УТВЕРЖДАЮ

Директор федерального государственного бюджетного учреждения «Федеральный центр тестирования»

_____ Ю.С. Егорова

«___» _____ 2024 г.

Единый регламент 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»

1. Общие положения

1.1. Настоящий Регламент (далее - Единый регламент) определяет порядок получения доступа (подключения) внешних пользователей (информационных систем) к государственным информационным системам 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 – ГИС).

1.2. Единый регламент устанавливает правила осуществления защищенного взаимодействия между узлами внешних пользователей (информационных систем) и ГИС, включая обязанности сторон.

1.3. Единый регламент не устанавливает правила подключения узлов внешних пользователей (информационных систем) к сегменту администрирования ГИС.

1.4. Все приложения, изменения и дополнения к Единому регламенту являются его составной и неотъемлемой частью.

1.5. Единый регламент распространяется путем его опубликования на официальном сайте ФГБУ «ФЦТ» в информационно-коммуникационной сети «Интернет» по адресу http://rustest.ru.

1.6. Порядок подключения к каждой из ГИС устанавливается частными регламентами подключения (далее – Частные регламенты), которые разрабатываются в соответствии с Единым регламентом.

1.7. Частные регламенты не должны противоречить Единому регламенту и требованиям нормативных правовых актов.

1.8. Единый регламент предусматривает:

- перечень нормативных правовых актов в области информационной безопасности, на основании которых он разработан;
- порядок подключения внешних пользователей к ГИС, включая требования к информационным системам внешних пользователей;
- комплект обязательных документов, предоставляемых внешними пользователями для подключения;
- требования, обеспечивающие подключение внешних пользователей, события, при наступлении которых происходит изменение параметров подключения к ГИС.

1.9. Описываемый в документе порядок является обязательным к применению внешними пользователями, подключаемыми к ГИС с использованием защищенных сетей передачи данных, построенных на основе сертифицированных ФСБ России средств криптографической защиты информации.

1.10. Лица, допустившие использование информационных систем или автоматизированных рабочих мест, не имеющих действующего аттестата соответствия требованиям по защите информации информационной системы, а также несертифицированных средств защиты информации, если они подлежат обязательной аттестации и сертификации, несут ответственность в соответствии со статьей 13.12 Кодекса Российской Федерации об административных правонарушениях.

1.11. Изменения (дополнения), вносимые в Единый регламент, за исключением изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для внешних пользователей, подключившихся к информационным

системам, с даты их публикации на официальном сайте ФГБУ «ФЦТ» в сети интернет по адресу rustest.ru.

2. Термины и определения

Административный сегмент сети	– средства, обеспечивающие администрирование, управление доступом и обеспечение безопасности информационных систем (ресурсов), в том числе выпуск необходимой ключевой и парольно-справочной информации для подключения внешних пользователей к информационным системам (ресурсам);
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	– федеральные государственные органы, органы исполнительной власти субъектов Российской Федерации, осуществляющие государственное управление в сфере образования; органы государственной власти субъектов Российской Федерации, осуществляющие переданные полномочия Российской Федерации в сфере образования, органы местного самоуправления, осуществляющие государственное управление в сфере образования; организации, осуществляющие образовательную деятельность, органы и организации, в ведение которых переданы архивы организаций, выдавших документы об образовании и (или) о квалификации, документы об обучении, образовательные организации, расположенные на территории Российской Федерации,

реализующие образовательные программы основного общего и (или) среднего общего образования, и другие.

Дистрибутив ключей – файл, создаваемый для доступа внешних пользователей по защищенным каналам связи к информационным системам (ресурсам), содержащий справочники и ключи, необходимые для обеспечения первичного запуска и последующей работы средств криптографической защиты информации, устанавливаемый на внешнем узле сети (на автоматизированном рабочем месте);

Заявитель – юридическое лицо, обратившееся для организации обмена информацией между его информационной системой (автоматизированном рабочим местом) и ГИС;

Защищенная сеть – защищенная сеть передачи данных, построенная на основе сертифицированных ФСБ России средств криптографической защиты информации;

Средства криптографической защиты информации – аппаратные, программные и аппаратно–программные 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 – техническое средство, на котором установлено сертифицированное ФСБ России средство криптографической защиты информации и подключенное (подключаемое) к защищенной сети.

3. Нормативные правовые акты в области информационной безопасности, на основании которых разработан Единый регламент

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

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрирован Минюстом России 31.05.2013, регистрационный № 28608).

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» (зарегистрирован Минюстом России 14.05.2013, регистрационный № 28375).

Приказ ФСТЭК России от 29.04.2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (зарегистрирован Минюстом России 10.08.2021 № 64589).

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» (зарегистрирован Минюстом России 06.08.2001, регистрационный № 2848).

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» (зарегистрирован Минюстом России 18.08.2014, регистрационный № 33620).

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)» (зарегистрирован Минюстом России 03.03.2005, регистрационный № 6382).

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» (зарегистрирован Минюстом России 23.11.2022, регистрационный № 71073).

