УТВЕРЖДАЮ

Директор федерального государственного бюджетного учреждения «Федеральный центр тестирования»

_____ Ю.С. Егорова

«_12_» _____марта_____ 2024 г.

Федеральная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования

Программный комплекс «Проведение ГИА в ППЭ»

Частный регламент подключения к личному кабинету пункта проведения экзамена посредством защищенной сети передачи данных ГИА № 21387

Оглавление

Термины и определения

Административный сегмент сети	–	средства, обеспечивающие администрирование, управление доступом и обеспечение безопасности ЗСПД ГИА № 21387, в том числе выпуск дистрибутива ключей для подключения внешних пользователей к ЗСПД ГИА № 21387
Автоматизированное рабочее место, АРМ	–	основной и/или резервный компьютер, предназначенный для работы с ЛК ППЭ в соответствии с Методическими рекомендациями по подготовке и проведению единого государственного экзамена в пунктах проведения экзаменов
Виртуальная защищенная сеть	–	технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования)
Внешние пользователи	–	образовательные организации, реализующие образовательные программы основного общего и (или) среднего общего образования и выступающие в качестве пунктов проведения экзаменов при организации и проведении государственной итоговой аттестации
ГИА	–	государственная итоговая аттестация
Дистрибутив ключей	–	файл, создаваемый для активации доступа внешних пользователей по защищенным каналам связи к ЗСПД ГИА № 21387, содержащий справочники и ключи,

		необходимые для обеспечения первичного запуска и последующей работы средств криптографической защиты информации, устанавливаемых на внешнем узле сети (на автоматизированном рабочем месте)
Заявитель	–	образовательная организация, обратившаяся для организации подключения к ЛК ППЭ посредством ЗСПД ГИА № 21387
ЗСПД	–	Защищенная сеть передачи данных
Информационная система	–	совокупность одного или нескольких автоматизированных рабочих мест, предназначенных для подключения к ЛК ППЭ посредством ЗСПД ГИА № 21387; совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
ЛК ППЭ	–	личный кабинет пункта проведения экзамена программного комплекса «Проведение ГИА в ППЭ» Федеральной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования
ОИВ	–	орган исполнительной власти субъектов Российской Федерации, осуществляющий государственное управление в сфере образования
ППЭ	–	пункт проведения экзаменов
РЦОИ	–	региональный центр обработки информации субъекта Российской Федерации
СЗИ	–	средства защиты информации

Средства криптографической защиты информации, СКЗИ	–	средства криптографической защиты информации, программные, программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении
Узел сети, сетевой узел, узел	–	автоматизированное рабочее место, на котором установлено сертифицированное ФСБ России средство криптографической защиты информации и подключенное (подключаемое) к защищенной сети
SecretDoc	–	система автоматизации организационных мероприятий по обеспечению информационной безопасности по работе с организационно-распорядительными документами в области информационной безопасности

1. Общие положения

1.1. Настоящий Частный регламент подключения к личному кабинету пункта проведения экзамена посредством защищенной сети передачи данных ГИА № 21387 (далее – Регламент) разработан в соответствии с Единым регламентом подключения к государственным информационным системам (ресурсам) Федеральной службы по надзору в сфере образования и науки, обеспечение функционирования и организация технической защиты которых осуществляется федеральным государственным бюджетным учреждением «Федеральный центр тестирования» (далее – Единый регламент), утвержденным 19.01.2024 директором федерального государственного бюджетного учреждения «Федеральный центр тестирования» (далее – ФГБУ «ФЦТ»). Для выполнения требований п. 8 Правил формирования и ведения ФИС ГИА и приема и РИС ГИА, утвержденных постановлением Правительства Российской Федерации от 29.11.2023 № 2085, в части функционирования федеральной и региональных информационных систем в защищенной сети передачи данных Регламент подключения к ЛК ППЭ посредством защищенной сети передачи данных ГИА № 21387 (далее соответственно – Регламент, ЗСПД ГИА № 21387) определяет порядок получения доступа (подключения) внешних пользователей к ЛК ППЭ.

