УТВЕРЖДЕН
Приказом
Министерства здравоохранения
Республики Татарстан
от «20» 12 2024 года №2902

РЕГЛАМЕНТ

подключения медицинских организаций частной формы собственности к государственной информационной системев сфере здравоохранения Республики Татарстан

1 Аннотация

1.1 Настоящий Регламент определяет требования, условия и порядок подключения медицинских организаций частной формы собственности (далее - Пользователь) к государственной информационной системе в сфере здравоохранения Республики Татарстан (ГИСЗ РТ).

2 Общие положения

2.1 Для организации защищенного соединения Пользователей с ГИСЗ РТ применяется технология виртуальных частных сетей (далее - VPN) сиспользованием сертифицированных ФСТЭК России и ФСБ России средств криптографической защиты информации «ЗАСТАВА-клиент ««VPN/FW «ЗАСТАВА, версия 6» (производитель компания АО "ЭЛВИС-ПЛЮС" (Россия)).

2.2 При разработке настоящего регламента использовались следующие нормативные правовые акты, нормативно-технические документы и методические материалы:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 09.02.2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения»;
- Постановление Правительства Российской Федерации от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- Постановление Правительства РФ от 06.07.2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Кабинета Министров Республики Татарстан от 11.05.2022 № 431 «Об утверждении Положения о государственной информационной системе

Республики Татарстан «Электронное здравоохранение Республики Татарстан»;

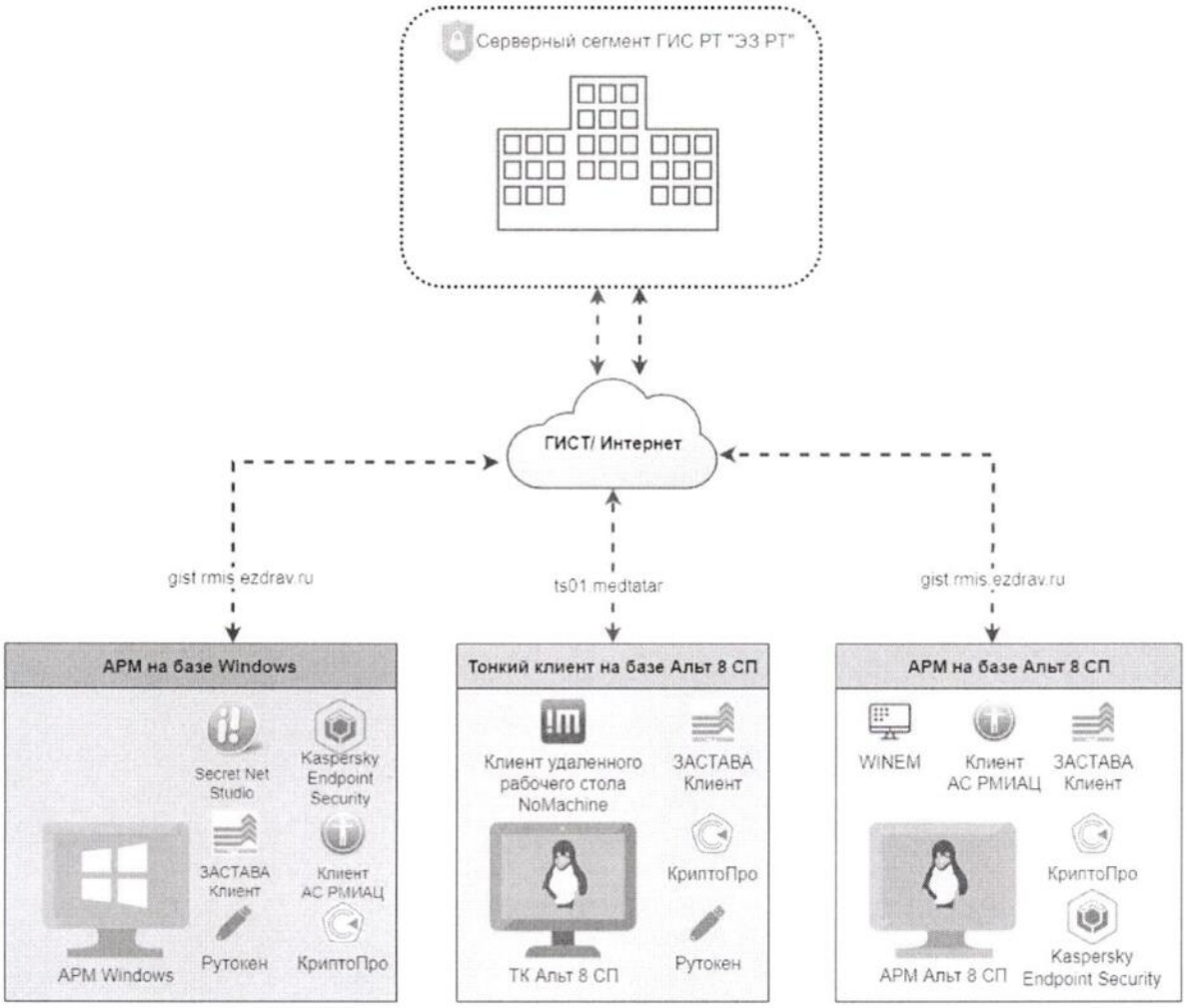
- нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30 августа 2002 года № 282;
- приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСБ России от 10 июля 2014 года № 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»;
- приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- приказ ФСТЭК России от 29 апреля 2021 года № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
- Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении 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»;
- Национальный проект «Здравоохранение», утвержденный 24.12.2018 г. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам;
- Приказ Минздрава России от 24.12.2018 г. №911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам и информационным системам фармацевтических организаций»;
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»;

