Федеральное государственное автономное научное учреждение
«Центр информационных технологий и систем органов исполнительной власти»
(ФГАНУ ЦИТиС)

УТВЕРЖДАЮ

Заместитель директора по
информационной безопасности
ФГАНУ ЦИТиС

В.Н. Труфанов

«16» ноября 2020 г.

Порядок подключения к защищенной сети передачи данных 3189 (Регламент)

Версия: 1.2

Начальник Центра безопасности
информации ФГАНУ ЦИТиС

Д.А. Щевелев

«16» ноября 2020 г.

Москва 2020

Оглавление

Оглавление 2
Перечень терминов, определений и сокращений 4
1 Назначение и область действия документа 6
2 Общие положения 6
3 Сеть 3189 7
4 Порядок подключения заявителя к сети 3189 8
5 Комплект документов на подключение к сети 3189 9
6 Передача заявителю парольной и справочно-ключевой информации 10
6.1 Порядок передачи парольной и справочно-ключевой информации 10
7 Действия заявителя в случае обнаружения нарушений в процессе передачи парольной и справочно-ключевой информации 12
8 Обязанности образовательных организаций 13
9 Изменение параметров подключения к сети 3189 13
Приложение № 1 15
Приложение № 2 18
Приложение № 3 19

Таблица изменений

Версия	Изменение
1.0	Исходная версия документа
1.1	Уточнен порядок подключения к сети 3189
1.2	Изменен порядок подключения к сети 3189

Перечень терминов, определений и сокращений

Административный сегмент сети 3189	–	средства, обеспечивающие работоспособность ЗСПД 3189 (включает программное обеспечение центр управления сетью, удостоверяющий и ключевой центр, а также координаторы сети ViPNet).
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)
Дистрибутив ключей	–	файл с расширением .dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого узла сети 3189. Содержит справочники и ключи, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на узле сети 3189. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на автоматизированное рабочее место
Заявитель	–	юридическое лицо, обратившееся в установленном настоящим Регламентом порядке в ФГАНУ ЦИТиС для подключения к сети 3189 с целью организации обмена информацией между принадлежащей ему информационной системой и информационной системой Рособрнадзора
Заявитель		юридическое лицо, подавшее заявление на подключение к сети 3189
Настоящий регламент		порядок подключения к защищенной сети передачи данных 3189
Образовательные организации		организации, осуществляющие образовательную деятельность в соответствии с нормативными правовыми

актами Российской Федерации в сфере образования

Сертификат получателя	– квалифицированный сертификат ключа проверки электронной подписи, выданный на лицо, получающее парольную и справочно-ключевую информацию
Сертификат уполномоченного подразделения	– квалифицированный сертификат ключа проверки электронной подписи работника уполномоченного подразделения
Сеть 3189, ЗСПД 3189	– виртуальная защищенная сеть передачи данных, построенная на основе технологии виртуальных защищенных сетей ViPNet
Средства криптографической защиты информации, СКЗИ	– 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 3189, сетевой узел	– техническое средство, на котором установлено программное обеспечение ViPNet, зарегистрированное в программе центра управления сетью 3189
Уполномоченное подразделение	уполномоченное структурное подразделение, являющееся органом криптографической защиты информации Федерального государственного автономного научного учреждения «Центр информационных технологий и систем органов исполнительной власти»
ФГАНУ ЦИТиС	– Федеральное государственное автономное научное учреждение «Центр информационных технологий и систем органов исполнительной власти»
ФИС ГНА	– Федеральная информационная система государственной научной аттестации
ФСБ России	– Федеральная служба безопасности Российской Федерации

1 Назначение и область действия документа

1.1 Требования настоящего Регламента распространяются на образовательные организации, подключаемые к защищенной сети передачи данных 3189 для организации защищенного информационного взаимодействия с ФИС ГНА.

1.2 Настоящий Регламент устанавливает порядок подключения информационных систем образовательных организаций к сети 3189, а также правила осуществления защищенного взаимодействия между узлами сети 3189, включая обязанности сторон.

1.3 Настоящий Регламент не устанавливает правила подключения узлов к сегменту администрирования сети 3189.

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

1.5 Настоящий Регламент распространяется в форме электронного документа на официальном сайте ФГАНУ ЦИТиС в сети Интернет по адресу https://citis.ru/3189.

2 Общие положения

2.1 Для организации защищенного информационного взаимодействия по сети Интернет с ФИС ГНА применяется технология виртуальных защищенных сетей, реализованная с использованием сертифицированных шифровальных (криптографических) средств, совместимых с решениями семейства ViPNet.