1.2. Регламент устанавливает правила осуществления защищенного взаимодействия между узлами сети внешних пользователей и ЛК ППЭ посредством ЗСПД ГИА № 21387, включая обязанности сторон.

1.3. Регламент не устанавливает правила подключения узлов внешних пользователей к сегменту администрирования ФИС ГИА и приема.

1.4. Регламент определяет:

– перечень нормативных правовых актов, на основании которых он разработан;

– порядок подключения узлов внешних пользователей к ЛК ППЭ посредством ЗСПД ГИА № 21387, включая требования к информационным системам;

– комплект обязательных документов, предоставляемых заявителем в уполномоченное подразделение ФГБУ «ФЦТ» для подключения;

– требования к уполномоченному подразделению ФГБУ «ФЦТ»,

обеспечивающему подключение узлов внешних пользователей;

– события, при наступлении которых происходит изменение параметров подключения к ЗСПД ГИА № 21387.

1.5. Описываемый в Регламенте порядок является обязательным к применению внешними пользователями, подключаемыми к ЛК ППЭ посредством ЗСПД ГИА № 21387.

1.6. Изменения (дополнения), вносимые в Регламент, за исключением изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для внешних пользователей, подключенных к ЛК ППЭ посредством ЗСПД ГИА № 21387, с даты их публикации на официальном сайте ФГБУ «ФЦТ» в информационно-коммуникационной сети интернет по адресу ***https://rustest.ru***.

1.7. Все приложения, изменения и дополнения к Регламенту являются его составной и неотъемлемой частью.

1.8. Регламент распространяется путем его опубликования на официальном сайте ФГБУ «ФЦТ» в информационно-коммуникационной сети интернет по адресу ***https://rustest.ru***. Дополнительно ФГБУ «ФЦТ» могут разрабатываться необходимые разъясняющие документы, размещаемые на официальном сайте ***https://rustest.ru***.

1.9. Лица, допустившие использование информационных систем (автоматизированных рабочих мест), не имеющих действующего аттестата соответствия требованиям по защите информации, а также не имеющих сертифицированные средства защиты информации, если они подлежат обязательной аттестации и сертификации, несут ответственность в соответствии со статьей 13.12 Кодекса Российской Федерации об административных правонарушениях.

2. Нормативные правовые акты, на основании которых разработан Регламент

Регламент разработан на основании следующих нормативных правовых актов и методических рекомендаций:

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

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

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– постановление Правительства Российской Федерации от 29.11.2021 № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»;

– приказ Министерства просвещения Российской Федерации и Федеральной службы по надзору в сфере образования и науки от 7 ноября 2018 г. № 190/1512 об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего общего образования, утвержденный;

– приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказ ФСТЭК России от 18.02.2013 № 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 29.04.2021 № 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 Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 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»;

– приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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 Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств»;

– Методические рекомендации по подготовке и проведению единого государственного экзамена в пунктах проведения экзаменов, ежегодно направляемые Рособрнадзором в субъекты Российской Федерации.

3. Порядок подключения узлов внешних пользователей к ЗСПД ГИА № 21387

3.1. Требования к рабочим станциям для подключения к ЛК ППЭ определены Требованиями к техническому оснащению в ППЭ (Приложение 2 к Методическим рекомендациям по подготовке и проведению единого государственного экзамена в пунктах проведения экзаменов).

3.2. Для организации подключения узлов внешних пользователей к ЗСПД ГИА № 21387 по сети интернет применяется технология виртуальных защищенных сетей, реализованная с использованием сертифицированных ФСБ России СКЗИ.

3.3. Организация доступа узлов внешних пользователей должна быть реализована по схеме подключения (приложение № 1 к Регламенту).

3.4. Организация доступа внешнего пользователя путем подключения с помощью межсетевого взаимодействия не допускается.

3.5. Подключение к ЗСПД ГИА № 21387 узлов внешних пользователей и техническое сопровождение подключения внешних пользователей к ЗСПД ГИА № 21387 осуществляет уполномоченное подразделение ФГБУ «ФЦТ».

3.6. Функции администратора ЗСПД ГИА № 21387, включая формирование дистрибутивов ключей и назначение связей узлам сети, осуществляют лица из числа работников уполномоченного подразделения ФГБУ «ФЦТ».

