Федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКАЯ АКАДЕМИЯ
НАРОДНОГО ХОЗЯЙСТВА и ГОСУДАРСТВЕННОЙ СЛУЖБЫ
при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

Москва

от «23» января 2025 года № 02 – 033

Об утверждении регламента эксплуатации и подключения к защищенной сети передачи данных РАНХиГС

Руководствуясь статьей 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 09 февраля 2005 г. № 66,

п р и к а з ы в а ю:

1. Утвердить прилагаемый регламент эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации".

2. Правовому управлению (А.В. Менкенов) разместить настоящий приказ в базе локальных нормативных актов.

3. Общему отделу (А.О. Копылова) довести настоящий приказ до сведения руководителей структурных подразделений (г. Москва) и директоров филиалов Академии.

4. Контроль за исполнением настоящего возложить на директора по информационной безопасности И.Е. Яблокова.

Ректор А.Г. Комиссаров

Проект вносит: директор по информационной безопасности И.Е. Яблоков

Приложение
к приказу от "23" января 2025 г.
№ 02-033

РЕГЛАМЕНТ

эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации"

I. Общие положения

1.1. Регламент эксплуатации и подключения к защищенной сети передачи данных (далее – Регламент) федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации", разработан в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, № 31, 31.07.2006, ст. 3448);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701);

– Федеральный закон от 06 апреля 2011 г. № 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, № 15, 11.04.2011, ст. 2036);

– Указ Президента Российской Федерации от 11 марта 2003 г. № 308 "О мерах по совершенствованию государственного управления в области безопасности Российской Федерации" (Собрание законодательства Российской Федерации, № 12, 24.03.2003);

– Указ Президента Российской Федерации от 06.03.1997 № 188 "Об утверждении перечня сведений конфиденциального характера (Собрание законодательства Российской Федерации, № 10, 10.03.97, ст. 1127);

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (Собрание законодательства Российской Федерации, № 45, 05.11.2012, ст. 6257);

– Постановление Правительства Российской Федерации от 16.04.2012 № 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию

услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" (Собрание законодательства Российской Федерации, № 17, 23.04.2012, ст. 1987);

– Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13 июня 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" (Зарегистрировано в Минюсте РФ 06 августа 2001 г. № 2848);

– Приказ Федеральной службы безопасности Российской Федерации от 09 февраля 2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (Зарегистрировано в Минюсте РФ 03 марта 2005 г. № 6382);

– Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" (Зарегистрировано в Минюсте России 18 августа 2014 г. № 33620).

1.2. Регламент определяет основные принципы использования ключевой информации, генерируемой с применением средств криптографической защиты информации, входящих в состав программных и программно-аппаратных комплексов ViPNet, разработанных АО "ИнфоТеКС".

1.3. Регламент устанавливает порядок, способы подключения и правила осуществления защищенного взаимодействия между узлами защищенной сети передачи данных Академии.

1.4. Регламент разработан с целью созданий условий для организации защищенного сетевого взаимодействия с информационными системами Академии.

1.5. Требования Регламента распространяются на юридических лиц (органы, организации), подключаемых посредством защищенной сети передачи данных к информационным системам Академии.

1.6. Организация защищенного взаимодействия с информационными системами Академии осуществляется по технологии виртуальных защищенных сетей, с использованием средств криптографической защиты информации ViPNet.

1.7. Подключение к защищенной сети передачи данных осуществляет оператор – орган криптографической защиты дирекции по информационной безопасности Академии:

– почтовый адрес: 119571, г. Москва, вн. тер. г. муниципальный округ Тропарево-Никулино, пр-кт Вернадского, д. 82, стр. 1;

– адрес электронной почты: okz@ranepa.ru;

– номера телефонов: +7 (499) 956-01-42, +7 (499) 956-01-97.

1.8. Регламент выступает в качестве соглашения, налагающего обязательства всем вовлеченным сторонам, а также средства официального уведомления и информирования сторон во взаимоотношениях, возникающих при регистрации в защищенной сети передачи данных Академии.

1.9. Распространение текста регламента в сети Интернет осуществляется по адресу (www.ranepa.ru) на официальном сайте оператора защищенной сети передачи данных, которым выступает Академия.

1.10.Помимо публикации Регламента на официальном сайте оператора, орган криптографической защиты дирекции по информационной безопасности хранит экземпляр Регламента с приложениями, прошитый, пронумерованный постранично, удостоверенный подписью ректора Академии. При подаче и регистрации заявления о присоединении к Регламенту, заявитель соглашается с тем, что в случае возникновения спора в качестве доказательства принимается текст Регламента и приложений к нему, который прошит, пронумерован постранично, удостоверен подписью ректора Академии.

1.11.Настоящий Регламент, изменения и дополнения к нему, вступают в силу со дня их официального опубликования и действуют бессрочно.

Официальное уведомление о прекращении действия Регламента осуществляется путем публикации соответствующей информации на официальном сайте оператора защищенной сети передачи данных.

1.12.Присоединение к Регламенту выполняется путем предоставления заявителем в орган криптографической защиты дирекции по информационной безопасности заявления о присоединении к Регламенту на бумажном носителе согласно форме, указанной в Приложении № 1 к Регламенту.

С момента регистрации заявления о присоединении к Регламенту в органе криптографической защиты дирекции по информационной безопасности юридическое лицо (орган, организация), от имени которого выступает заявитель, считается присоединенным к Регламенту, и является с оператором совместно именуемыми сторонами Регламента.

Оснований для отказа в приеме заявления о присоединении к Регламенту не предусмотрено.

Основанием для отказа регистрации заявителя в защищенной сети передачи данных Академии является несоответствие требованиям Регламента предоставленных заявителем документов.

Основаниями отказа в создании справочно-ключевой информации и (или) информации первичного межсетевого экспорта могут быть:

– заявление о создании справочно-ключевой информации (информации первичного межсетевого экспорта), доверенность на получение справочно-ключевой информации (информации первичного межсетевого экспорта) и (или) организационно-распорядительный документ о назначении ответственного за средства криптографической защиты информации в органе (организации), оформлены с нарушением требований и (или) документы, технические средства, указанные в пункте 3.4 Регламента, представлены не в полном объеме.

Факт присоединения заявителя к Регламенту является полным принятием им условий Регламента и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении к Регламенту в органе криптографической защиты дирекции по информационной безопасности Академии. Стороны Регламента принимают дальнейшие изменения и дополнения, вносимые в Регламент, в соответствии с условиями Регламента.

После присоединения к Регламенту, оператор и присоединившаяся сторона Регламента считаются вступившими в договорные отношения на неопределенный срок.

1.13.Договорные отношения могут быть прекращены по инициативе одной из сторон в следующих случаях:

– по желанию одной из сторон с указанием обоснованных причин;
– при ликвидации/реорганизации одной из сторон;
– при нарушении одной из сторон условий Регламента.

В случае расторжения договорных отношений инициативная сторона письменно уведомляет другую сторону о своих намерениях за 30 (тридцать) календарных дней до предполагаемой даты расторжения договорных отношений по форме, указанной в Приложении № 2 к Регламенту. Договорные отношения считаются расторгнутыми после выполнения сторонами своих обязательств.

Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его исполнение (ненадлежащее исполнение).

