**Частное учреждение здравоохранения**

**«Клиническая больница «РЖД-Медицина» города Пермь»**

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**на оказание услуг по предоставлению неисключительных прав и сертификатов активации сервиса технической поддержки средств криптографической защиты информации и средств защиты информации для организации доступа**

**к Единой информационной системе здравоохранения Пермского края**

№ закупки: 25130209059 (согласно плана-графика закупок на 2025 год)

Пермь

2024

Содержание

[1 Общие сведения 3](#_Toc178844869)

[1.1 Полное наименование услуг 3](#_Toc178844870)

[1.2 Полное наименование системы 3](#_Toc178844871)

[1.3 Сокращенное обозначение системы 3](#_Toc178844872)

[1.4 Заказчик 3](#_Toc178844873)

[1.5 Перечень документов, на основании которых и в соответствии с которыми оказываются услуги 3](#_Toc178844874)

[1.6 Место оказания услуг 3](#_Toc178844875)

[1.7 Сроки оказания услуг 3](#_Toc178844876)

[1.8 Перечень сокращений 3](#_Toc178844877)

[2 Цель и назначение услуг 4](#_Toc178844878)

[3 Характеристики ЕИСЗ ПК 4](#_Toc178844879)

[4 Требования к поставляемым средствам защиты информации и средствам криптографической защиты информации 6](#_Toc178844880)

[4.1 Общие требования 6](#_Toc178844881)

[4.2 Требования к средствам криптографической защиты информации, передаваемой по каналам связи 6](#_Toc178844882)

[**4.2.1** **Общие требования** 6](#_Toc178844883)

[**4.2.2** **Требования к клиентскому программному обеспечению средств криптографической защиты информации ЕИСЗ ПК** 6](#_Toc178844884)

[4.3 Требования к средствам защиты информации от несанкционированного доступа 7](#_Toc178844885)

[**4.3.1** **Общие требования** 7](#_Toc178844886)

[**4.3.2** **Требования к функциональности СЗИ от НСД** 8](#_Toc178844887)

[5 Этапы и сроки оказания услуг 11](#_Toc178844888)

[6 Требования к Исполнителю 11](#_Toc178844889)

[7 Требования к патентной чистоте 12](#_Toc178844890)

[8 Техническая поддержка от Исполнителя 12](#_Toc178844891)

# Общие сведения

## Полное наименование услуг

Оказание услуг по предоставлению неисключительных прав и сертификатов активации сервиса технической поддержки средств криптографической защиты информации и средств защиты информации для организации доступа к Единой информационной системе здравоохранения Пермского края.

## Полное наименование системы

Полное наименование системы – Единая информационная система здравоохранения Пермского края.

## Сокращенное обозначение системы

Сокращенное обозначение системы – ЕИСЗ ПК.

## Заказчик

Наименование заказчика – ЧУЗ КБ «РЖД-Медицина» г. Пермь.

## Перечень документов, на основании которых и в соответствии с которыми оказываются услуги

* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Федеральный закон Российской Федерации от 27 июля 2006 г.
 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
* Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд;
* Приказ Министерства здравоохранения Российской Федерации от 24 декабря 2018 г. № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций»;
* Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

## Место оказания услуг

Передача Заказчику неисключительных прав и технической документации на СЗИ и СКЗИ, сертифицированных комплектов с верифицированным программным обеспечением СЗИ и СКЗИ, сертификатов технической поддержки на СЗИ и СКЗИ осуществляется силами Исполнителя по адресу: г. Пермь, ул. Василия Каменского, д.1.

## Сроки оказания услуг

В соответствии с Таблицей 3 настоящего технического задания.

## Перечень сокращений

АРМ – Автоматизированное рабочее место

ЕИСЗ ПК – Единая информационная система здравоохранения Пермского края

МО – Медицинская организация

НСД – Несанкционированный доступ

ОМС – Обязательное медицинское страхование

РФ – Российская Федерация

СЗИ – Средство защиты информации

СКЗИ – средство криптографической защиты информации

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

ФСБ России – Федеральная служба безопасности

# Цель и назначение услуг

Целью оказания услуг является обеспечение защиты информации при работе
в Единой информационной системе здравоохранения Пермского края с автоматизированных рабочих мест пользователей.