3.7. Принятие всех условий Регламента осуществляется путем предоставления заявителем в уполномоченное подразделение ФГБУ «ФЦТ» комплекта документов на подключение к ЗСПД ГИА № 21387, указанных в п. 3.10.6. настоящего Регламента.

3.8. В качестве заявителя для подачи заявки на подключение внешних пользователей к ЗСПД ГИА № 21387 могут также выступать органы исполнительной власти субъектов Российской Федерации, осуществляющие государственное управление в сфере образования (ОИВ) или организации, осуществляющие организационное и технологическое обеспечение проведения экзаменов на территориях субъектов Российской Федерации (РЦОИ).

3.9. Началом функционирования сетевого узла внешнего пользователя (заявителя) считается момент его подключения к ЗСПД ГИА № 21387 при выполнении условий, указанных в п. 3.10 настоящего Регламента.

3.10. Общий порядок и состав действий по подключению узлов внешних пользователей к ЗСПД ГИА № 21387:

3.10.1. Заявителю для подключения к ЗСПД ГИА № 21387 необходимо иметь:

– СКЗИ ViPNet Client сети № 21387;

– действующий аттестат соответствия требованиям по защите информации информационной системы (автоматизированного рабочего места) внешнего пользователя, взаимодействующего с ЛК ППЭ;

– учетную запись в системе автоматизации организационных мероприятий по обеспечению информационной безопасности SecretDoc (далее – система SecretDoc) расположенную в сети Интернет (***https://secretdoc.rustest.ru***).

3.10.2. Заявитель направляет обращение на предоставление учетной записи в системе автоматизации организационных мероприятий по обеспечению информационной безопасности SecretDoc на портал поддержи ***https://help.rustest.ru*** с указанием темы обращения «Подключение (полное наименование организации) к ЗСПД ГИА № 21387».

3.10.3. После обращения пользователя служба поддержки предоставляет пользователю данные учетной записи и инструкции по использованию системы SecretDoc.

3.10.4. В случае возникновения вопросов, связанных с подключением к ЗСПД ГИА № 21387, Заявитель может обратиться в техническую поддержку ЗСПД ГИА № 21387 через систему SecretDoc.

3.10.5. Заявитель формирует с использованием системы SecretDoc проекты следующих документов:

– письмо-запрос на имя директора ФГБУ «ФЦТ» на получение дистрибутива ключей (приложение № 2 к настоящему Регламенту);

– форму «Данные о заявителе, для подключения к ЗСПД ГИА № 21387 ФГБУ «ФЦТ» (приложение № 3 к настоящему Регламенту);

– приказ «О назначении ответственных лиц» (приложение № 4 к настоящему Регламенту).

3.10.6. Комплект документов в электронном виде, размещаемый в системе SecretDoc, не должен превышать 30 Mb, формат файлов – PDF. Указанный комплект включает в себя:

– скан-копию письма-запроса на имя директора ФГБУ «ФЦТ» на получение дистрибутива ключей (приложение № 2 к настоящему Регламенту);

– скан-копию формы «Данные о заявителе, для подключения к ЗСПД ГИА № 21387 ФГБУ «ФЦТ» (приложение № 3 к настоящему Регламенту);

– скан-копию приказа «О назначении ответственных лиц» (приложение № 4 к настоящему Регламенту);

– скан-копию аттестата соответствия требованиям по защите информации информационной системы (автоматизированного рабочего места) внешнего пользователя, взаимодействующей с ЛК ППЭ посредством ЗСПД ГИА № 21387

– скан-копию технического паспорта информационной системы (автоматизированного рабочего места) внешнего пользователя, взаимодействующей с ЛК ППЭ посредством ЗСПД ГИА № 21387.

3.10.7. Заявитель загружает документы, указанные в п. 3.10.6. настоящего Регламента, подписанные и заверенные усиленной квалифицированной электронной подписью уполномоченного лица, в систему SecretDoc (заверение возможно произвести непосредственно в системе SecretDoc при загрузке).

3.10.8. Заявитель создает в разделе Техническая поддержка системы SecretDoc обращение на подключение к ЗСПД ГИА № 21387.