1.14.Внесение изменений (дополнений) в Регламент, включая приложения к нему, производятся оператором в одностороннем порядке в следующих случаях:

– при изменении процессов и технологий обработки конфиденциальной информации в Академии;

– по результатам проверок органов государственной безопасности РФ и иных контрольно-надзорных органов, уполномоченных на проведение соответствующих проверочных мероприятий;

– в случае выявления нарушений по результатам внутренних проверок системы защиты информации;

– при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности конфиденциальной информации.

Уведомление о внесении изменений (дополнений) в регламент осуществляется оператором путем обязательного размещения указанных изменений (дополнений) в сети Интернет по адресу (www.ranepa.ru).

Все изменения (дополнения), вносимые в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 5 (пяти) календарных дней с даты размещения указанных изменений (дополнений) по адресу (www.ranepa.ru).

Все изменения (дополнения), вносимые в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) указанных в нормативных правовых актах действующего законодательства.

Все изменения (дополнения) в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

В случае несогласия с изменениями (дополнениями) сторона Регламента имеет право до вступления в силу таковых изменений (дополнений) подать отзыв заявления о присоединении к Регламенту по форме, указанной в Приложении № 2 к Регламенту.

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

1.15.Настоящий Регламент не регламентирует порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений, составляющих государственную тайну.

1.16.Предоставление персональных данных представителей заявителя является необходимым условием для исполнения договорных отношений и в соответствии с п. 5 ч. 1 ст. 6п. 5 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" не требует получения отдельного согласия на обработку персональных данных. Данное условие применяется в рамках исполнения настоящего Регламента и не противоречит требованиям законодательства Российской Федерации о защите персональных данных.

1.17. Во всех случаях, не урегулированных настоящим Регламентом или другими нормативными документами Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, необходимо руководствоваться действующим законодательством Российской Федерации.

1.18. Настоящий Регламент вступает в силу с момента его утверждения и действует до замены его новым Регламентом.

1.19. Все изменения в Регламент вносятся приказом ректора Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

II. Термины и определения

Стороны Регламента понимают термины, применяемые в Регламенте, строго в контексте общего смысла Регламента.

2.1. Абонентский пункт (сетевой узел) – узел, на котором установлено программное обеспечение специального назначения (ViPNet), являющийся начальной или конечной точкой передачи данных, зарегистрированный в защищенной сети передачи данных.

Администратор ЗСПД – уполномоченное должностное лицо оператора, отвечающее за управление защищенной сетью передачи данных, создание и обновление справочников и ключей для абонентских пунктов (сетевых узлов) защищенной сети передач данных, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программному комплексу ViPNet Administrator.

2.2. 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).

2.3. Дистрибутив ключей – файл с расширением *.dst, создаваемый в программном комплексе ViPNet Administrator для каждого абонентского пункта (сетевого узла).

Содержит справочники, ключи и файл лицензии, необходимые для первичного запуска и последующей работы программного комплекса ViPNet Client на абонентском пункте (сетевом узле).

2.4. Заявитель (сторона Регламента) – юридическое лицо (орган, организация), обратившаяся в установленном настоящим Регламентом порядке в орган криптографической защиты дирекции по информационной безопасности для подключения к защищенной сети передачи данных с целью организации обмена информацией между принадлежащей ему информационной системой и информационной системой Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации.

2.5. Заявление – заявление юридического лица (органа, организации) на подключение к защищенной сети передачи данных.

2.6. ЗСПД – виртуальная защищенная сеть передачи данных, построенная на основе технологии виртуальных защищенных сетей ViPNet.

2.7. Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

2.8. Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

2.9. Ключевой документ – электронный документ на любом носителе информации, а также документ на бумажном носителе, содержащий ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

2.10.Ключевой носитель – носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

2.11.Контейнер ключа – файл, в котором хранится закрытый ключ и соответствующий ему сертификат открытого ключа.

2.12.Криптографический ключ – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

2.13.Оператор – орган криптографической защиты дирекции по информационной безопасности Академии.

2.14.Первичная инициализация – процедура установки справочно-ключевой информации на абонентском пункте (сетевом узле) и (или) файла информации первичного межсетевого экспорта в программном комплексе ViPNet Administrator.

2.15.Пользователь ЗСПД – зарегистрированное в защищенной сети передачи данных юридическое лицо (орган, организация), чьи данные внесены в реестр пользователей защищенной сети передачи данных.

2.16.Представитель пользователя ЗСПД – физическое лицо, уполномоченное в установленном законом порядке представлять интересы пользователя ЗСПД.

2.17.Программный комплекс ViPNet Client – программное обеспечение специального назначения, реализующее функцию защиты рабочего места от внешних и внутренних сетевых атак за счет фильтрации трафика, обеспечивающее защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей.

2.18.Программный комплекс ViPNet Administrator – программное обеспечение специального назначения, реализующее функцию настройки и управления защищенной сетью передачи данных, включающее в себя:

а) ViPNet NCC (Центр управления сетью, ЦУС) – приложение, предназначенное для создания и управления конфигурацией защищенной сети передачи данных, позволяющее решить следующие задачи:

– построение виртуальной защищенной сети, состоящей из сетевых объектов и связей между ними, включая межсетевое взаимодействие;

– изменение конфигурации виртуальной защищенной сети;

– формирование и рассылка защищенных адресных справочников абонентских пунктов (сетевых узлов), защищенных таблиц маршрутизации;

– рассылка ключей абонентских пунктов (сетевых узлов) и ключей пользователей;

– формирование информации о связях абонентских пунктов (сетевых узлов) и пользователей;

– конфигурирование параметров абонентских пунктов (сетевых узлов) и полномочий пользователей

– централизованное обновление программного обеспечения на абонентских пунктах (сетевых узлах) защищенной сети передачи данных;

– управление журналами событий и журналами аудита.

б) ViPNet КСА (Удостоверяющий и ключевой центр, УКЦ) – приложение, предназначенное для управления ключевой структурой защищенной сети и выполнения функций удостоверяющего центра, позволяющее решить следующие задачи:

– генерация ключевой информации, выпуск ключевых контейнеров, автоматизация реагирования на компрометацию ключей пользователей;

– издание сертификатов для аутентификации, электронной подписи, шифрования и других криптографических операций.

2.19.Программно-аппаратный комплекс ViPNet Coordinator – шлюз безопасности, предназначенный для построения виртуальной защищенной сети ViPNet и обеспечения безопасной передачи данных между ее защищенными сегментами, а также фильтрации IP-трафика.

2.20.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.

2.21.Туннелируемый узел – узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне (третий уровень сетевой модели OSI), но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

III. Назначение, порядок подключения к защищенной сети передачи данных, обновления справочно-ключевой информации (информации первичного межсетевого экспорта) и предоставления доступа к ее информационным ресурсам

3.1. Защищенная сеть передачи данных предназначена для создания защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи путем организации виртуальной защищенной сети.