2.2 Правом подключения к сети 3189 обладают только образовательные организации, осуществляющие образовательную деятельность и имеющие диссертационные советы.

2.3 Подключение к сети 3189 образовательных организаций и техническое сопровождение сети 3189 осуществляет уполномоченное подразделение.

2.4 Уполномоченное подразделение

2.4.1 Наименование структурного подразделения ФГАНУ ЦИТиС, выполняющего функции уполномоченного подразделения: Центр безопасности информации.

2.4.2 Контактные данные уполномоченного подразделения:

2.4.2.1 адрес электронной почты: 3189vipnet@citis.ru;

2.4.2.2 номер телефона: +7 (495) 197-65-91, +7 (800) 200-65-64;

2.4.2.3 почтовый адрес: 123557, Москва, Пресненский Вал, 19, стр. 1. При отправке документов осуществляется пометка на конверте «Подключение к ViPNet-сети 3189».

2.5 Присоединение к настоящему Регламенту

2.5.1 Присоединение к настоящему Регламенту и принятие всех условий настоящего Регламента осуществляется путем подписания и предоставления образовательными организациями в уполномоченное подразделение заявления на подключение к сети 3189 (приложение № 1 к настоящему Регламенту).

2.5.2 С момента регистрации заявления на подключение к сети 3189 в ФГАНУ ЦИТиС Заявитель, считается присоединившимся к настоящему Регламенту и принявшим все условия настоящего Регламента.

2.5.3 Началом функционирования сетевого узла заявителя считается момент его подключения к сети 3189 при выполнении условия, указанного в подпункте 6 пункта 4.1.

2.6 Изменение настоящего Регламента

2.6.1 Внесение изменений (дополнений) в настоящий Регламент, включая приложения к нему, производится ФГАНУ ЦИТиС в одностороннем порядке.

2.6.2 Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется ФГАНУ ЦИТиС путем обязательного размещения указанных изменений (дополнений) в сети Интернет по адресам https://citis.ru/3189 в разделе «Новости» и https://vak.minobrnauki.gov.ru в разделе «Новости».

2.6.3 Все изменения в разделы настоящего Регламента вносятся с изменением номера версии данного документа.

2.6.4 Все изменения (дополнения), вносимые в настоящий Регламент, вступают в силу после опубликования на официальном сайте ФГАНУ ЦИТиС в сети Интернет по адресу https://citis.ru/3189.

3 Сеть 3189

3.1 Сеть 3189 создана и функционирует с целью обеспечения функционирования ФИС ГНА в части обеспечения защищенного взаимодействия внешних информационных систем, подключенных к сети 3189 в соответствии с настоящим Регламентом, с ФИС ГНА.

3.2 В сети 3189 для построения виртуальных защищенных сетей используются только сертифицированные ФСБ России и совместимые с ViPNet СКЗИ.

3.3 Техническое обеспечение защищенного взаимодействия информационных систем образовательных организаций с ФИС ГНА осуществляется посредством криптографической защиты передаваемых данных между узлами сети 3189.

3.4 Функции администратора сети 3189, включая формирование дистрибутивов ключей и назначение связей узлам сети, осуществляют лица из числа работников уполномоченного подразделения.

3.5 Подключение к сети 3189 образовательных организаций осуществляется с использованием средства вычислительной техники образовательной организации, оснащенного СКЗИ ViPNet Client сети 3189, имеющего действующий сертификат соответствия ФСБ России.

4 Порядок подключения заявителя к сети 3189

4.1 Общий порядок и состав действий по подключению заявителя к сети 3189:

1) Заявителю необходимо иметь:

– необходимое количество СКЗИ ViPNet Client (для Windows) версии, имеющей действующий сертификат соответствия ФСБ России и лицензии на право использования данных СКЗИ в составе сети 3189 (количество СКЗИ ViPNet Client определяется каждым заявителем в соответствии с собственными потребностями);

– действующий квалифицированный сертификат ключа проверки электронной подписи, выданный на лицо, получающее парольную и справочно-ключевую информацию (далее – сертификат получателя)[1];

– средство электронной подписи с функцией зашифрования и расшифрования файлов (ViPNet PKI Client, КриптоАРМ или аналогичное средство).

2) Заявитель формирует комплект документов на подключение к сети 3189 (далее – комплект документов) и направляет по адресу электронной почты, указанному в п. 2.4.2.1, в уполномоченное подразделение на предварительное согласование совместно с файлом, содержащим сертификат получателя. Порядок создания и обработки комплекта документов приведен в разделе 5 настоящего Регламента.

