Сахалинск, ул. Комсомольская, 125

Почтовый адрес: 693020, г. Южно-Сахалинск, ул. Комсомольская, 125

ОГРН 1116501000770

ИНН 6501233462

КПП 650101001

Приемная: 8 (4242) 67 21 00

Адрес электронной почты: cit@sakhalin.gov.ru

Адрес местонахождения: _____

Почтовый адрес: _____

e-mail: _____

ИНН: _____

КПП: _____

ОГРН: _____

- 6.6. При передаче информации ограниченного доступа, не относящейся к служебной информации ограниченного распространения, Передающая Сторона обязана осуществить её классификацию в соответствии с Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» и сообщить Принимающей стороне особенности правовой охраны данной такой информации.
- 6.7. При передаче **персональных данных** Передающая Сторона обязана осуществить такую передачу с оформлением поручения на обработку персональных данных в соответствии с требованиями части 3 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 30.12.2020) «О персональных данных».
- 6.8. Риски ненадлежащего оформления Информации, в соответствии с требованиями настоящего раздела Соглашения, несет Передающая Сторона.
- 7. Разглашение информации:**
- 7.1. Под разглашением информации ограниченного доступа понимается действие или бездействие, в результате которого информация ограниченного доступа в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданско-правовому договору.
- 7.2. При утрате, разглашении или подозрении на разглашение информации ограниченного доступа, Стороны обязуются незамедлительно информировать друг друга и принять все необходимые меры по предотвращению дальнейшего разглашения ограниченного доступа, а также выявлению причинённого ущерба или иных отрицательных последствий, вызванных ее утратой или разглашением.
- 7.3. Принимающая Сторона не несет никаких обязательств или ограничений относительно любой Информации в случае, когда может доказать, что:
- информация ограниченного доступа стала общественным достоянием до ее раскрытия Принимающей Стороной;

- информация ограниченного доступа была передана с нарушением требований раздела 5 и 6 настоящего Соглашения.
- информация ограниченного доступа в течение действия Соглашения или до истечения, указанного в п.9.1 Соглашения срока, стала общеизвестной и публичной иначе, чем в результате нарушения Соглашения;
- информация ограниченного доступа уже была известна Принимающей Стороне, о чем свидетельствует соответствующий письменный документ в архиве Принимающей Стороны;
- информация ограниченного доступа была независимо добросовестно разработана сотрудниками Принимающей Стороны, не имевшими доступа к такой Информации;
- информация ограниченного доступа одобрена для раскрытия третьим лицам посредством ясно выраженного письменного разрешения Передающей Стороны.

8. Ответственность:

- 8.1. Принимающая Сторона, допустившая разглашение Информации, при условии предоставления Передающей Стороной доказательств вины Принимающей Стороны, обязана компенсировать в полном объеме весь действительный ущерб, причиненный Передающей Стороне таким разглашением.
 - 8.1.1. Принимающая Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации за разглашение информации ограниченного доступа, то есть за свои действия или бездействие, в результате которых информация ограниченного доступа становится известной Третьим лицам в нарушение условий настоящего Соглашения. Ответственность Принимающей стороны ограничивается размером реального документально подтвержденного ущерба, понесенного Передающей стороной в результате виновных действий Принимающей стороны.
- 8.2. Все разногласия и споры, возникающие при исполнении Соглашения или в связи с ним, Стороны будут решать путем проведения переговоров. В случае не достижения согласия, споры будут передаваться на рассмотрение в Арбитражный суд г. Южно-Сахалинска.