Структурно защищенная сеть передачи данных представляет собой совокупность технических и программных средств, средств защиты информации, в том числе средств криптографической защиты информации, а также программных комплексов, предназначенных для выполнения основных функций защищенной сети передачи данных:

– регистрация абонентских пунктов (сетевых узлов) в защищенной сети передачи данных;

– распределение задач для абонентских пунктов (сетевых узлов), программно-аппаратных комплексов ViPNet Coordinator;

– установление и изменение разрешенных связей между абонентскими пунктами (сетевыми узлами) и туннелируемыми узлами;

– формирование и рассылка адресных справочников, справочно-ключевой информации и (или) информации первичного межсетевого экспорта, формируемой УКЦ, для абонентских пунктов (сетевых узлов);

– формирование справочников для удостоверяющего и ключевого центра;

– формирование ключей пользователей, абонентских пунктов (сетевых узлов), паролей.

3.2. Последовательность действий, выполняемых при регистрации Пользователей ЗСПД и их представителей:

а) прием, проверка правильности оформления заявления и прилагаемых к нему документов, наличия технических средств, последующая регистрация;

б) конфигурирование параметров абонентского пункта (сетевого узла) и полномочий пользователя;

в) формирование справочно-ключевой информации (дистрибутива ключей, пароля и парольной фразы) и (или) файла информации первичного межсетевого экспорта;

г) установление связей между абонентскими пунктами, сетевыми и туннелируемыми узлами при наличии соответствующего заявления.

3.3. Установление личности пользователя ЗСПД или его представителя, действующего на основании доверенности, оформленной в установленном законом порядке, осуществляется по основному документу, удостоверяющему личность гражданина Российской Федерации на территории Российской Федерации.

3.4. Основанием для регистрации пользователя ЗСПД в защищенной сети передачи данных является предоставление уполномоченному должностному лицу оператора следующего перечня документов и технических средств:

– два экземпляра заявления о присоединении к Регламенту, согласно форме, указанной в Приложении № 1 к Регламенту;

– два экземпляра заявления на создание справочно-ключевой информации (информации первичного межсетевого экспорта), согласно форме, указанной в Приложении № 3 к Регламенту (оформляется при каждой смене справочно-ключевой информации, информации межсетевого экспорта);

– копия действующей лицензии на право использования программного комплекса ViPNet Client (в случае подключения с использованием программного комплекса ViPNet Client) (верность копии должна быть удостоверена уполномоченным должностным лицом);

– копия действующей лицензии на право использования программного комплекса ViPNet Administrator (в случае подключения с использованием технологии межсетевого взаимодействия) (верность копии должна быть удостоверена уполномоченным должностным лицом);

– копия документа, подтверждающего выполнение требований безопасности, предъявляемых к информационным системам персональных данных, не ниже уровня защищенности персональных данных, установленного для соответствующей информационной системы персональных данных, к которой предоставляется доступ (в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных) (верность копии должна быть удостоверена уполномоченным должностным лицом);

– копию универсального передаточного документа (товарной накладной) на приобретенные программные и (или) программно-аппаратные комплексы защищенной сети передачи данных (верность копии должна быть удостоверена уполномоченным должностным лицом);

– копия организационно-распорядительного акта о назначении Пользователя ЗСПД (его представителя) владельцем справочно-ключевой информации, в случае, если Пользователем ЗСПД выступает руководитель организации – предоставляется копия организационно-распорядительного акта о назначении руководителя на должность (верность копий должна быть удостоверена уполномоченным должностным лицом);

– доверенность, согласно форме, указанной в Приложении № 4 к Регламенту (в случае, если справочно-ключевую информацию, файл информации межсетевого экспорта получает не ее владелец);

– основной документ, удостоверяющий личность гражданина Российской Федерации на территории Российской Федерации;

– отчуждаемый носитель информации объемом не менее 512 Мб.

Оператор оставляет за собой право запросить у стороны Регламента дополнительные сведения, необходимые для проведения проверочных

мероприятий, доступ к которым не ограничен действующим законодательством.

Заявитель (сторона Регламента) несет персональную ответственность за достоверность сведений, предоставленных оператору для регистрации в защищенной сети передачи данных, формирования справочно-ключевой информации и (или) информации межсетевого экспорта.

Уполномоченное должностное лицо оператора проверяет полноту, правильность заполнения и достоверность сведений, содержащихся в предъявленных документах.

В случае если предоставленный комплект документов и технических средств оформлен с нарушением требований, установленных Регламентом, полученный комплект возвращается заявителю до устранения указанных несоответствий.

В случае соответствия предоставленного комплекта документов и технических средств требованиям Регламента уполномоченное должностное лицо оператора регистрирует документы в соответствующих реестрах.

Время регистрации справочно-ключевой информации (информации межсетевого экспорта) составляет не менее 40 минут. В случае если на момент регистрации предоставленного комплекта документов уполномоченное должностное лицо оператора выполняет иные процедуры создания и (или) обновления справочно-ключевой информации (информации межсетевого экспорта) или количество экземпляров справочно-ключевой информации (информации межсетевого экспорта), запрашиваемых заявителем более двух, оператор оставляет за собой право увеличить время рассмотрения комплекта документов, уведомив об этом заявителя.

Справочно-ключевая информация (информация межсетевого экспорта) выдается на срок не более 12 месяцев с момента регистрации, после чего аннулируется оператором.

3.5. Установка справочно-ключевой информации (информации межсетевого экспорта) (первичная инициализация) производится с использованием выданной ключевой информации и ключевых документов пользователем ЗСПД самостоятельно.

Замена (плановая, внеплановая) справочно-ключевой информации производится (информации межсетевого экспорта) в порядке, предусмотренном пунктом 3.4 настоящего Регламента.

Обновление (актуализация) справочно-ключевой информации (информации межсетевого экспорта) производится автоматически средствами защищенной сети передачи данных в течение двух рабочих дней.

3.6. Установление связей между абонентскими пунктами, предоставление доступа к информационным ресурсам защищенной сети передачи данных производится на основании заявки, указанной в Приложении № 5 к Регламенту, направленной на сетевой узел Администратора защищенной сети передачи данных или предоставленной в бумажном виде.

При получении заявки, обновление справочно-ключевой информации (информации межсетевого экспорта) формируется и высылается

на абонентский пункт автоматически средствами защищенной сети передачи данных.

В случае если изменение (добавление, удаление) абонентского пункта, предоставление доступа к информационным ресурсам влечет внесение изменений в конфигурации доверенных сетей, обновление справочно-ключевой информации (информации межсетевого экспорта) будет сформировано и выслано на абонентский пункт автоматически после обработки полученных изменений администратором соответствующей доверенной сети.

3.7. Взаимодействие (техническая поддержка) пользователей ЗСПД и их представителей с оператором.

При возникновении у пользователей ЗСПД и их представителей необходимости получения консультации по работе с программно-аппаратными и программными комплексами ViPNet следует обращаться в орган криптографической защиты дирекции по информационной безопасности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации согласно контактной информации, указанной в пункте 1.6. настоящего Регламента.

Перед обращением за консультацией необходимо проверить наличие:

– актуальной версии программного обеспечения, в том числе его сборки;

– действительной справочно-ключевой информации (информации межсетевого экспорта);

– актуального часового пояса, даты и времени;

– корректно настроенных средств защиты информации (средства антивирусной защиты, межсетевой экран, средства контроля от несанкционированного доступа и иные);

– наличие Интернет-подключения;

– корректной настройки программно-аппаратного и (или) программного комплекса ViPNet;

– доступности необходимых абонентских пунктов.