3) Уполномоченное подразделение выполняет проверку комплекта документов на соответствие требованиям настоящего Регламента и сообщает заявителю о положительном результате проверки или уведомляет заявителя о порядке исправления несоответствия комплекта документов требованиям настоящего Регламента.

---

[1] Срок окончания действия сертификата получателя должен быть не менее месяца с момента отправления оригинала заявления на подключение к сети 3189 в адрес ФГАНУ ЦИТиС

4) После получения подтверждения проверки заявитель направляет комплект документов с оригиналом подписанного заявления, оформленного на бланке организации, в адрес уполномоченного подразделения.

5) После получения оригинала подписанного заявления уполномоченное подразделение выполняет формирование и передачу парольной и справочно-ключевой информации заявителю и письма-уведомления о передаче парольной и справочно-ключевой информации (порядок передачи парольной и справочно-ключевой информации приведен в п. 6.1 настоящего Регламента).

6) Заявитель получает парольную и справочно-ключевую информацию.

7) Заявитель направляет почтовым отправлением в адрес ФГАНУ ЦИТиС (уполномоченному подразделению) письмо-уведомление о получении парольной и справочно-ключевой информации.

4.2 Обязательства уполномоченного подразделения по участию в процедуре подключения заявителя к сети 3189 считаются выполненными при наступлении события, указанного в подпункте 5 пункта 4.1 настоящего Регламента.

4.3 Обязательства заявителя по участию в процедуре подключения к сети 3189 считаются выполненными при наступлении события, указанного в подпункте 7 пункта 4.1 настоящего Регламента.

4.4 Заявитель организует настройку собственных узлов сети 3189, включая установку дистрибутивов ключей.

4.5 В случае необходимости проведения повторного подключения заявителя, уже подключённого к сети 3189, общий порядок и состав действий по получению заявителем парольной и справочно-ключевой информации аналогичен общему порядку и составу действий при первоначальном подключении.

5 Комплект документов на подключение к сети 3189

5.1 Комплект документов на подключение к сети 3189 включает:

– заявление;

– заверенную копию лицензии на право пользования ViPNet Client для сети 3189;

5.2 Заявление содержит информацию, необходимую уполномоченному подразделению для корректного формирования парольной и справочно-ключевой информации.

5.3 Первоначальное подключение узла сети 3189 осуществляется при заполнении формы заявления, приведённой в приложении № 1 к настоящему Регламенту.

5.4 Повторное подключение заявителя (переподключение) также осуществляется при заполнении формы заявления, приведённой в приложении №1 к настоящему Регламенту.

5.5 Если заявление на подключение (переподключение) к сети 3189 подписано лицом, действующим от имени заявителя на основании доверенности, то вместе с заявлением заявитель должен передать в уполномоченное подразделение заверенную копию указанной доверенности.

5.6 Заявитель направляет комплект документов на предварительное согласование в уполномоченное подразделение на адрес электронной почты.

5.7 Уполномоченное подразделение в течение 5 рабочих дней с момента получения комплекта документов, отправленного заявителем, выполняет проверку на соответствие настоящему Регламенту.

5.8 Уполномоченное подразделение по результатам проверки комплекта документов направляет заявителю на адрес электронной почты перечень обнаруженных замечаний, если таковые имелись.

5.9 Заявитель в течение 30 рабочих дней с момента отправки замечаний должен их устранить и направить необходимые документы в уполномоченное подразделение.

5.10 В случае если по истечении указанного срока заявителем не будут предоставлены документы с устраненными замечаниями, запрос на подключение аннулируется. Заявителю потребуется повторно направить весь комплект документов на подключение к сети 3189 в уполномоченное подразделение.

5.11 После предварительного согласования заявитель передает комплект документов с оригиналом подписанного заявления, оформленного на бланке организации, в адрес ФГАНУ ЦИТиС (уполномоченного подразделения).

6 Передача заявителю парольной и справочно-ключевой информации

6.1 Порядок передачи парольной и справочно-ключевой информации

6.1.1 В течение 10 рабочих дней с момента получения и регистрации комплекта документов с оригиналом подписанного заявления уполномоченное подразделение выполняет проверку комплекта документов на соответствие настоящему Регламенту, формирование и отправку (передачу) ключевой информации заявителю, содержащую файл парольной и справочно-ключевой информации, зашифрованный на ключе проверки электронной подписи получателя (входит в состав сертификата получателя).