3.10.9. В течение 10-ти рабочих дней уполномоченное подразделение ФГБУ «ФЦТ» выполняет проверку комплекта документов на соответствие требованиям Регламента и сообщает заявителю о результате проверки в системе SecretDoc.

3.10.10. Передача дистрибутива ключей и другой информации для подключения к ЗСПД ГИА № 21387 производится уполномоченным подразделением ФГБУ «ФЦТ» в порядке, установленном Инструкцией 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, утверждённой приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152.

3.11. Порядок выдачи (передачи) заявителю дистрибутива ключей для подключения к ЗСПД ГИА № 21387 устанавливается в соответствии с разделом 5 настоящего Регламента.

3.12. ФГБУ «ФЦТ» имеет право отказать заявителю в подключении к ЗСПД ГИА № 21387 по следующим основаниям:

– заявителем необходимые документы для подключения предоставлены не в полном объеме;

– класс и тип используемых СКЗИ не соответствуют СКЗИ, применяемым в ФГБУ «ФЦТ»;

– на стороне заявителя не выполняются требования по обеспечению безопасности обрабатываемой информации (отсутствует аттестат соответствия требованиям по защите информации);

– АРМ не соответствует требованиям, предъявляемым к информационным системам (автоматизированным рабочим местам) – узлам внешних пользователей, подключаемых к ЛК ППЭ (раздел 4 настоящего Регламента).

3.13. Деловая переписка ведется в системе SecretDoc в рамках обращения.

3.14. Уполномоченное подразделение ФГБУ «ФЦТ» в случае несоответствия комплекта документов требованиям настоящего Регламента и (или) необходимости получения дополнительной информации по заявке на подключение к ЗСПД ГИА № 21387 имеет право запросить у заявителя дополнительную информацию. Заявителю необходимо предоставить дополнительную информацию в ФГБУ «ФЦТ» в течение 5 (пяти) рабочих дней с момента запроса. Если в течение указанного времени требуемая информация в ФГБУ «ФЦТ» не предоставляется, то заявка считается закрытой.

4. Требования к подключаемым информационным системам (автоматизированным рабочим местам) – узлам внешних пользователей

4.1. Информационные системы или автоматизированные рабочие места (объекты информатизации) узлов внешних пользователей, подключаемых к ЗСПД ГИА № 21387, должны соответствовать требованиям безопасности, предъявляемым к информационным системам персональных данных, в которых установлена необходимость обеспечения четвертого уровня защищенности персональных данных, и/или требованиям безопасности, предъявляемым к информационным системам, в которых установлена необходимость обеспечения третьего класса защищенности.

4.2. Класс используемых СКЗИ - КС2.

4.3. Внешние пользователи при информационном обмене и обработке информации в информационных системах обязаны принимать необходимые правовые, организационные и технические меры, направленные на защиту информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в ее отношении.

4.4. Для обеспечения защиты информации внешними пользователями должны реализовываться организационные и технические меры защиты информации.

4.5. К организационным мерам защиты информации относятся:

1) разработка и утверждение организационно-распорядительной документации для доступа к информационной системе;

2) контроль доступа;

3) ведение журналов учета (в том числе аппаратного журнала АРМ и журнала учета СКЗИ).

4.6. К техническим мерам защиты информации относятся:

1) применение сертифицированных средств антивирусной защиты;

2) применение сертифицированных средств защиты информации от несанкционированного доступа;

3) применение сертифицированных средств межсетевого экранирования;

4) применение сертифицированных средств криптографической защиты.

5. Порядок выдачи (получения) дистрибутива ключей для подключения внешних пользователей к ЗСПД ГИА № 21387

5.1. ФГБУ «ФЦТ» приступает к изготовлению дистрибутива ключей после получения от АО «ИнфоТеКС» регистрационного файла и лицензии на приобретенное заявителем СКЗИ, а также комплекта документов от заявителя, указанные в п. 3.10.6 настоящего Регламента.

5.2. После изготовления дистрибутива ключей ФГБУ «ФЦТ» направляет заявителю в ответ на заявку на подключение информацию о готовности передачи дистрибутива ключей.