В случае, если указанные выше действия не приведут к положительному результату, оформить обращение с указанием:

– номера защищенной сети передачи данных;

– пользователя ЗСПД (владельца справочно-ключевой информации (информации межсетевого экспорта);

– используемых СКЗИ;

– краткого и информативного изложения сути проблемы.

Уполномоченное должностное лицо оператора самостоятельно определяет уровень критичности (важности) возникшей неисправности и оставляет за собой право устанавливать приоритет обработки поступающих заявок.

IV. Защита информации

4.1. Криптографическая защиты информации

Программные и (или) программно-аппаратные комплексы защищенной сети передачи данных необходимо эксплуатировать согласно технической (эксплуатационной) документации к таким средствам.

Электронные ключевые носители многократного (долговременного) использования должны храниться в местах, исключающих бесконтрольный доступ к ним.

Хранимые и (или) используемые пользователем ЗСПД или его представителем программные и (или) программно-аппаратные комплексы, техническая (эксплуатационная) документация к ним, ключевые документы подлежат поэкземплярному учету согласно установленным формам.

Средства вычислительной техники, на которых установлены программные комплексы ViPNet, должны быть учтены и оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены программные и (или) программно-аппаратные комплексы защищенной сети передачи данных, должны обеспечивать сохранность конфиденциальной информации, предаваемой в инфраструктуре защищенной сети передачи данных.

Пользователю ЗСПД (его представителю), использующему программные и (или) программно-аппаратные комплексы защищенной сети передачи данных, переданные оператором в безвозмездное пользование на основании договора, при внесении любых изменений, связанных с работоспособностью программных и (или) программно-аппаратных комплексов защищенной сети передачи данных, необходимо уведомлять оператора о таких изменениях не менее чем за один рабочий день до предстоящих изменений.

Пользователю ЗСПД (его представителю), использующему программные комплексы защищенной сети передачи данных, в случае планируемой замены аппаратного средства, на котором установлен программный комплекс защищенной сети передачи данных, либо в случае переустановки такого комплекса, необходимо уведомить оператора не менее чем за один рабочий день до предстоящих изменений.

4.2. Инженерно-техническая защита информации

Технические средства защищенной сети передачи данных размещаются режимных (специальных, выделенных) помещениях.

Режимные (специальные) помещения должны быть оборудованы:

– системой контроля управления доступом;

– исполнительным устройством идентификации по пропускным картам с установленным режимом шифрования не ниже security level 2 (рекомендуемый режим шифрования – security level 3);

– исполнительным устройством электромеханического типа.

Технические средства защищенной сети передачи данных подключаются к общегородской сети электроснабжения, электрические сети и

электрооборудование должны соответствовать требованиям следующих документов:

– Правила устройства электроустановок;

– Правила технической эксплуатации электроустановок потребителей электрической энергии, утверждены приказом Минэнерго России от 12 августа 2022 г. № 811;

– Правила по охране труда при эксплуатации электроустановок, утверждены приказом Минтруда России от 15.12.2020 № 903н.

Технические средства защищенной сети передачи данных подключаются к источникам бесперебойного питания, обеспечивающим их работу в течение не менее 1 часа после прекращения основного электроснабжения.

Режимные (специальные) помещения оборудуются средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Режимные (специальные) помещения оборудуются системой пожарной сигнализации и дымоудаления. Пожарная безопасность обеспечивается в соответствии с нормами и требованиями СНиП 21-01-97 по классу ФЗ.5, установленными законодательством Российской Федерации.

4.3. Программно-аппаратная защита информации

Средства вычислительной техники, входящие в состав защищенной сети передачи данных, оснащаются средствами антивирусной защиты информации, средствами контроля от несанкционированного доступа, сертифицированными в системе сертификации ФСТЭК России.

Средства защиты информации, в том числе средства криптографической защиты информации, установленные на средствах вычислительной техники, входящих в состав защищенной сети передачи данных, подлежат ежедневному контролю целостности. Система контроля целостности основывается на программном контроле целостности до загрузки операционной системы.

Контроль целостности технических средств, входящих в состав защищенной сети передачи данных, обеспечивается опечатыванием (пломбировкой) корпусов устройств, препятствующим их неконтролируемому вскрытию. Опечатывание (пломбировка) технических средств выполняется перед их вводом в постоянную (промышленную) эксплуатацию, после выполнения регламентных работ.

4.4. Организационная защита информации

Уполномоченные должностные лица оператора должны:

– иметь высшее образование по специальности (направлению подготовки) в области информационной безопасности и (или) профессиональную переподготовку в области информационной безопасности в объеме не менее 512 часов по программе, согласованной с ФСТЭК России и ФСБ России, а также стаж работы в этой области не менее одного года;

– периодически повышать квалификацию в областях знаний согласно занимаемым должностям.

Охрана здания и режимных (специальных) помещений должна обеспечивать:

– обнаружение и задержание нарушителей, пытающихся проникнуть в здание и (или) режимные (специальные) помещения оператора;

– сохранность материальных ценностей и документов;

– предупреждение происшествий и ликвидацию их последствий.

4.5. Правовая защита информации

Для документирования деятельности, связанной с работой со средствами криптографической защиты информации, в том числе с использованием программных и (или) программно-аппаратных комплексов защищенной сети передачи данных, необходимо разработать внутренние организационно-распорядительные документы, регламентирующие:

– порядок обеспечения безопасности конфиденциальной информации, с использованием средств криптографической защиты информации;

– установление границ контролируемой зоны;

– назначение ответственных пользователей средств криптографической защиты информации;

– допуск физических лиц к работе со средствами криптографической защиты информации;

– допуск физических лиц в режимные (специальные) помещения со средствами криптографической защиты информации;

– должностные обязанности физических лиц, допущенных к работе со средствами криптографической защиты информации;

– ввод в эксплуатацию (вывод из эксплуатации) средств криптографической защиты информации, уничтожение средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

– поэкземплярный учет средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

– фиксацию и учет процедуры опечатывания (пломбирования) технических средств защищенной сети передачи данных;

– учет хранилищ ключевых документов, технической и эксплуатационной документации к ним;

– учет ключей от хранилищ ключевых документов, технической и эксплуатационной документации к ним;

– организацию и планирование внутреннего контроля за эксплуатацией средств криптографической защиты информации;

– проверку исправности системы контроля управления доступом, исполнительного оборудования, сигнализации.

V. Права и обязанности сторон Регламента

5.1. Права и обязанности оператора защищенной сети передачи данных:

Оператор обязан:

– обеспечивать регистрацию пользователей ЗСПД в инфраструктуре защищенной сети передачи данных в соответствии со сведениями, полученными из документов, предоставляемых заявителем;

– изготавливать справочно-ключевую информацию (информацию межсетевого экспорта);

– обеспечивать конфиденциальность, целостность и доступность изготовляемой справочно-ключевой информации (информации межсетевого экспорта);

– обеспечивать уникальность регистрационной информации пользователя ЗСПД, вносимой в программный комплекс ViPNet Administrator, используемой для идентификации владельцев справочно-ключевой информации (информации межсетевого экспорта);

– аннулировать (отзывать) регистрацию пользователя ЗСПД и выданную справочно-ключевую информацию (информацию межсетевого экспорта);

– уведомлять владельца справочно-ключевой информации (информации межсетевого экспорта) о фактах, которые стали известны уполномоченному должностному лицу оператора и которые существенным образом могут сказаться на возможности дальнейшего использования справочно-ключевой информации (нарушение конфиденциальности, целостности и доступности);

– добавлять, удалять связи между абонентскими пунктами (сетевыми узлами) по согласованному с оператором заявлению пользователя ЗСПД;

Оператор вправе:

– запросить у заявителя надлежащим образом оформленные документы и технические средства, необходимые для регистрации в защищенной сети передачи данных;

– отказать в регистрации и изготовлении справочно-ключевой информации (информации межсетевого экспорта) в случае ненадлежащего оформления документов или предоставлении неполного комплекта документов и (или) технических средств.