6.1.2 Одновременно с этим уполномоченное подразделение направляет письмо-уведомление о направлении парольной и справочно-ключевой информации в адрес заявителя (приложение № 2 к настоящему Регламенту).

6.1.3 Если в результате проверки комплекта документов были обнаружены замечания, уполномоченное подразделение отправляет заявителю на адрес электронной почты перечень обнаруженных замечаний.

6.1.4 Заявитель в течение 30 рабочих дней с момента отправки замечаний должен их устранить и направить необходимые документы в уполномоченное подразделение.

6.1.5 В случае если по истечении указанного срока заявителем не будут предоставлены документы с устраненными замечаниями, запрос на подключение аннулируется. Заявителю потребуется повторно предоставить весь комплект документов в уполномоченное подразделение.

6.1.6 Заявитель после получения отправления от уполномоченного подразделения выполняет его проверку вложения электронного письма на наличие файла, содержащего парольную и справочно-ключевую информацию в зашифрованном виде (файл с расширением .enc).

6.1.7 Заявитель выполняет расшифрование файла, содержащего парольную и справочно-ключевую информацию, с использованием средства электронной подписи и ключа электронной подписи сертификата получателя.

6.1.8 Заявитель выполняет проверку содержимого расшифрованного файла на наличие парольной (файл с расширением .xps) и справочно-ключевой информации (файл с расширением .dst).

6.1.9 В случае обнаружения нарушений проверки полученного электронного отправления заявитель должен действовать в соответствии с разделом 7 Регламента и не использовать парольную и справочно-ключевую информацию до получения отдельного указания от уполномоченного подразделения.

6.1.10 При получении письма-уведомления о передаче парольной и справочно-ключевой информации заявитель проверяет соответствие информации, указанной в письме.

6.1.11 В случае если в результате проверки полученных отправлений не было выявлено нарушений, заявитель направляет письмо-уведомление о получении парольной и справочно-ключевой информации в адрес уполномоченного подразделения (приложение № 3 к настоящему Регламенту).

6.1.12 Процесс передачи парольной и справочно-ключевой информации заявителю считается завершенным с момента получения уполномоченным подразделением письма-уведомления о получении парольной и справочно-ключевой информации.

7 Действия заявителя в случае обнаружения нарушений в процессе передачи парольной и справочно-ключевой информации

7.1 В случае обнаружения нарушений процесса передачи парольной и справочно-ключевой информации до получения указания от уполномоченного подразделения заявитель не должен использовать парольную и справочно-ключевую информацию.

7.2 В случае обнаружения нарушений процесса передачи парольной и справочно-ключевой информации заявитель должен выполнить следующие действия:

1) зафиксировать нарушения средствами фотосъемки и/или скриншотов экрана;

2) сохранить в неизменном виде сообщения электронной почты, относящиеся к процессу передачи парольной и справочно-ключевой информации;

3) передать уполномоченному подразделению информацию об обнаруженном нарушении, фотографии и/или скриншоты экрана (при наличии) нарушений, средствами электронной почты или почтовым отправлением.

7.3 При получении уполномоченным подразделением письма уполномоченное подразделение производит оценку ситуации, включая причины возникновения нарушений, значимость нарушений и сроки возможного устранения последствий.

7.4 В ответ уполномоченное подразделение отправляет посредством электронной почты информацию, содержащую дальнейшие указания к действию, такие как:

1) запрос дополнительной информации о состоянии отправления;

2) указания к уничтожению файлов парольной и справочно-ключевой информации;

3) разрешение использовать парольную и справочно-ключевую информацию.

7.5 Уполномоченным подразделением может быть принято решение о формировании новой парольной и справочно-ключевой информации.

7.6 В случае получения заявителем уведомления от уполномоченного подразделения о формировании и отправке новой парольной и справочно-ключевой информации заявитель ожидает получения нового отправления в порядке, определенном разделом 6 настоящего Регламента.

7.7 Уполномоченное подразделение может запросить дополнительную информацию для принятия решения о дальнейших действиях.

7.8 В случае указания уполномоченного подразделения уничтожить файлы парольной и справочно-ключевой информации заявитель должен осуществить уничтожение информации в соответствии с порядком, установленным эксплуатационной документацией на соответствующее СКЗИ, и отправить в

уполномоченное подразделение уведомление об уничтожении парольной и справочно-ключевой информации.