4. Порядок подключения внешних пользователей к ГИС

4.1. Для организации подключения внешних пользователей к ГИС по сети Интернет применяется технология виртуальных защищенных сетей, реализованная с использованием сертифицированных ФСБ России шифровальных (криптографических) средств защиты информации.

4.2. Подключение к ГИС внешних пользователей и техническое сопровождение подключения внешних пользователей к ГИС осуществляет ФГБУ «ФЦТ».

4.3. Функции администратора защищенной сети, включая формирование дистрибутивов ключей и назначение связей узлам сети, осуществляют лица из числа работников ФГБУ «ФЦТ». Список лиц закрепляется приказом ФГБУ «ФЦТ».

4.4. Подключение к ГИС внешних пользователей осуществляется с использованием средств криптографической защиты информации, имеющих действующие сертификаты соответствия ФСБ России.

4.5. Частные регламенты утверждаются руководителем ФГБУ «ФЦТ» и размещаются на официальном сайте rustest.ru в сети интернет. Дополнительно ФГБУ «ФЦТ» может разрабатывать необходимые разъясняющие документы, размещаемые на официальном сайте rustest.ru (методические рекомендации, типовые схемы подключения и др.).

4.6. Подключение к ГИС производится в соответствии с Единым и Частными регламентами.

4.7. Подключение к ГИС и принятие всех условий Единого и Частных регламентов осуществляется путем подписания и предоставления внешними пользователями в ФГБУ «ФЦТ» заявлений на подключение к ГИС.

4.8. С момента регистрации заявления на подключение к ГИС в ФГБУ «ФЦТ» заявитель считается принявшим все условия Единого и соответствующего Частного регламента.

4.9. Началом функционирования сетевого узла заявителя считается момент его подключения к ГИС при выполнении условия, указанного в подпункте 4.11.5 Единого регламента.

4.10. Организация доступа внешних пользователей путем межсетевого взаимодействия допускается только в случае, если межсетевое взаимодействие предусмотрено соответствующим Частным регламентом и при условии предоставления документального подтверждения выполнения требований безопасности информации (скан аттестата соответствия требованиям по защите информации информационной системы) для каждого из сетевых узлов (автоматизированных рабочих мест) в защищенной сети, получающих доступ к ГИС в порядке, установленном соответствующим Частным регламентом.

4.11. Общий порядок и состав действий по подключению внешних пользователей к ГИС:

4.11.1. Внешнему пользователю для подключения к ГИС необходимо иметь:

– средства криптографической защиты информации (далее – СКЗИ), совместимые с СКЗИ защищенной сети, используемой для доступа к ГИС (закупка осуществляется внешним пользователем самостоятельно);

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

– другие средства криптографической защиты информации, необходимые для организации доступа к ГИС и определяемые соответствующим Частным регламентом.

4.11.2. Внешний пользователь формирует комплект документов на подключение к ГИС (далее – комплект документов) в порядке, установленном соответствующим Частным регламентом, направляет его в адрес ФГБУ «ФЦТ».

4.11.3. ФГБУ «ФЦТ» выполняет проверку комплекта документов на соответствие требованиям Единого регламента и соответствующего Частного регламента подключения к ГИС и сообщает заявителю о положительном результате проверки или уведомляет заявителя о несоответствии комплекта документов требованиям Единого регламента (Частного регламента). При положительном результате проверки комплекта документов 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, и соответствующим Частным регламентом, производит выдачу необходимой парольной информации, дистрибутива ключей и другой информации для подключения к ГИС.

4.11.4. Комплект обязательных документов на подключение к ГИС должен включать:

– заявление, включающее основание необходимости доступа к ГИС, с указанием наименования организации;

– заверенную копию лицензии на право использования СКЗИ, совместимых с СКЗИ защищенной сети, используемой для доступа к ГИС;

– копию аттестата соответствия требованиям по защите информации информационной системы (автоматизированного рабочего места) внешнего пользователя, взаимодействующей с ГИС;

– другую информацию, определяемую соответствующим Частным регламентом.

4.11.5. ФГБУ «ФЦТ» имеет право отказать внешнему пользователю в подключении к ГИС по следующим основаниям:

а) внешним пользователем необходимые документы для подключения предоставлены не в полном объеме;

б) класс и тип используемых средств криптографической защиты информации не соответствуют СКЗИ защищенной сети, используемой для доступа к ГИС;

в) внешним пользователем не выполняются требования по обеспечению безопасности обрабатываемой информации (отсутствует аттестат соответствия требованиям по защите информации информационной системы);

г) внешний пользователь не является легитимным пользователем ГИС.

4.11.6. Решение об отказе в подключении заявителя к ГИС направляется на электронный адрес заявителя в течение пяти рабочих дней со дня принятия указанного решения.

5. Требования к подключаемым информационным системам внешних пользователей

5.1. Для информационных систем или автоматизированных рабочих мест внешних пользователей, подключаемых к ГИС, должны выполняться требования, предъявляемые нормативными правовыми актами Российской Федерации в области защиты информации к обеспечению третьего уровня защищенности персональных данных (не ниже), и к обеспечению защищенности государственных информационных систем не ниже класса К3.

5.2. 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.