5.2. Права и обязанности пользователя ЗСПД (его представителя):

Пользователь ЗСПД (его представитель) обязан:

– предоставлять достоверную информацию и необходимые документы, технические средства, при регистрации, аннулировании (отзыве) регистрации, добавлении или удалении связей с абонентскими пунктами (сетевыми узлами) в защищенной сети передачи данных;

– хранить справочно-ключевую информацию (информацию межсетевого экспорта), пароль и парольную фразу в строгом соответствии с действующим законодательством Российской Федерации, предпринимать все возможные меры для предотвращения нарушения конфиденциальности,

целостности и доступности справочно-ключевой информации (информации межсетевого экспорта), пароля, парольной фразы и информации, предаваемой в защищенной сети передачи данных;

– письменно информировать оператора о фактах компрометации справочно-ключевой информации (информации межсетевого экспорта), пароля и парольной фразы;

– соблюдать требования раздела IV настоящего Регламента в части создания системы защиты информации, в том числе применения криптографических, инженерно-технических, программно-аппаратных, организационных и правовых мер защиты информации на объектах и в информационно-телекоммуникационной инфраструктуре, подключенной к защищенной сети передачи данных;

– использовать справочно-ключевую информацию только для целей, разрешенных соответствующими областями использования, определенными в сертификате ключа (при наличии);

– обновлять справочно-ключевую информацию (информацию межсетевого экспорта) не реже одного раза в 12 (двенадцать) месяцев с момента ее создания;

– применять при защищенном электронном взаимодействии, в том числе защищенном электронном документообороте, только действительную справочно-ключевую информацию;

– при внесении любых изменений, связанных с функционированием программных и программно-аппаратных комплексов защищенной сети передачи данных, уведомлять оператора не менее чем за один рабочий день до предстоящих изменений;

– в случае замены аппаратного средства, на котором был установлен программный комплекс ViPNet Client, либо в случае переустановки такого комплекса, уведомлять оператора не менее чем за один рабочий день до предстоящих изменений.

Пользователь ЗСПД (его представитель) вправе:

– обратиться к оператору для обновления (замены) справочно-ключевой информации (информации межсетевого экспорта);

– обратиться к оператору за консультацией в порядке, предусмотренном пунктом 3.7 настоящего Регламента.

VI. Условия межсетевого взаимодействия

6.1. Для организации взаимодействия между защищенной сетью передачи данных пользователя ЗСПД и защищенной сетью передачи данных Академии производится установление доверительных отношений в рамках межсетевого взаимодействия.

6.2. Установление доверительных отношений между защищенными сетями осуществляется при условии заключения между оператором и пользователем ЗСПД соглашения о межсетевом взаимодействии, согласно форме, указанной в приложении № 6 к Регламенту.

6.3. Технологическое взаимодействие по установлению доверительных отношений между оператором и пользователем ЗСПД осуществляется в соответствии с технической (эксплуатационной) документацией на программные и программно-аппаратные комплекты, используемые в защищенной сети передачи данных.

VII. Изменение параметров подключения к защищенной сети передачи данных

7.1. Изменение параметров подключения абонентских пунктов (сетевых узлов) осуществляется оператором при наступлении следующих событий:

– изменение официального наименования юридического лица (органа, организации) – пользователя ЗСПД;

– установленный факт нарушения законодательства Российской Федерации в области информации, информационных технологий и защиты информации, требований настоящего Регламента;

– компрометация справочно-ключевой информации (информации межсетевого экспорта), пароля и парольной фразы.

7.2. Порядок действий при наступлении событий, указанных в пункте 7.1 настоящего Регламента:

№ п/п	Наименование события	Предпринимаемые оператором действия
1.	Изменение официального наименования юридического лица (органа, организации)	Изменение наименования абонентского пункта (сетевого узла)
2.	Установленный факт нарушения законодательства Российской Федерации в области информации, информационных технологий и защиты информации, требований настоящего Регламента	Отключение абонентского пункта (сетевого узла), расследование инцидента информационной безопасности
3.	Компрометация справочно-ключевой информации (информации межсетевого экспорта), пароля и парольной фразы	
4.	Предоставление не полной информации о подключаемых абонентских пунктах (сетевых узлах)	Отказ в принятии межсетевого экспорта

VIII. Ответственность

8.1. Сторона Регламента, не исполнившая или ненадлежащим образом исполнившая свои обязательства в соответствии с Регламентом, несет ответственность за убытки, причиненные другой стороне, в соответствии с действующим законодательством Российской Федерации.

8.2. Оператор не несет ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях:

– если оператор обоснованно полагался на сведения, указанные в документах, предоставленных заявителем;

– подделки, подлога либо иного искажения заявителем (пользователем ЗСПД, его представителем и иными третьими лицами) информации, содержащейся в документах, предоставленных заявителем;

8.3. При возникновении конфликтных ситуаций стороны Регламента предпринимают все необходимые действия для урегулирования вопросов, которые могут возникнуть в рамках действия Регламента, путем совместных переговоров.

8.4. Споры между сторонами Регламента, не урегулированные в процессе совместных переговоров, разрешаются в порядке, предусмотренном действующим законодательством Российской Федерации.

Приложение № 1 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

(оформляется на официальном бланке юридического лица)

Заявление
о присоединении к Регламенту эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации"

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Регламенту эксплуатации и подключения к защищенной сети передачи данных Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (далее – оператор), условия которого определены оператором и опубликованы на официальном сайте по адресу – www.ranepa.ru

Адрес места нахождения:

указать адрес места нахождения юридического лица (органа, организации)

Государственный регистрационный номер записи о создании юридического лица (ОГРН):

(указать ОГРН)

Индивидуальный номер налогоплательщика (ИНН):

Работник, уполномоченный по вопросам присоединения к Регламенту (наименование должности, Ф.И.О., последнее – при наличии, номер телефона, адрес электронной почты):

С Регламентом эксплуатации и подключения к защищенной сети передачи данных Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации и приложениями к нему ознакомлен, обязуюсь исполнять требования указанного документа.

должность руководителя	подпись	расшифровка подписи

(оборотная сторона)

Заявление о присоединении к Регламенту эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" зарегистрировано в реестре пользователей защищенной сети передачи данных:

регистрационный № _____ "_____" _____ 20___ г.