7.9 В случае получения разрешения использовать парольную и справочно-ключевую информацию заявитель может использовать парольную и справочно-ключевую информацию для подключения к защищенной сети передачи данных 3189.

8 Обязанности образовательных организаций

8.1 Образовательные организации, подключающиеся к сети 3189, обязаны:

8.1.1 Осуществлять получение парольной и справочно-ключевой информации только способом, описанным в настоящем Регламенте.

8.1.2 Использовать ключи шифрования, входящие в комплект парольной и справочно-ключевой информации, только в соответствии с документацией на используемое СКЗИ и только для одного объекта информатизации, принадлежащего образовательной организации.

8.1.3 Соблюдать требования эксплуатационной документации на используемое СКЗИ.

8.1.4 Сообщать в уполномоченное подразделение о фактах компрометации парольной и ключевой информации.

8.1.5 Своевременно и в полном объеме выполнять инструкции по обновлению мастер-ключей сети 3189, публикуемые уполномоченным подразделением на официальном сайте ФГАНУ ЦИТиС по адресу https://citis.ru/3189.

9 Изменение параметров подключения к сети 3189

9.1 Изменение параметров подключения узлов сети 3189 осуществляется уполномоченным подразделением при наступлении следующих событий:

1) не завершен процесс подключения к сети 3189;

2) уполномоченному подразделению становится известно, что образовательная организация лишились права взаимодействия с ФИС ГИА;

3) уполномоченному подразделению становится известно об изменении официального наименования юридического лица, владельца узла сети;

4) уполномоченному подразделению становится известно о фактах нарушения положений настоящего Регламента;

5) уполномоченному подразделению становится известно о факте компрометации парольной и справочно-ключевой информации узла образовательной организации.

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

Таблица – Изменения параметров подключения узлов в сети 3189

№ п/п	Событие	Условие	Действие
1	не завершен процесс подключения к сети 3189	уполномоченное подразделение не получило письма-уведомления о получении парольной и справочно-ключевой информации	отключение узла от сети
2	уполномоченному подразделению становится известно, что образовательная организация лишились права взаимодействия с ФИС ГИА	у образовательной организации не остается прав на взаимодействие с ФИС ГИА	отключение узла от сети
3	уполномоченному подразделению становится известно об изменении официального наименования юридического лица, владельца узла сети	–	изменение наименования узла
4	уполномоченному подразделению становится известно о фактах нарушения положений настоящего Регламента	в случае оценки факта нарушения, совершенного образовательной организацией, как серьезного	отключение узла от сети
5	уполномоченному подразделению становится известно о факте компрометации парольной и справочно-ключевой информации узла образовательной организации.	–	отключение узла от сети

Приложение № 1
к Регламенту подключения к сети 3189

Форма заявления на подключение к сети 3189 юридического лица

(Оформляется на бланке юридического лица-заявителя)

ФГАНУ ЦИТиС

123557, г. Москва,
ул. Пресненский Вал, д.19, стр.1

Прошу Вас осуществить процесс подключения *(наименование юридического лица-заявителя)* к защищенной сети передачи данных 3189 в соответствии со сведениями о *(наименование юридического лица-заявителя)*, приведенными ниже в настоящем письме.

1. Сведения о юридическом лице

Полное официальное наименование юридического лица	

(полное официальное наименование юридического лица, совпадающее с информацией, указанной в выписке из ЕГРЮЛ, доступной на официально ресурсе налогового органа в сети Интернет)

Сокращенное наименование юридического лица	

(сокращенное официальное наименование юридического лица, совпадающее с информацией, указанной в выписке из ЕГРЮЛ, доступной на официально ресурсе налогового органа в сети Интернет)

ИНН юридического лица	

Почтовый адрес	

E-mail	

Должность руководителя юридического лица	

(указывается должность лица, которое может действовать без доверенности от имени юридического лица)

Ф.И.О. руководителя юридического лица	

(ФИО лица, которое имеет право действовать без доверенности от имени юридического лица)

Документ(-ы), на основании которых действует руководитель юридического лица	

(устав, приказ о головной организации о назначении и т.д.)