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

5.3.1. К организационным мерам защиты информации относятся:

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

б) контроль доступа;

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

5.3.2. К техническим мерам защиты информации относятся:

а) применение сертифицированных средств антивирусной защиты;

б) применение сертифицированных средств защиты информации от несанкционированного доступа;

в) применение сертифицированных средств межсетевого экранирования;

г) применение сертифицированных средств криптографической защиты.

6. Требования к ФГБУ «ФЦТ»

6.1. ФГБУ «ФЦТ», обеспечивающее подключение к ГИС, обязано:

6.1.1. Руководствоваться положениями Единого регламента и соответствующих Частных регламентов.

6.1.2. Вести учет всех внешних пользователей, подключенных к ГИС.

6.1.3. Осуществлять выдачу парольной информации и дистрибутивов ключей.

6.1.4. Использовать ключи шифрования, входящие в комплект дистрибутивов 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. Осуществлять контроль наличия действующих аттестатов соответствия требованиям по защите информации у всех внешних пользователей, подключаемых и подключенных ГИС.

6.1.7. Осуществлять контроль наличия действующих документов проведения периодического контроля уровня защиты информации на аттестованном объекте информатизации (протоколы контроля защиты информации на аттестованном объекте информатизации) у всех внешних пользователей, подключенных ГИС.

6.1.8. При выявлении у подключенных к ГИС внешних пользователей недействующего аттестата соответствия требованиям по защите информации или отсутствия протокола контроля защиты информации на аттестованном объекте

информатизации предупредить о разрыве подключения к ГИС в связи с невыполнением с их стороны требований безопасности информации и, при отсутствии подтверждения о проведённых мероприятиях в 3-х месячный срок, отключить от защищенной сети.

6.1.9. Отключить от защищенной сети внешних пользователей, работающих в ГИС, при передаче ими информации в интересах третьих лиц, не попадающих под перечень определения внешних пользователей Единого регламента.

7. Изменение параметров подключения к информационной системе (ресурсу)

7.1. Изменение параметров подключения узлов к ГИС осуществляется ФГБУ «ФЦТ» при наступлении следующих событий:

7.1.1. Выявлен факт незавершенного процесса подключения к ГИС;

7.1.2. ФГБУ «ФЦТ» выявлен факт, что внешние пользователи лишился права взаимодействия с ГИС;

7.1.3. ФГБУ «ФЦТ» выявлен факт об изменении официального наименования внешнего пользователя;

7.1.4. ФГБУ «ФЦТ» выявлены факты нарушения положений Единого регламента или соответствующего Частного регламента;

7.1.5. ФГБУ «ФЦТ» выявлен факт компрометации дистрибутива ключей узла внешнего пользователя;

7.1.6. ФГБУ «ФЦТ» выявлен факт завершения действия аттестата соответствия требованиям безопасности информации;

7.1.7. ФГБУ «ФЦТ» выявлен факт непроведения периодического контроля уровня защиты информации на аттестованном объекте информатизации не реже одного раза в два года;

7.1.8. ФГБУ «ФЦТ» выявлен факт передачи информации третьим лицам;

7.1.9. ФГБУ «ФЦТ» выявлен факт превышения согласованного количества подключенных внешних пользователей при межсетевом взаимодействии.

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

Таблица – Изменения параметров подключения узлов к информационным сетям ФГБУ «ФЦТ»

№ п/п	Событие	Условие	Действие
1	Не завершен процесс подключения к информационной системе (ресурсу)	ФГБУ «ФЦТ» не получило письмо-уведомление о получении парольной и справочно-ключевой информации	Отключение узла от сети
2	ФГБУ «ФЦТ» выявлен факт, что внешний пользователь лишился права взаимодействия с ГИС	У внешнего пользователя не остается прав на взаимодействие с ГИС	Отключение узла от сети
3	ФГБУ «ФЦТ» выявлен факт об изменении официального наименования внешнего пользователя	–	Изменение наименования узла
4	ФГБУ «ФЦТ» выявлен факт нарушения положений Единого регламента, соответствующего Частного регламента	–	Отключение узла от сети
5	ФГБУ «ФЦТ» выявлен факт компрометации дистрибутива ключей узла внешнего пользователя	–	Отключение узла от сети
6	ФГБУ «ФЦТ» выявлен факт завершения действия аттестата соответствия требованиям безопасности информации	В течение 3-х месяцев с момента окончания действия аттестата соответствия требованиям безопасности информации не представлен новый аттестат	Отключение узла от сети
7	ФГБУ «ФЦТ» выявлен факт непроведения периодического контроля уровня защиты информации на аттестованном объекте информатизации не реже одного раза в два года	В течение 3-х месяцев с момента выявления несоответствия требованиям безопасности информации не представлен протокол контроля защиты информации	Отключение узла от сети
8	ФГБУ «ФЦТ» выявлен факт передачи информации третьим лицам	-	Отключение узла от сети

№ п/п	Событие	Условие	Действие
9	ФГБУ «ФЦТ» выявлен факт превышения согласованного количества подключенных внешних пользователей при межсетевом взаимодействии	-	Отключение узла от сети