должность уполномоченного лица	подпись	расшифровка подписи

Приложение № 2 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

(оформляется на официальном бланке юридического лица)

Отзыв заявления

о присоединении к Регламенту эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации"

_____

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

_____

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

_____

Адрес места нахождения:

_____

указать адрес места нахождения юридического лица (органа, организации)

Государственный регистрационный номер записи о создании юридического лица (ОГРН):

_____

(указать ОГРН)

Индивидуальный номер налогоплательщика (ИНН):

_____

Работник, уполномоченный по вопросам присоединения к Регламенту (наименование должности, Ф.И.О., последнее – при наличии, номер телефона, адрес электронной почты):

уведомляет об отзыве (аннулировании) заявления о присоединении к Регламенту эксплуатации и подключения к защищенной сети передачи данных Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, зарегистрированного в реестре пользователей защищенной сети передачи данных, регистрационный № _____ "_____"_____20___г.

_____	_____	_____
должность руководителя	подпись	расшифровка подписи

(оборотная сторона)

Заявление о присоединении к Регламенту эксплуатации и подключения к защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации", зарегистрированное в реестре пользователей защищенной сети передачи данных:

регистрационный № _____ "_____"_____20___г.,

отозвано (аннулировано) "_____"_____20___г.

_____	_____	_____
должность уполномоченного лица	подпись	расшифровка подписи

Приложение № 3 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

(оформляется на официальном бланке юридического лица)

Заявление

на создание справочно-ключевой информации (информации первичного межсетевого экспорта)

_____

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

_____

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

_____

просит сформировать справочно-ключевую информацию на предоставленное техническое средство для подключения к защищенной сети передач данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" согласно следующим данным:

№ п/п	Наименование сведений	Предоставляемые сведения
1.	Полное наименование юридического лица	
2.	Сокращенное наименование юридического лица	
3.	ОГРН	
4.	ИНН	
5.	Юридический адрес	
6.	Фактический адрес	
7.	Наименование должности, Ф.И.О., последнее – при наличии, номер телефона, адрес электронной почты заявителя (его представителя)	
8.	Наименование информационных (автоматизированных) систем, доступ к которым необходим на законном основании	(заполняется в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных)

_____ _____ _____

должность руководителя подпись расшифровка подписи

Приложение № 4 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

Доверенность

место и дата совершения доверенности

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

уполномочивает:

(должность, фамилия, имя, отчество, последнее – при наличии, сведения о документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации с указанием серии, номера, даты выдачи и выдавшем его органе)

выступать в роли уполномоченного представителя пользователя защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" (далее – оператор) и осуществить следующие действия:

1. Подать заявление на создание справочно-ключевой информации (информации первичного межсетевого экспорта).
2. Получить от уполномоченного должностного лица оператора справочно-ключевую информацию (информацию первичного межсетевого экспорта).
3. Расписаться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по "_____" _____ 20___ г.

Подпись уполномоченного представителя:

удостоверяю:

должность руководителя	подпись	расшифровка подписи

Приложение № 5 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

(оформляется на официальном бланке юридического лица)

Заявление

на добавление связей между абонентскими пунктами (сетевыми узлами) защищенной сети передачи данных

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

просит для абонентского пункта (сетевого узла):

(наименование и идентификационный номер абонентского пункта (сетевого узла)

добавить / удалить связь со следующими абонентскими пунктами (сетевыми узлами):

№ п/п	Наименование абонентского пункта (сетевого узла)	Номер ЗСПД, в которой зарегистрирован абонентский пункт (сетевой узел)	Обоснование необходимости
1	2	3	4

добавить / удалить связь со следующими туннелируемыми IP-адресами:

№ п/п	Туннелируемый IP-адрес	Обоснование необходимости
1	2	3

Обоснование необходимости предоставления доступа (установления связи с туннелируемыми IP-адресами):

должность руководителя	подпись	расшифровка подписи

Приложение № 5 к Регламенту эксплуатации и подключения к защищенной сети передачи данных

Форма

Гриф секретности
или ограничительная пометка
Экз. №

Соглашение
об установлении межсетевого взаимодействия

_____	Москва	_____
дата	место подписания	номер

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации", в лице директора по информационной безопасности (указать фамилию и инициалы), действующего на основании (указать правовые основания), в дальнейшем именуемая Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, с одной стороны, и

_____
(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

_____
(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

_____

именуемое в дальнейшем

_____
(краткое наименование юридического лица (органа, организации)

с другой стороны, совместно именуемые "Стороны", заключили настоящее соглашение о нижеследующем.

I. Предмет соглашения

1. Стороны договорились об установления межсетевого взаимодействия и доверия между защищенной сетью передачи данных (указать номер сети) Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации и защищенной сетью передачи данных (указать номер сети)

_____
(краткое наименование юридического лица (органа, организации)

Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между разрешенными абонентскими пунктами (сетевыми узлами) защищенных сетей передачи данных сторон соглашения.

1.2. Отношения между стороны регулируются следующими нормативными документами:

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, № 31, 31.07.2006, ст. 3448);

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701);

– Указ Президента Российской Федерации от 06.03.1997 № 188 "Об утверждении перечня сведений конфиденциального характера (Собрание законодательства Российской Федерации, № 10, 10.03.97, ст. 1127);

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (Собрание законодательства Российской Федерации, № 45, 05.11.2012, ст. 6257);

– Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13 июня 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" (Зарегистрировано в Минюсте РФ 06 августа 2001 г. № 2848);

– Приказ Федеральной службы безопасности Российской Федерации от 09 февраля 2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (Зарегистрировано в Минюсте РФ 03 марта 2005 г. № 6382);

– Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" (Зарегистрировано в Минюсте России 18 августа 2014 г. № 33620).

1.3. Взаимодействие сторон осуществляется на безвозмездной основе.

II. Права и обязанности сторон

2.1. При организации межсетевого взаимодействия Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации принимает на себя следующие права и обязанности:

а) обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов защищенной сети передачи данных в границах зоны своей ответственности.

б) обеспечивает организацию взаимодействия с абонентскими пунктами (сетевыми узлами) защищенной сети передачи данных согласно разделу III настоящего соглашения;

2.2. При организации межсетевого взаимодействия

_____

(краткое наименование юридического лица (органа, организации)

принимает на себя следующие права и обязанности:

а) обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов защищенной сети передачи данных в границах зоны своей ответственности;

б) обеспечивает организацию взаимодействия с абонентскими пунктами (сетевыми узлами) защищенной сети передачи данных согласно разделу III настоящего соглашения.

2.3. Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между ViPNet NCC защищенных сетей передачи данных. Файлы информации первичного межсетевого экспорта импортируются в ViPNet NCC соответствующей сети (приложение № 1).

III. Организация межсетевого взаимодействия

3.1. Лицами, ответственными за организацию межсетевого взаимодействия являются Администраторы ЗСПД Сторон.

Установление доверия между защищенными сетями передачи данных Сторон обеспечивается организацией межсетевого взаимодействия между абонентскими пунктами (сетевыми узлами) Администраторов ЗСПД Сторон через программно-аппаратный комплекс ViPNet Coordinator.

3.2. Процедура организации межсетевого взаимодействия завершается подписанием протокола установления межсетевого взаимодействия (приложение № 2).

3.3. Установление связей между абонентскими пунктами (сетевыми узлами) защищенных сетей передачи данных Сторон осуществляется Администраторами ЗСПД Сторон на основании заявки (приложение № 3).

3.4. По факту согласования обновленного реестра абонентских пунктов (сетевых узлов) Администраторы ЗСПД Сторон обмениваются файлами информации межсетевого экспорта и производят необходимые действия для установления связей между абонентскими пунктами (сетевыми узлами).