9. Срок действия:

- 9.1. Соглашение вступает в силу с даты его подписания Сторонами и действует в течении действия договорных отношений сторон по *государственному контракту (договору, реализации пилотного проекта)* №_____ от _____ /до _____., при этом ни одна из сторон не в праве разглашать информацию ограниченного доступа сторон после окончания действия настоящего Соглашения, до тех пор, пока такое разглашение не будет разрешено в письменной форме Передающей стороной.
- 9.2. Во всем остальном, что не предусмотрено условиями Соглашения, Стороны будут руководствоваться действующим законодательством Российской Федерации.
- 9.3. Ни одна из Сторон не вправе передавать свои права и обязанности по Соглашению третьим лицам без письменного согласия на это другой Стороны.
 - 9.3.1. В случаях реорганизации Принимающей стороны, последняя обязуется не позднее чем за 60 (шестьдесят) календарных дней уведомить о предстоящей реорганизации Передающую сторону.
 - 9.3.2. Права и обязанности Сторон по настоящему Соглашению в случае реорганизации какой-либо из Сторон переходят к соответствующему правопреемнику (правопреемникам) реорганизованной Стороны, и такие правопреемники будут нести все права и обязанности по настоящему Соглашению в отношении другой Стороны.

- 9.3.3. В случае ликвидации Принимающей стороны, она обязана до завершения ликвидации вернуть Передающей стороне все оригиналы и копии (или обеспечить уничтожение копий) всех материальных носителей с информацией ограниченного доступа, переданной по настоящему Соглашению.
- 9.4. Любые изменения и дополнения к Соглашению действительны, только если они составлены в письменной форме и подписаны уполномоченными представителями обеих Сторон.
- 9.5. Соглашение подписано в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из сторон.

10. Реквизиты и подписи сторон:

Адрес
местонахождения _____
Почтовый адрес:

e-mail: _____
Тел.: _____
ИНН: _____
КПП: _____
ОГРН: _____

_____/ ФИО
М.П.

Государственное казенное учреждение
Сахалинской области «Центр
региональной цифровой
трансформации» (ГКУ СО «ЦРЦТ»)
Юридический (почтовый) адрес:
693020, г. Южно-Сахалинск, ул.
Комсомольская, 125
ИНН/КПП 6501233462 / 650101001
ОГРН 1116501000770
Тел.: (4242) 67 21 00
Факс: (4242) 67 21 97
cit@sakhalin.gov.ru

_____/ А.А. Брюханов
М.П.

УТВЕРЖДАЮ

Руководитель подключаемого учреждения

ФИО

« »

2026 г.

М.П.

АКТ

настройки средств защиты на автоматизированном рабочем месте, подключаемом к информационно-телекоммуникационной инфраструктуре ГКУ СО «ЦРЦТ»

Настоящий акт составлен по результатам установки и настройки средств защиты информации (далее – СЗИ) криптографических средств защиты информации (далее – СКЗИ) на автоматизированном рабочем месте (далее – АРМ), подключаемом к информационно-телекоммуникационной инфраструктуре ГКУ СО «ЦРЦТ» были проведены работы по установке, настройке и проверки СЗИ и СКЗИ (далее – СрЗИ) в составе, отраженном в таблице № 2. Данные об АРМ, на котором произведена установка и настройка СрЗИ отражены в Таблице №1).

1. По окончании установки была проведена проверка работоспособности систем, а также основных защитных функций СрЗИ и реализованных механизмов защиты. По результатам проверки замечания к работоспособности систем, с установленными СрЗИ и их настроек выявлены не были.

2. Настройки осуществлены в соответствии с эксплуатационной документацией на СрЗИ и требованиями руководящих документов в области защиты информации.

3. Все СрЗИ имеют следующую комплектацию:

- копия сертификата соответствия ФСБ России/ФСТЭК России;
- руководство пользователя;
- верифицированный дистрибутив;
- формуляр.

Наименование подключаемых АРМ:

Таблица №1

Наименование АРМ	Учетный (инвентарный) номер	ФИО работника	Должность работника

Состав СрЗИ:

Таблица №2

Тип СрЗИ	Наименование	Версия	Дата установки и настройки	Серийный номер (СЗЗ)	Сертификат соответствия ФСТЭК России (ФСБ России)
АРМ № ____					
Средство защиты					

<i>информации от несанкционированного доступа со средством межсетевого экранирования</i>					
<i>Средство антивирусной защиты</i>					
<i>Средство криптографической защиты информации</i>					

Ответственный за обеспечение защиты подключаемых АРМ _____ ФИО