5.3. Уполномоченное подразделение ФГБУ «ФЦТ» подготавливает дистрибутив ключей и инструкцию по установке для передачи их заявителю.

5.4. Передача осуществляется в соответствии с п. 3.10 настоящего Регламента.

5.5. Полученный дистрибутив ключей используется заявителем для итоговой настройки программных продуктов семейства «ViPNet» и подключения к ЗСПД ГИА № 21387.

5.6. При возникновении обстоятельств, требующих замены дистрибутива ключей, а именно: компрометация, утеря, поломка носителя информации, невозможность чтения информации, реорганизация организации заявителя, заявителю необходимо:

– сформировать с использованием системы SecretDoc письмо-запрос на повторное формирование дистрибутива ключей (приложение № 5);

– загрузить письмо подписанное и заверенное усиленной квалифицированной электронной подписью уполномоченного лица, в систему SecretDoc (заверение возможно произвести непосредственно в системе SecretDoc при загрузке);

– создать в системе SecretDoc в адрес ФГБУ «ФЦТ» обращение на повторное формирование дистрибутива ключей.

5.7. В случае возникновения в организации заявителя инцидентов информационной безопасности, связанных с несанкционированным доступом к информации, передаваемой посредством ЗСПД ГИА № 21387 ФГБУ «ФЦТ», ФГБУ «ФЦТ» вправе проводить расследования возможных инцидентов и запрашивать у заявителя сведения, необходимые для выяснения обстоятельств таких инцидентов.

6. Требования к уполномоченному подразделению ФГБУ «ФЦТ»

6.1. Уполномоченное подразделение ФГБУ «ФЦТ», обеспечивающее подключение к ЗСПД ГИА № 21387, обязано:

6.1.1. Руководствоваться положениями настоящего Регламента.

6.1.2. Вести учет всех внешних пользователей, подключенных к ЗСПД ГИА № 21387.

6.1.3. Осуществлять выдачу дистрибутива ключей.

6.1.4. Использовать ключи шифрования, входящие в комплект дистрибутива ключей, только в соответствии с документацией на используемое СКЗИ и только для одного объекта информатизации, принадлежащего внешнему пользователю.

6.1.5. Соблюдать требования эксплуатационной документации на используемое СКЗИ.

6.1.6. Учитывать и контролировать наличие действующих аттестатов соответствия требованиям по защите информации у всех внешних пользователей, подключенных к ЗСПД ГИА № 21387.

6.1.7. При выявлении уже подключенных узлов внешних пользователей с недействующим аттестатом соответствия требованиям по защите информации и/или с недействующим сертификатом соответствия на СЗИ и СКЗИ уведомить внешних пользователей о разрыве подключения к ЗСПД ГИА № 21387 в связи с невыполнением с их стороны требований по защите информации и, при отсутствии подтверждения о проведённых мероприятиях, в 2-х месячный срок отключить от ЗСПД ГИА № 21387.

7. Изменение параметров подключения к ЗСПД ГИА № 21387

7.1. Изменение параметров подключения узлов к ЗСПД ГИА № 21387 осуществляется уполномоченным подразделением ФГБУ «ФЦТ» при наступлении следующих событий:

– не завершен процесс подключения к ЗСПД ГИА № 21387;

– уполномоченным подразделением ФГБУ «ФЦТ» выявлен факт, что внешние пользователи лишились права взаимодействия с ЛК ППЭ;

– уполномоченным подразделением ФГБУ «ФЦТ» выявлен факт изменения официального наименования внешнего пользователя;

– уполномоченным подразделением ФГБУ «ФЦТ» выявлены факты нарушения положений настоящего Регламента;

– уполномоченным подразделением ФГБУ «ФЦТ» выявлен факт компрометации дистрибутива ключей узла сети внешнего пользователя.