3.5. Реестр абонентских пунктов (сетевых узлов) защищенных сетей передачи данных Сторон и связей между ними фиксируется в матрице связей (приложение № 4).

IV. Профилактические мероприятия

4.1. Проведение профилактических мероприятий по поддержанию работоспособности (техническое обслуживание) программных и программно-аппаратных средств защищенной сети передачи данных осуществляется Сторонами в границах зоны своей ответственности при соблюдении следующих условий:

– срок проведения профилактических мероприятий (технического обслуживания) не должен превышать 1 рабочий день;

– профилактические мероприятия (техническое обслуживание) должно проводится в пределах первых пяти дней календарного месяца;

– о сроках проведения профилактических мероприятий (технического обслуживания) Сторона-инициатор должна оповестить вторую Сторону заблаговременно, не позднее, чем за 7 дней до дня проведения таких мероприятий.

V. Ответственность сторон

5.1. Стороны несут ответственность за обеспечение безопасности информации, передаваемой по защищенной сети передачи данных, в границах зоны своей ответственности в соответствии с законодательством Российской Федерации.

5.2. Стороны не несут ответственность за содержание информации, передаваемой по защищенной сети передачи данных.

VI. Срок действия соглашения

6.1. Настоящее соглашения вступает в силу с момента его подписания и действует в течение одного года.

6.2. Настоящее соглашение может быть досрочно расторгнуто по обоюдному согласию Сторон, либо в одностороннем порядке с предупреждением другой Стороны за два месяца до расторжения соглашения.

VII. Форс-мажор

7.1. При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего соглашения одной из Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от Сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую Сторону в течение трех рабочих дней

с предоставлением документов компетентных органов, подтверждающих наличие данных обстоятельств.

VIII. Дополнительные условия

8.1. При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между защищенными сетями передачи данных, Стороны прилагают совместные усилия по устранению этих обстоятельств.

8.2. Любые изменения и дополнения к соглашению действительны, если они совершены в письменной форме и подписаны уполномоченными представителями Сторон.

8.3. Настоящее соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

8.4. Настоящее соглашение имеет следующие приложения в качестве неотъемлемой части:

а) приложение № 1 – состав защищенных сетей передачи данных и границы зон ответственности сторон;

б) приложение № 2 – форма протокола установления межсетевого взаимодействия между защищенными сетями передачи данных;

в) приложение № 3 – форма заявления на добавление абонентского пункта (сетевого узла) в файл информации межсетевого экспорта защищенной сети передачи;

г) приложение № 4 – форма заявления на добавление туннелируемого IP-адреса (координатора или иного устройства) в файл информации межсетевого экспорта защищенной сети передачи данных;

д) приложение № 5 – реестр абонентских пунктов (сетевых узлов) защищенных сетей передачи данных Сторон и связей между ними (матрица связей).

Реквизиты и подписи сторон

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" Юридический адрес: 119571, город Москва, пр-кт Вернадского, д. 82 стр. 1 ИНН/КПП: 7729050901/772901001 ОГРН: 1027739610018 **Директор по информационной безопасности**	Наименование юридического лица (органа, организации) с указанием организационно-правовой формы

Приложение № 1 к Соглашению об установлении межсетевого взаимодействия

Гриф секретности
или ограничительная пометка
Экз. №

СОСТАВ
защищенных сетей передачи данных и границы зон ответственности сторон

1. Состав защищенной сети передачи данных федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации":

а) программный комплекс ViPNet Administrator, которым управляется защищенная сетью передачи данных № (указать номер ЗСПД);

б) шлюзовой программно-аппаратный комплекс ViPNet Coordinator, через который проходит весь сетевой трафик защищенной сети передачи данных № (указать номер ЗСПД);

в) абонентские пункты (сетевые узлы) защищенной сети передачи данных № (указать номер ЗСПД);

2. Состав защищенной сети передачи данных

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

а) программный комплекс ViPNet Administrator, которым управляется защищенная сетью передачи данных № (указать номер ЗСПД);

б) шлюзовой программно-аппаратный комплекс ViPNet Coordinator, через который проходит весь сетевой трафик защищенной сети передачи данных № (указать номер ЗСПД);

в) абонентские пункты (сетевые узлы) защищенной сети передачи данных № (указать номер ЗСПД).

3. Схема межсетевого взаимодействия сторон с указанием границ зон ответственности

Схема межсетевого взаимодействия сторон с указанием границ зон ответственности представлена на рисунке 1.

4. Граница зон ответственности сторон

4.1. Федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" несет

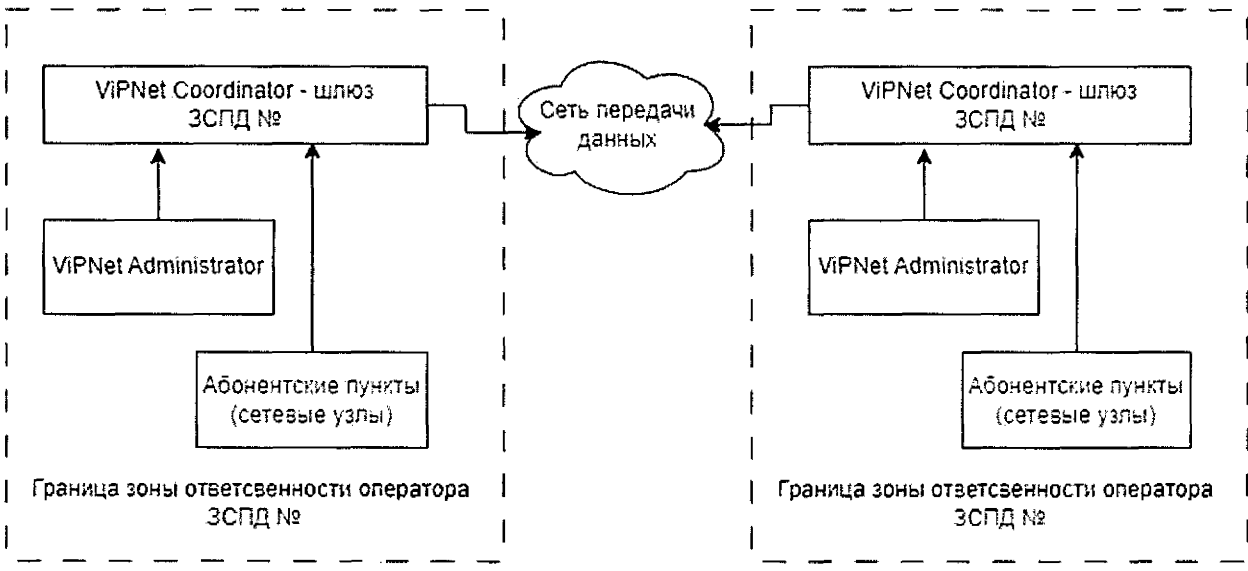
ответственность за работоспособность программных и программно-аппаратных комплексов защищенной сети передачи данных № (указать номер ЗСПД) в соответствии со схемой, представленной на рисунке 1.

4.2. _____

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

несет ответственность за работоспособность программных и программно-аппаратных комплексов защищенной сети передачи данных № (указать номер ЗСПД) в соответствии со схемой, представленной на рисунке 1.