(Если настоящее заявление подписал не руководитель юридического лица, то в заявлении необходимо указать реквизиты документов, устанавливающих право лица, подписавшего данное заявление, обращаться в ФГАНУ ЦИТиС от имени юридического лица с целью подключения к защищенной сети 3189)

2. Сведения о лице, ответственном за процесс подключения к защищенной сети передачи данных 3189 и за подтверждение факта приема/передачи парольной и справочно-ключевой информации

(с этим лицом будут связываться работники уполномоченного подразделения ФГАНУ ЦИТиС для уточнения параметров процедуры подключения к защищенной сети, в том числе для передачи отправлений, содержащих парольную и справочно-ключевую информацию, в этом разделе могут содержаться сведения о более чем одном ответственном лице)

Ф.И.О.	
Должность	
Телефон (рабочий)	

(Номер телефона необходимо указать в формате +7 (XXX) XXX-XXXX)

Телефон (мобильный)	

(Номер телефона необходимо указать в формате +7 (XXX) XXX-XXXX)

E-mail	

3. Сведения о лице, имеющем право получения отправлений, содержащих парольную и справочно-ключевую информацию защищенной сети передачи данных 3189

(в этом разделе необходимо указать информацию о лице, которое имеет право получения отправлений, содержащих парольную и справочно-ключевую информацию, передаваемых в соответствии с настоящим заявлением, которому принадлежит квалифицированный сертификат ключа проверки электронной подписи (ключ проверки электронной подписи которого используется при шифровании файлов парольной и справочно-ключевой информации)

Ф.И.О.	
Должность	
Телефон (рабочий)	

(Номер телефона необходимо указать в формате +7 (XXX) XXX-XXXX)

Телефон (мобильный)	

(Номер телефона необходимо указать в формате +7 (XXX) XXX-XXXX)

E-mail	
Срок действия квалифицированного сертификата ключа проверки электронной подписи	

(сертификат должен принадлежать лицу, указанному в этом пункте)

Серийный номер квалифицированного сертификата ключа проверки электронной подписи	

(сертификат должен принадлежать лицу, указанному в этом пункте)

Подтверждаем ознакомление и согласие со всеми положениями порядка подключения к защищенной сети передачи данных 3189.

Подтверждаем выполнение в информационной системе *(наименование юридического лица-заявителя)*, подключаемой к защищенной сети передачи данных 3189,

предъявленных к ней требований о защите информации в соответствии с действующим законодательством Российской Федерации.

Достоверность предоставленных данных гарантируем. Обо всех изменениях параметров подключения *(наименование юридического лица)* к защищенной сети передачи данных 3189 обязуемся уведомлять уполномоченное подразделение ФГАНУ ЦИТиС.

_____	_____	_____
(наименование должности руководителя юридического лица-заявителя)	*(подпись)*	*(Ф.И.О.)*

МП

Приложение № 2
к Регламенту подключения к сети 3189

Форма письма-уведомления о передаче парольной и справочно-ключевой информации ЗСПД 3189

(Оформляется на бланке юридического лица)

(наименование юридического лица)

(почтовый адрес юридического лица)

Настоящим письмом уведомляем о том, что ФГАНУ ЦИТиС направило на указанный в заявлении на подключение адрес (*адрес заявителя*) парольную и справочно-ключевую информацию для подключения к защищенной сети передачи данных 3189. Указанная информация зашифрована с использованием сертификата ключа проверки электронной подписи владельца сертификата, указанного в заявлении на подключение.

Просим подтвердить получение парольной и справочно-ключевой информации после проведения процедуры расшифрования путем отправки ответного письма-уведомления (образец можно скачать на официальном сайте ФГАНУ ЦИТиС по адресу https://citis.ru/docs/notification3189.docx).

Количество и состав переданной в соответствии с настоящим уведомлением парольной и справочно-ключевой информации:

Состав парольной и справочно-ключевой информации (после расшифрования)	*Наименование файла .dst (размер КБ)* *Наименование файла .xps (размер КБ)*

(наименование должности руководителя)	*(подпись)*	*(Ф.И.О.)*

Приложение № 3
к Регламенту подключения к сети 3189

Форма письма-уведомления о получении парольной и справочно-ключевой информации ЗСПД 3189

(Оформляется на бланке юридического лица)

Федеральное государственное автономное научное учреждение «Центр информационных технологий и систем органов исполнительной власти»

ул. Пресненский Вал, д.19, стр.1
123557, г. Москва

Настоящим письмом информируем о том, что *(наименование юридического лица)* получена и расшифрована отправленная в зашифрованном виде парольная и справочно-ключевая информацию для подключения к защищенной сети передачи данных 3189.

Количество и состав переданной парольной и справочно-ключевой информации полностью соответствует указанной в письме *(реквизиты письма-уведомления, направленного ФГАНУ ЦИТиС).*

_____	_____	_____
(наименование должности руководителя)	*(подпись)*	*(Ф.И.О.)*