7.2. Соотнесение указанных событий с предпринимаемыми на их основании действиями приведено в таблице:

Таблица – Изменения параметров подключения узлов к ЗСПД ГИА № 21387

№ п/п	Событие	Условие	Действие
1	не завершен процесс подключения к ЗСПД ГИА № 21387	уполномоченное подразделение не получило письмо-уведомление о получении дистрибутива ключей	отключение узла от ЗСПД ГИА № 21387
2	уполномоченным подразделением выявлен факт, что внешний пользователь лишился права взаимодействия с ЛК ППЭ	у внешнего пользователя не остается прав на взаимодействие с информационной системой	отключение узла от ЗСПД ГИА № 21387
3	уполномоченным подразделением выявлен факт изменения официального наименования внешнего пользователя	–	изменение наименования узла ЗСПД ГИА № 21387
4	уполномоченным подразделением выявлен факт нарушения положений Регламента	–	отключение узла от ЗСПД ГИА № 21387
5	уполномоченным подразделением выявлен факт компрометации дистрибутива ключей узла внешнего пользователя	–	отключение узла от ЗСПД ГИА № 21387

Приложение № 1 к Регламенту

Схема подключения к ЗСПД ГИА № 21387

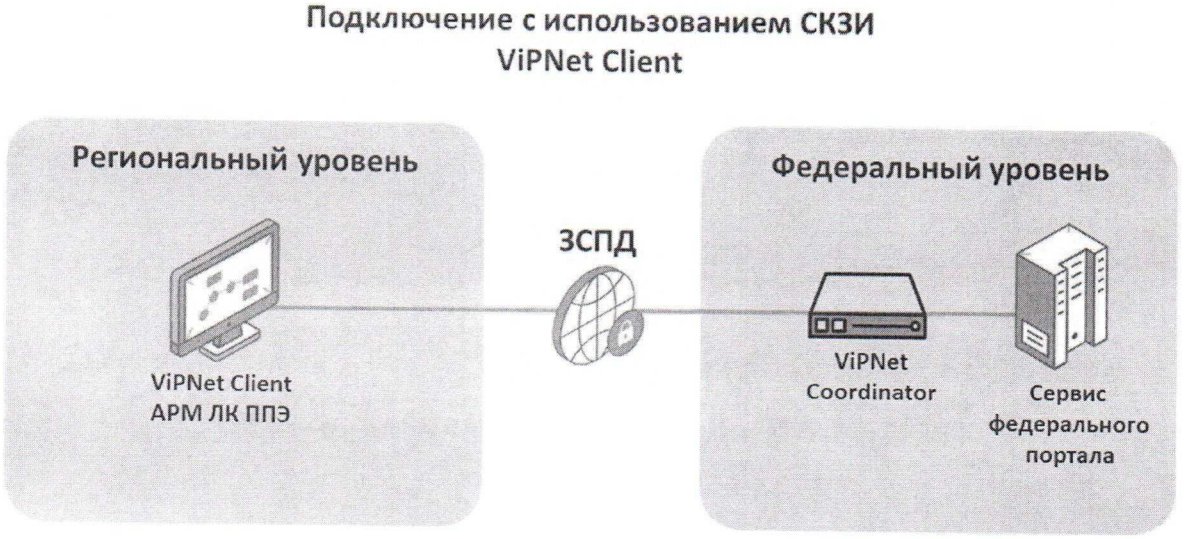

Рисунок 1. Схема подключения с использованием ViPNet Client для сети № 21387

Приложение № 2 к Регламенту

Письмо – запрос на получение дистрибутива ключей

Дата и исх. номер

Директору
ФГБУ «ФЦТ»

В соответствии с Частным регламентом подключения к личному кабинету пункта проведения экзамена посредством защищенной сети передачи данных ГИА № 21387 (далее – Частный регламент) просим подключить нашу организацию **[наименование вашей организации]** к ЗСПД ГИА № 21387.

Работы по реализации схемы подключения к ЗСПД ГИА № 21387 будет проводить **[наименование организации]**, обладающее(ая) необходимыми лицензиями ФСТЭК России и ФСБ России.

В целях закрепления персональной ответственности за функционирование **[наименование объекта информатизации (информационной системы, автоматизированного рабочего места]**, а также в целях обеспечения функционирования и безопасности криптографических средств в **[наименование Вашей организации]** назначены ответственные лица.

В рамках реализации требований раздела 5 Частного регламента прошу предоставить дистрибутив ключей для подключения к ЗСПД ГИА № 21387 ФГБУ «ФЦТ».