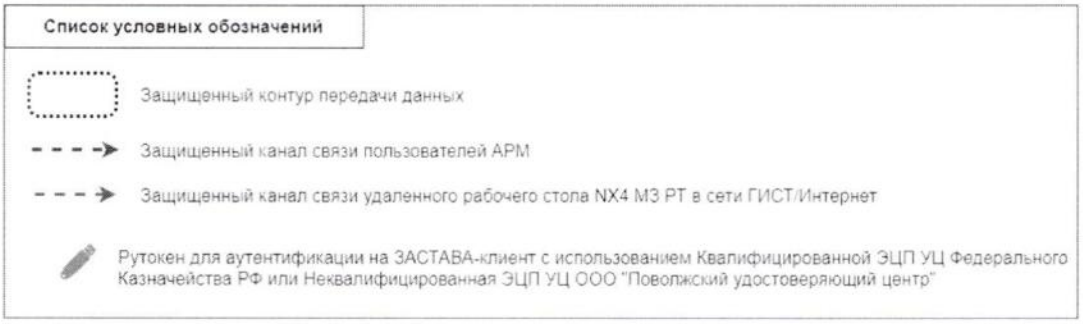
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

2.3 Подключение Пользователей к ГИСЗ РТ должно выполняться в соответствии с:

- требованиями нормативных правовых актов Российской Федерации в области защиты информации;
- требованиями нормативно-технических и методических документов в области обеспечения безопасности информации (ФСТЭК России, ФСБ России);

2.4 Схема подключения должна быть согласована с ГАУЗ «РМИАЦ» (Оператором ГИСЗ РТ) до начала выполнения работ по подключению Пользователей к ГИСЗ РТ.





3 Требования к реализации защищенного взаимодействия

3.1 Для обеспечения защиты информации при подключении Пользователей кГИСЗ РТ должны выполняться требования к системе защиты информации (далее - СЗИ) согласно приказу ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также организационные и технические мероприятия по требованиям документов, указанных в п. 1.2 настоящего Регламента.