Для достижения указанной цели должны быть оказаны следующие услуги:

* поставка программных и программно-аппаратных СЗИ и СКЗИ для автоматизированных рабочих мест;
* организация технической поддержки СЗИ и СКЗИ.

# Характеристики ЕИСЗ ПК

ЕИСЗ ПК создана и эксплуатируется в соответствии с приказом Министерства здравоохранения Пермского края от 23.09.2016 г. № СЭД-34-01-06-736 «Об утверждении Положения о ЕИСЗ ПК», приказом Министерства здравоохранения Пермского края от 26.07.2018 № СЭД-34-01-06-634 «О внесении изменений в приказ Министерства здравоохранения Пермского края от 23.09.2016 г. №СЭД-34-01-06-736».

Защищенная сеть для подключения к ЕИСЗ ПК построена на базе СКЗИ «ViPNet» (номер сети - 13123).

ЕИСЗ ПК используется для реализации следующих основных задач:

* централизованное предоставление населению и организациям государственных услуг в сфере здравоохранения через единый портал государственных услуг;
* автоматизация процесса сбора, хранения и анализа данных о случаях оказания медицинской помощи гражданам;
* формирование и поддержка актуальности единого банка данных случаев оказания медицинской помощи и паспортов МО;
* ведение единой электронной медицинской карты гражданина;
* ведение специализированных регистров по заболеваниям и карт диспансерного наблюдения;
* автоматизация учетной и отчетной медицинской деятельности МО, органа управления здравоохранением региона;
* информационно-технологическая поддержка системы финансирования МО
в системе ОМС региона за фактически оказанную медицинскую помощь на основании персонифицированных реестров;
* поддержка информационного обмена в системе обеспечения лекарственными препаратами, изделиями медицинского назначения и специализированными продуктами лечебного питания при амбулаторном лечении за счет средств федерального бюджета и бюджета Пермского края;
* ведение реестра льготных категорий граждан, имеющих право на меры социальной поддержки в лекарственном обеспечении за счет средств бюджета Пермского края;
* учет движения лекарственных препаратов, изделий медицинского назначения и специализированных продуктов лечебного питания по программам обеспечения необходимыми лекарственными средствами, регионального лекарственного обеспечения и семи высокозатратных нозологий;
* организация, мониторинг и управление потоками пациентов при оказании плановой и экстренной медицинской помощи населению;
* мониторинг деятельности системы здравоохранения Пермского края и состояния здоровья граждан в Пермском крае;
* автоматизированный контроль качества и доступности оказания медицинской помощи;
* централизованное предоставление населению и организациям государственных услуг в сфере здравоохранения по принципу «единого окна»;
* обмен информацией с другими информационными системами;
* мониторинг диспансеризации определенной категории граждан взрослого населения и медицинских осмотров несовершеннолетних.

Пользователями ЕИСЗ ПК являются:

* сотрудники Министерства здравоохранения Пермского края и подведомственных ему организаций.

# Требования к поставляемым средствам защиты информации и средствам криптографической защиты информации

## Общие требования

Для обеспечения защиты информации, содержащейся в ЕИСЗ ПК, должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» и в соответствии с порядком, установленным нормативными документами ФСТЭК России и ФСБ России соответственно, указанными в п. 1.5 настоящего технического задания.

## Требования к средствам криптографической защиты информации, передаваемой по каналам связи

### **Общие требования**

Исполнитель должен поставить сертифицированные версии программного обеспечения, лицензии в соответствии с требованиями к комплектации в виртуальную защищенную сеть ViPNet № 13123, созданную для ЕИСЗ ПК.

Требования к комплектации представлены в Таблица 1.