Приложение:

1. Подписанные данные о заявителе, для подключения к ЗСПД ГИА № 21387 в формате PDF (*оформляется согласно приложению № 3 Частного регламента*).

2. Приказ о назначении ответственных лиц (*оформляется согласно приложению № 4 Частного регламента*).

[должность руководителя организации] **[И.О. Фамилия]**

подпись руководителя

М.П.

Приложение № 3 к Регламенту

Данные о заявителе, для подключения к ЗСПД ГИА № 21387

(все поля обязательны к заполнению)

Организация

1.	Код и наименование субъекта РФ	
		Две цифры и полное наименование субъекта РФ
2.	Полное наименование образовательной организации	
		Полное наименование подключаемой организации. Наименование должно совпадать с данными из Устава организации
3.	ИНН организации	
		Из выписки ЕГРЮЛ
4.	Код образовательной организации	
		Шесть цифр, присвоенные ОО в РИС/ФИС
5.	Код ППЭ	
		Четыре цифры, присвоенные ППЭ в РИС/ФИС
6.	Фактический адрес ППЭ	
		Индекс, область, город, район, улица, дом, строение/корпус

Ответственное лицо

1.	Ф. И. О. руководителя организации или лица, его замещающего	
		Из выписки ЕГРЮЛ
2.	Телефон рабочий	
		В формате +7 (XXX) XXX-XXXX
3.	Адрес электронной почты (e-mail)	
		Действующий адрес электронной почты

Аттестат соответствия требованиям по защите информации информационной системы (автоматизированного рабочего места) внешнего пользователя, взаимодействующей с ЛК ППЭ посредством ЗСПД ГИА № 21387

1.	Наименование объекта информатизации (информационной системы, автоматизированного рабочего места)	
2.	Срок действия	
3.	Номер аттестата	
4.	Наименование органа по аттестации, выдавшего аттестат	

«___»_____20__г.

Дата

Подпись ответственного лица или руководителя

Достоверность предоставленных данных гарантируем. Обязуемся не нарушать схему подключения к ЗСПД ГИА № 21387 ФГБУ «ФЦТ» и производить изменения только по согласованию с ФГБУ «ФЦТ».

М.П.

Приложение № 4 к Регламенту

Приказ о назначении ответственных лиц

ПРИКАЗ №__

О назначении лица, ответственного за функционирование **[наименование объекта информатизации (информационной системы, автоматизированного рабочего места)]**, и лица, ответственного за обеспечение функционирования и безопасности криптографических средств в соответствии с требованиями:

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказа ФАПСИ 13.06.2001 № 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»;

– приказа ФСБ России от 10.07.2014 № 378 «Состав и содержание 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».

П Р И К А З Ы В А Ю:

1. Назначить **[ФАМИЛИЯ Имя Отчество]**, **[должность]**, ответственным за функционирование **[наименование объекта информатизации (информационной системы, автоматизированного рабочего места)]**;
2. Назначить **[ФАМИЛИЯ Имя Отчество]**, **[должность]**, лицом, ответственным за обеспечение функционирования и безопасности криптографических средств;
3. Контроль за исполнением настоящего приказа оставляю за собой.

[должность руководителя организации] **[И.О. Фамилия]**

подпись руководителя

С приказом ознакомлен(а)

[дата] **[И.О. Фамилия]**

подпись ответственного лица

[дата] **[И.О. Фамилия]**

подпись ответственного лица

Приложение № 5 к Регламенту

Письмо-запрос на повторное формирование дистрибутива ключей

Дата и исх. номер

Директору
ФГБУ «ФЦТ»

Уважаемый/ая_____!

В соответствии с п 5.6 Частного регламента подключения к личному кабинету пункта проведения экзамена посредством защищенной сети передачи данных ГИА № 21387 прошу повторно сформировать дистрибутив ключей для подключения к ЗСПД ГИА № 21387 согласно сведениям из таблицы 1 в связи с **[компрометацией, утерей, другая причина]** дистрибутива ключей.

Таблица 1.

User ID	*Пример: APT id_0 QWERTY*
Имя DST файла	*Пример: abn_0000.dst*

[должность руководителя организации] **[И.О. Фамилия]**

подпись руководителя

М.П.