3.2 Для проведения работ по монтажу и установке средств защиты информации (далее – СрЗИ) на объектах Пользователей ГИСЗ РТ, подключению

СрЗИ и технических средств, обеспечения их интеграции в информационную систему, а также для установки и настройки СКЗИ в соответствии со ст. 12 Федерального закона от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности» Пользователи ГИСЗ РТ могут привлечь Организацию, имеющую:

- лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа средств защиты информации;
- лицензию ФСБ России 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 сиспользованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

3.3 После выполнения указанных выше работ, должны быть проведены мероприятия по аттестации информационной системы Пользователя ГИСЗ РТ требованиям по безопасности информации, согласно Приказу ФСТЭК России от 29 апреля 2021 года № 77 «Об утверждении Порядка организации и проведения работпо аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», или должны быть проведены работы по оценке эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных с привлечением на договорной основе юридических лиц или индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4 Требования к видам обеспечения

4.1 Требования к средствам защиты информации и программному обеспечению.

Для медицинских организаций обязательно выполнение требований по

обеспечению 3-го уровня защищенности персональных данных и 3-го класса защищенности государственной информационной системы, что может быть реализовано применением сертифицированных по требованиям безопасности информации средств защиты информации:

Обязательные средства защиты информации:

а) средства контроля съемных машинных носителей информации 5 класса;б) средства антивирусной защиты не ниже 5 класса;

в) системы обнаружения вторжений не ниже 5 класса;г) межсетевой экран не ниже 5 класса;

д) средства доверенной загрузки не ниже 5 класса.

Для обеспечения защищенного взаимодействия Пользователей с ГИСЗ РТ через сеть Интернет, должны применяться средства криптографической защиты информации «ЗАСТАВА-Клиент «VPN/FW «ЗАСТАВА, версия 6».

4.2 Требования к техническому обеспечению.

АРМ для установки компонентов подсистем СЗИ должно удовлетворять техническим требованиям, предусмотренным в эксплуатационной документации к программным и программно-аппаратным средствам, входящим в состав подсистем.

4.3 Требования к организационному обеспечению.

4.3.1 Разрабатываемые организационно-распорядительные документы по защите информации должны определять следующие правила и процедуры:

- управления (администрирования) системой защиты информации информационной системы;
- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
- управления конфигурацией информационной системы и системы защиты информации информационной системы;
- контроля (мониторинга) за обеспечением уровня защищенности информации,содержащейся в информационной системе;
- защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

4.3.2 При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступасубъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;
- проверка полноты и детальности описания в организационно-

распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

- отработка действий должностных лиц и подразделений, ответственных зареализацию мер защиты информации.

4.3.2 Состав технических и организационно-распорядительных документов определяются Пользователями в соответствии с нормативными правовыми актами Российской Федерации в области защиты информации и нормативно-технических и методических документов в области обеспечения безопасности информации.

5 Контроль реализации подключения к ГИСЗ РТ

Ответственность за соблюдение требований безопасности информации, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и СКЗИ в составе системы защиты информации, лежит на Пользователе ГИСЗ РТ.

В соответствии с п.32 Приказа ФСТЭК России от 29 апреля 2021 года № 77, Пользователь ГИСЗ РТ не реже одного раза в 2 года предоставляет втерриториальный орган ФСТЭК России протокол контроля защиты информации на аттестованном объекте, заверенную копию которого направляет Оператору. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации не реже одного раза в 3 года.

ГАУЗ «РМИАЦ» имеет право осуществлять контроль за выполнением Пользователями ГИСЗ РТ требований по защите информации на соответствие настоящему Регламенту.

В случае выявления нарушений требований безопасности информации, ГАУЗ «РМИАЦ» в праве уведомить Пользователя ГИСЗ РТ о выявленном нарушении и потребовать устранения выявленных нарушений в согласованные сроки.

ГАУЗ «РМИАЦ» вправе немедленно прекратить доступ Пользователя к ГИСЗ РТ с последующим уведомлением Пользователя в случае выявления критичного нарушения, которое может привести к нарушению конфиденциальности информации, обрабатываемой в ГИСЗ РТ, ее целостности и доступности.