Таблица 1 – Комплектация средств криптографической защиты информации ЕИСЗ ПК

| **Наименование** | **Кол-во** |
| --- | --- |
| Право на использование клиентского программного обеспечения ViPNet Client на ОС Windows на 13 АРМ (бессрочная лицензия) | 1 |
| Дистрибутив программно-аппаратного комплекса ViPNet Coordinator, включающий в себя: сертифицированную версию программного обеспечения, формуляр на программное обеспечение | 1 |
| Сертификат активации сервиса совместной расширенной технической поддержки производителя программного обеспечения ViPNet Client (47 шт.) и программно-аппаратного комплекса ViPNet Coordinator на срок 1 год | 1 |

### **Требования к клиентскому программному обеспечению средств криптографической защиты информации ЕИСЗ ПК**

В качестве клиентского программного обеспечения средств криптографической защиты информации ЕИСЗ ПК, устанавливаемого на АРМ пользователей, должен использоваться программный комплекс, отвечающий следующим требованиям:

* должен быть полностью совместим с ПК управления виртуальной защищенной сетью ЕИСЗ ПК в части:
1. обновления ПО;
2. автоматического обновления справочной и ключевой информации виртуальной защищенной сети ЕИСЗ ПК;
3. управления политиками безопасности;
* должен быть полностью совместим с программно-аппаратным шлюзом безопасности, предназначенным для защиты ЕИСЗ ПК, размещенных в сегменте ЦОД;
* поддерживать прозрачную работу через различные NAT-устройства;
* обеспечивать безопасную передачу (прием) данных шлюзам безопасности и клиентам (точка-точка) с использованием произвольной телекоммуникационной инфраструктуры IP-сетей, включая сети связи общего пользования;
* содержать драйвер сетевой защиты, непосредственно взаимодействующий с драйвером сетевого интерфейса и осуществляющий контроль, и фильтрацию сетевого трафика;
* содержать сервис управления драйвером сетевой защиты, обеспечивающий функционирование узла в защищенной сети, а именно загрузку в драйвер защиты правил фильтрации, справочной информации о структуре защищенной сети и ключей шифрования, сведений о сетевых параметрах доступа для узлов защищенной сети, передачу в клиентское программное обеспечение результатов обработки IP-пакетов;
* содержать драйвер шифрования IP-пакетов, осуществляющий шифрование и имитозащиту сетевого трафика на ключах, созданных в ПК управления виртуальной защищенной сети ЕИСЗ ПК;
* обеспечивать конфиденциальность, целостность и аутентификацию каждого IP-пакета;
* обеспечивать настройки сетевых фильтров, параметров доступа к узлам сети и аудита событий;
* содержать приложение, осуществляющее настройку фильтров, подготовку необходимых фильтров и ключевой информации для загрузки в драйвере, аудит основных событий, ограничение интерфейса пользователя и администратора в клиентском программном обеспечении, а также установку соответствующих фильтров IP-трафика в дополнение к собственным настроенным правилам фильтрации трафика;
* содержать систему обновления, обеспечивающую обновление ключевой и справочной информации, а также клиентского программного обеспечения;
* содержать сервис регистрации пользователя, обеспечивающий обработку событий аутентификации пользователя;
* содержать службу контроля приложений, осуществляющую контроль сетевой активности приложений и позволяющую реализовывать политики доступа приложений в сеть;
* содержать ПО для обмена зашифрованными и подписанными сообщениями;
* содержать модуль, реализующий обмен управляющей, адресной и ключевой информацией с программным обеспечением централизованного управления защищенной сетью, отправку, прием и маршрутизацию электронных документов (почтовых конвертов);
* содержать программу, осуществляющую первичную установку справочно-ключевой информации, сформированной в центре управления защищенной сетью;
* осуществлять функции персонального межсетевого экрана, обеспечивающие:
1. контроль сетевого трафика, проходящего через сетевые интерфейсы;
2. фильтрацию IP-пакетов по заданным правилам для зашифрованного и открытого сетевых трафиков по совокупности критериев (IP-адреса, протоколы, порты);
3. реализацию режима инициативных соединений;
* иметь в своем составе ПО для осуществления защищенных почтовых услуг с возможностями аутентификации отправителя и получателя, квитирования (доставлено, прочитано), электронной подписи (далее – ЭП);
* автоматически обрабатывать обновления, полученные из средств управления виртуальной защищенной сетью ЕИСЗ ПК;
* должен функционировать под управлением следующих ОС:
1. Windows 8.1 (32/64-разрядная);
2. Windows 10 (32/64-разрядная);
* обеспечивать шифрование IP-трафика, файлов и почтовых сообщений в режиме программирования с обратной связью, а также имитозащиту информации в соответствии с ГОСТ 28147-89;
* должен соответствовать требованиям документов «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016);
* должен соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3.