Рис. 1 - Схема межсетевого взаимодействия сторон с указанием границ зон ответственности (необходимо вписать номера сетей):



4.3. Стороны несут ответственность за контроль передачи данных через своего провайдера.

4.4. Стороны не несут ответственность за прекращение передачи данных, вызванных по вине провайдера.

5. Ответственность сторон

5.1. В случае нарушения работоспособности программных и программно-аппаратных комплексов защищенной сети передачи данных № (указать номер ЗСПД) федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" несет ответственность за в соответствии с законодательством Российской Федерации.

5.2. В случае нарушения работоспособности программных и программно-аппаратных комплексов защищенной сети передачи данных № (указать номер ЗСПД)

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

несет ответственность за в соответствии с законодательством Российской Федерации.

Реквизиты и подписи сторон

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации" Юридический адрес: 119571, город Москва, пр-кт Вернадского, д. 82 стр. 1 ИНН/КПП: 7729050901/772901001 ОГРН: 1027739610018 **Директор по информационной безопасности**	Наименование юридического лица (органа, организации) с указанием организационно-правовой формы

Приложение № 2 к Соглашению об установлении межсетевого взаимодействия

Форма

Гриф секретности
или ограничительная пометка
Экз. №

Утверждаю
Директор по информационной безопасности
федерального государственного бюджетного образовательного учреждения высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации"

_____
(подпись)
"___"_____20____г.

Утверждаю
Наименование должности руководителя юридического лица (органа, организации)

_____
(подпись)
"___"_____20____г.

ПРОТОКОЛ

установления межсетевого взаимодействия между защищенными сетями передачи данных

_____	Москва	_____
дата	место подписания	номер

1. Межсетевое взаимодействие между защищенными сетями передачи данных установлено:

Номер ЗСПД	Наименование организации
	Федеральное государственное бюджетное образовательное учреждение высшего образования "Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации"
	Наименование юридического лица (органа, организации) с указанием организационно-правовой формы

2. Процедуру установления межсетевого взаимодействия осуществили:

Номер	Должность администратора ЗСПД	Фамилия, имя отчество

ЗСПД		(последнее – при наличии)

3. Передача файлов информации первичного межсетевого и ответного экспорта защищенных сетей передачи данных осуществлена, конфиденциальность и целостность указанных файлов не нарушена.

4. Использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в защищенной сети передачи данных № (указать номер ЗСПД).

5. Назначены серверы-маршрутизаторы, выполняющие функции сетевого шлюза в соответствующей защищенной сети передачи данных:

а) в сети № (указать номер ЗСПД) – указать ip-адрес шлюза;

б) в сети № (указать номер ЗСПД) – указать ip-адрес шлюза;

6. Произведен обмен справочниками защищенных сетей передачи данных, созданы связи между абонентскими пунктами (сетевыми узлами).

Подписи сторон

Администратор защищенной сети передачи данных № (указать номер ЗСПД)	Администратор защищенной сети передачи данных № (указать номер ЗСПД)
_____ (подпись)	_____ (подпись)
"___"_____20____г.	"___"_____20____г.

Приложение № 3 к Соглашению об установлении межсетевого взаимодействия

Форма

Гриф секретности
или ограничительная пометка
Экз. №

(оформляется на официальном бланке юридического лица)

Заявление
на добавление абонентского пункта (сетевого узла)
в файл информации межсетевого экспорта защищенной сети передачи данных № (указать номер ЗСПД)

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

просит организовать защищенный канал связи в соответствии со следующей информацией:

№ п/п	Наименование сведений	Предоставляемые сведения
1.	Полное наименование юридического лица	
2.	Сокращенное наименование юридического лица	
3.	ОГРН	
4.	ИНН	
5.	Юридический адрес	
6.	Фактический адрес	
7.	Наименование абонентского пункта (сетевого узла), однозначно идентифицирующее абонентский пункт (сетевой узел) (инвентарный, учетный, серийный или иной номер)	
8.	Наименование структурного подразделения, в котором	

	эксплуатируется абонентский пункт (сетевой узел)	
9.	Фамилия, имя, отчество (последнее – при наличии) работника, допущенного к эксплуатации абонентского пункта (сетевого узла)	
10.	Фамилия, имя, отчество (последнее – при наличии) администратора ЗСПД	
11.	Контактная информация (последнее – при наличии) администратора ЗСПД	
12.	Номер ЗСПД	
13.	Наименование информационных (автоматизированных) систем, доступ к которым необходим на законном основании	(заполняется в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных)
14.	Обоснование необходимости предоставления доступа (установления связи с туннелируемыми IP-адресами)	(заполняется в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных)

_____	_____	_____
должность руководителя	подпись	расшифровка подписи

Приложение № 4 к Соглашению об установлении межсетевого взаимодействия

Форма

Гриф секретности
или ограничительная пометка
Экз. №

(оформляется на официальном бланке юридического лица)

Заявление
на добавление туннелируемого IP-адреса (координатора или иного устройства) в файл информации межсетевого экспорта защищенной сети передачи данных № (указать номер ЗСПД)

(наименование юридического лица (органа, организации) с указанием организационно-правовой формы)

в лице

(должность, фамилия, имя, отчество, последнее – при наличии, руководителя юридического лица (органа, организации)

действующего на основании

просит организовать защищенный канал связи в соответствии со следующей информацией:

№ п/п	Наименование сведений	Предоставляемые сведения
1.	Полное наименование юридического лица	
2.	Сокращенное наименование юридического лица	
3.	ОГРН	
4.	ИНН	
5.	Юридический адрес	
6.	Фактический адрес	
7.	Наименование координатора (иного устройства), IP-адрес которого туннелируется	
8.	Туннелируемый IP-адрес	
9.	Фамилия, имя, отчество (последнее – при наличии) администратора ЗСПД	

10.	Контактная информация (последнее – при наличии) администратора ЗСПД	
11.	Номер ЗСПД	
12.	Наименование информационных (автоматизированных) систем, доступ к которым необходим на законном основании	(заполняется в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных)
13.	Обоснование необходимости предоставления доступа (установления связи с туннелируемыми IP-адресами)	(заполняется в случае подключения к защищенной сети передачи данных с предоставлением доступа к информационной системе персональных данных)

_____	_____	_____
должность руководителя	подпись	расшифровка подписи

Приложение № 5 к Соглашению об установлении межсетевого взаимодействия

Форма

Гриф секретности
или ограничительная пометка
Экз. №

РЕЕСТР

абонентских пунктов (сетевых узлов) защищенных сетей передачи данных сторон и связей между ними (матрица связей)

ЗСПД № / ЗСПД №	ViPNet Administrator	ViPNet Coordinator	Абонентский пункт (сетевой узел № 1)	Абонентский пункт (сетевой узел № 2)
ViPNet Administrator	+	+	+	+
ViPNet Coordinator	+	+	+	+
Абонентский пункт (сетевой узел № 1)	+	+	+	
Абонентский пункт (сетевой узел № 2)	+	+		+

Подписи сторон

Администратор защищенной сети передачи данных № (указать номер ЗСПД)	Администратор защищенной сети передачи данных № (указать номер ЗСПД)
_____ (подпись)	_____ (подпись)
"___"_____20____г.	"___"_____20____г.