6 Порядок предоставления и прекращения доступа к ГИСЗ РТ

6.1 Пользователь направляет на имя министра здравоохранения Республики Татарстан письмо о подключении к ГИСЗ РТ по форме в Приложении № 1.

6.2 При получения положительного решения по п.6.1, настоящего Регламента, Пользователь согласовывает с ГАУЗ «РМИАЦ» схему подключения АРМ или информационной системы к ГИСЗ РТ с применением программного vpn-клиента «ЗАСТАВА-Клиент «VPN/FW «ЗАСТАВА, версия 6» или программно-аппаратного комплекса ЗАСТАВА.

6.3 Пользователь приобретает и устанавливает (организует установку и настройку) средств защиты информации.

6.4 Пользователь выполняет работы по аттестации объектов информатизации на соответствие требованиям безопасности персональных данных или работы по оценке эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных.

6.5 Пользователь направляет в отдел информационной безопасности ГАУЗ «РМИАЦ» по адресу: 420073, Республика Татарстан, город Казань, ул. Аделя Кутуя, д.88, по почте или нарочным: два экземпляра проекта Соглашения о предоставлении доступа к ГИСЗ РТ (предоставляются ГАУЗ «РМИАЦ») и документы, указанные в приложениях к Соглашению. Проект Соглашения предоставляется Пользователю после подтверждения им выполнения требований безопасности информации.

6.6 Отделом информационной безопасности Оператора проводится контроль выполнения Пользователем требований на подключение медицинских организаций к ГИСЗ РТ.

6.7 Пользователь предоставляет открытый ключ электронной подписи, который изготавливает любой аккредитованный удостоверяющий центр, отделу информационной безопасности Оператора. Срок действия электронной подписи составляет 15 месяцев с даты выдачи Пользователю аккредитованным удостоверяющим центром. До истечения указанного срока, Пользователь должен инициировать перевыпуск электронной подписи и направив открытый ключ отделу информационной безопасности Оператора ГИСЗ РТ.

6.8 Учетные записи для работников Пользователя в ГИСЗ РТ создаются на основании заключенного Соглашения, и копии приказа Пользователя о принятии на работу сотрудника (ов) и оригинала письма организации с указанием перечня сотрудников и их должностей, подключение которых к ГИСЗ РТ запрашивается.

6.9 При увольнении работника, имеющего доступ к ГИСЗ РТ, Пользователь обязан направить в адрес отдела информационной безопасности Оператора письмо на адрес mz.rmiac@tatar.ru копию приказа об увольнении лица, ранее имевшего доступк ГИС «ЭЗ РТ» для блокирования учетной записи, не позднее дня увольнения. Использование учетной записи уволенного сотрудника другими сотрудниками не допускается.

Используемые сокращения

ГИСЗ РТ	Государственная информационная система в сфере здравоохранения Республики Татарстан
ГАУЗ «РМИАЦ»	Государственное автономное учреждение здравоохранения «Республиканскиймедицинский информационно-аналитический центр. Оператор ГИСЗ РТ
АРМ	Автоматизированное рабочее место
ИС	Информационная система
ГИС	Государственная информационная система
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
Пользователи ГИСЗ РТ	Медицинские организации, подключенные к ГИСЗ РТ
СЗИ	Система защиты информации
СКЗИ	Средство криптографической защиты информации
СрЗИ	Средства защиты информации
ФЗ	Федеральный закон
ФСТЭК	Федеральная служба по техническому и экспортному контролю РФ
ФСБ	Федеральная служба безопасности Российской Федерации
ЭД	Эксплуатационная документация

Фирменный бланк заявителя Приложение №1

Министру здравоохранения
Республики Татарстан
М.М.Миннуллину

Уважаемый Марсель Мансурович!

Просим Вас рассмотреть возможность взаимодействия медицинской организации *<<Полное наименование организации>>* с государственной информационной системой в сфере здравоохранения Республики Татарстан.

Руководитель *(подпись)* *Ф.И.О.*
М.П.