## Требования к средствам защиты информации от несанкционированного доступа

### **Общие требования**

Средство защиты информации от НСД для конечных точек должно осуществлять:

* защиту рабочих станций от НСД;
* контроль входа пользователей в систему, в том числе
с возможностью использования дополнительных аппаратных средств защиты;
* разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
* разграничение доступа пользователей к информации.

Требования к комплектации представлены таблице 2:

Таблица 2– Комплектация средств защиты информации от НСД

| **Наименование** | **Кол-во** |
| --- | --- |
| Право на использование модуля защиты от НСД и контроля устройств средства защиты информации на ОС Windows на 142 АРМ (на срок 1 год) | 1 |
| Сертификат активации сервиса совместной стандартной технической поддержки производителя программного обеспечения модуль защиты от НСД и контроля устройств средства защиты информации на ОС Windows на 142 АРМ (на срок 1 год) | 1 |

### **Требования к функциональности СЗИ от НСД**

СЗИ должно выполнять следующие функции по защите информации:

* Контроль входа пользователей в систему и работа пользователей в системе:
1. проверка пароля пользователя при входе в систему;
2. поддержка аппаратных средств аутентификации;
3. возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;
4. возможность блокирования входа в систему локальных пользователей;
5. возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
6. возможность блокировки сеанса работы пользователя по истечении интервала неактивности;
7. возможность управления политикой сложности паролей;
8. поддержка возможности входа в систему по сертификатам;
9. возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.
* Избирательное (дискреционное) управление доступом:
1. возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
2. возможность наследования прав доступа для файлов, каталогов и устройств;
3. возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту.
* Контроль аппаратной конфигурации компьютера и подключаемых устройств:
1. Должны контролироваться следующие устройства:
2. последовательные и параллельные порты;
3. локальные устройства;
4. сменные, физические и оптические диски;
5. программно-реализованные диски;
6. USB-устройства;
7. PCMCIA-устройства;
8. IEEE1394 (FireWire)-устройства;
9. устройства, подключаемые по шине Secure Digital.
10. Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.
11. Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации.
12. Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации:
13. должна быть возможность поиска по именам файлов, сохраненных в хранилище теневых копий;
14. должна быть возможность поиска по содержимому файлов, сохраненных в хранилище теневых копий. Должна обеспечиваться поддержка форматов, поддерживаемых компонентом Windows Search.
* Контроль сетевых интерфейсов:

Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).

Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя.

* Контроль целостности файлов, каталогов, элементов системного реестра:
1. Должна быть возможность проведения контроля целостности до загрузки операционной системы (при применении с аппаратными средствами доверенной загрузки), в процессе загрузки ОС, в фоновом режиме при работе пользователя.
2. Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.
3. Должна быть возможность восстановления исходного состояния контролируемого объекта.
4. Должна быть возможность контроля исполняемых файлов по встроенной ЭП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭП.
5. При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.
* Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей.
* Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации.
* Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию.
* Функциональный контроль ключевых компонентов системы.
* Регистрация событий безопасности в журнале.
1. Должна быть возможность формирования отчетов по результатам аудита.
2. Должна быть возможность поиска и фильтрации при работе с данными аудита.
* Получение отчета по параметрам системы защиты.
* Контроль за использованием ПО:
	1. Должна быть возможность ограничения использования ПО на компьютере.
	2. Должна быть возможность ограничения использования скриптов Active Scripts на компьютере.
	3. Должна быть возможность проверки неизменности разрешенных к запуску модулей перед их запуском.
* Контроль печати:
	1. Должна быть возможность ограничения категорий конфиденциальности документов, выводимых на печать.
	2. Должна быть возможность ограничения пользователей, допущенных к печати конфиденциальной информации.
	3. Должна быть возможность маркировки напечатанных документов.
	4. Должна быть возможность установки отдельных маркеров для первой, последней страницы и оборота последней страницы.

СЗИ от НСД должно иметь возможность функционирования совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей.

Требования к операционной платформе и аппаратной части:

* СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):
1. Windows 10;
2. Windows 8.1;
* Должна быть возможность установки СЗИ по произвольному пути;
* Должна быть возможность автоматического создания точки восстановления ОС MS Windows перед установкой СЗИ;
* СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory;
* СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ;
* СЗИ не должно требовать при развертывании модификации топологии локальной вычислительной сети;
* Обновление СЗИ должно выполняться в защищенном режиме вне сессии пользователя;
* СЗИ должно иметь в составе дистрибутива драйвера для поддержки аппаратных идентификаторов.

СЗИ должно соответствовать требованиям руководящих документов по 4 уровню доверия, 5 классу защищенности СВТ, 4 классу защиты СКН (ИТ.СКН.П4.ПЗ).

СЗИ должно допускать использование в следующих информационных системах:

* государственные информационные системы – до 2 класса защищенности (включительно);
* информационные системы персональных данных – до 2 уровня защищенности персональных данных (включительно).

# Этапы и сроки оказания услуг

Периоды и сроки поставки СЗИ и СКЗИ указаны в таблице 3.

Таблица 3 – Сроки поставки СЗИ и СКЗИ

| **№****этапа** | **Наименование**  | **Наименование периода** | **Отчетная документация** | **Срок**  |
| --- | --- | --- | --- | --- |
| 1 | Поставка СЗИ и СКЗИ | Поставка СЗИ и СКЗИ в соответствии с разделом 4 настоящего ТЗ | - Сертификаты технической поддержки для СЗИ и СКЗИ (1 год) | В течении 60 (шестидесяти) календарных дней с даты заключения договора |

# Требования к Исполнителю

Исполнитель должен обладать лицензией, подтверждающей его квалификацию и возможность обеспечить требуемое качество при оказании услуг:

* действующей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации, выданной после вступления в силу постановления Правительства Российской Федерации от 03.02 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации», включающей следующие виды работ (услуг):

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

е) услуги по установке, монтажу, наладке, испытаниям средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

* действующей лицензией ФСБ России, выданной уполномоченным органом государственной власти на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), включающей в себя пункт 12, 20, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, утвержденного Постановлением Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

# Требования к патентной чистоте

Поставляемые при выполнении требований настоящего технического задания СЗИ и СКЗИ должны иметь соответствующие лицензии на их использование и иметь сертификаты ФСТЭК России и\или ФСБ России, подтверждающие соответствие СЗИ и СКЗИ заданному функционалу.

Все передаваемые права на СЗИ и СКЗИ должны соответствовать требованиям к составу, количеству и характеристикам, необходимым для эксплуатации поставляемых в рамках настоящего технического задания СЗИ и СКЗИ. Объем передаваемых прав должен обеспечивать возможность использования Заказчиком СЗИ и СКЗИ в соответствии с Техническим заданием.

# Техническая поддержка от Исполнителя

Срок оказания технической поддержки Исполнителем - в течение 1 года с момента подписания акта, выраженный в форме универсального передаточного документа, рекомендованного письмом Федеральной налоговой службы от 21 октября 2013 № ММВ-20-3/96@ (далее – УПД).

В техническую поддержку Исполнителя включены следующие услуги:

* приём от Заказчика обращений и консультирование по электронной почте (security@center-ris.ru) и телефону (+7 (342) 254-04-16 (доб.11)) с 09:00 ч. до 18:00 ч. по местному времени Исполнителя по вопросам функционирования установленных в рамках настоящего Договора СЗИ;
* в случае необходимости: переустановка, в том числе на другое АРМ, и наладка установленных в рамках настоящего технического задания СЗИ посредством доступа к АРМ с помощью программы удаленной техподдержки. Выезд специалиста Исполнителя до места нахождения Заказчика не осуществляется.

Техническая поддержка не является гарантийным обязательством на поставляемое СЗИ. Гарантийные обязательства на поставляемые СЗИ несет производитель СЗИ.

Сроки решения неисправностей в работоспособности СЗИ и/или СКЗИ, выявленные Заказчиком в ходе эксплуатации - 8 часов с момента обращения.