МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ЧЕЛЯБИНСКИЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ»

ул. Комсомольская, 20-а, г. Челябинск, 454111, тел.: 8 (351) 217-30-89

e-mail: info@rcokio.ru, www.rcokio.ru

ПРИКАЗ

24.03.2023 № 220-ОД

Об утверждении регламента
функционирования защищенной сети
Министерства образования и науки
Челябинской области

С целью выполнения приказов Министерства образования и науки Челябинской области от 31.12.2019 №03/4829 «Об утверждении Положения о защищенной сети Министерства образования и науки Челябинской области» и от 30.12.2022 №01/3059 «Об утверждении показателей объема (содержания) и качества работ в рамках государственного задания государственного бюджетного учреждения дополнительного профессионального образования «Челябинский институт развития образования» в 2023 году»

ПРИКАЗЫВАЮ:

1. Утвердить регламент функционирования защищенной сети Министерства образования и науки Челябинской области (приложение 1 к настоящему приказу).

2. Начальнику отдела обеспечения информационной безопасности Гнедкову А.В.:

2.1. Заменить регламент функционирования защищенной сети Министерства образования и науки Челябинской области на официальном сайте в сети «Интернет» ГБУ ДПО «ЧИРО».

2.2. Провести семинар для всех пользователей защищенной сети Министерства образования и науки Челябинской области 20.04.2023, на котором

ознакомить таких пользователей с положениями регламента функционирования защищенной сети Министерства образования и науки Челябинской области.

2.3. Обеспечить функционирование защищенной сети Министерства образования и науки Челябинской области в соответствии с приложением 1 к настоящему документу.

3. Считать недействительным приказ ГБУ ДПО «Региональный центр оценки качества и информатизации образования» от 29.06.2020 №396-ОД.

4. Контроль за выполнением настоящего приказа возложить на начальника управления информационного обеспечения системы образования Томина Б.П.

Ректор

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 30190eaa43a77be593085357a115137d
Владелец **Барабас Андрей Александрович**
Действителен с 12.12.2022 по 06.03.2024

А.А. Барабас

Гнедков Андрей Владимирович
Худорожков Иван Владимирович
8 (351) 217-30-94
Рассылка: дело, ООИБ, Томину Б.П.

Приложение 1
к приказу ГБУ ДПО «ЧИРО»
от 24.03.2023 № 220-ОД

Регламент функционирования защищенной сети Министерства образования и науки Челябинской области

Челябинск
2023 г.

Оглавление

1. Общие сведения.

1.1. Регламент функционирования защищенной сети Министерства образования и науки Челябинской области (далее – Регламент) определяет:

1.1.1. Пользователей защищенной сети Министерства образования и науки Челябинской области.

1.1.2. Цели и задачи защищенной сети Министерства образования и науки Челябинской области (далее – Защищенная сеть).

1.1.3. Права, обязанности и ответственность пользователей Защищенной сети.

1.1.4. Порядок обновления мастер ключей.

1.1.5. Порядок обновления дистрибутивов ключей.

1.1.6. Порядок подключения к Защищенной сети.

1.1.7. Техническая поддержка и консультация пользователей Защищенной сети.

1.1.8. Порядок межсетевого взаимодействия с Защищенной сетью.

1.1.9. Порядок отключения от Защищенной сети.

1.1.10. Порядок действий при компрометации дистрибутивов ключей.

1.2. В настоящем документе используются термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области персональных данных, защиты информации и обеспечения информационной безопасности.

1.3. Обработка персональных данных оператором Защищенной сети осуществляется в соответствии с действующим законодательством Российской Федерации в области персональных данных и политикой оператора в отношении обработки персональных данных, опубликованной на официальном сайте оператора Защищенной сети.

1.4. Исполнение обязанностей настоящего Регламента со стороны ГБУ ДПО «ЧИРО» реализуются отделом обеспечения информационной безопасности ГБУ ДПО «ЧИРО».

1.5. Все изменения в Регламент вносятся приказом ГБУ ДПО «ЧИРО», который публикуется на официальном сайте оператора Защищенной сети в информационно-телекоммуникационной сети «Интернет»

(https://rcokio.ru/normativnye-dokumenty-1/) без дополнительного уведомления пользователей Защищенной сети.

1.5.1. Регламент вступает в силу через 7 календарных дней с момента его опубликования.

1.6. Порядок разрешения вопросов, не урегулированных настоящим регламентом, определяется законодательством Российской Федерации.

1.7. Настоящий Регламент разработан во исполнение приказов Министерства образования и науки Челябинской области:

1.7.1. От 30.12.2022 № 01/3059 «Об утверждении показателей объема (содержания) и качества работ в рамках государственного задания государственного бюджетного учреждения дополнительного профессионального образования «Челябинский институт развития образования».

1.7.2. От 31.12.2019 № 03/4829 «Об утверждении Положения о Защищенной сети Министерства образования и науки Челябинской области» (Далее – положение о Защищенной сети).

2. Пользователи Защищенной сети.

2.1. Владелец Защищенной сети – Министерство образования и науки Челябинской области.

2.2. Оператор Защищенной сети - Государственное бюджетное учреждение дополнительного профессионального образования «Челябинский институт развития образования».

2.2.1. Информация об операторе Защищенной сети:

2.2.1.1. Место нахождения: Российская Федерация, Челябинская область, город Челябинск, Комсомольская улица, дом 20а.

2.2.1.2. Номер телефона: +7 (351) 217-30-94.

2.2.1.3. Адрес электронной почты для получения консультаций в рамках Защищенной сети: support@rcokio.ru.

2.2.1.4. Официальный сайт: https://rcokio.ru.

2.2.1.5. График работы: с понедельника по четверг с 08:30 до 17:15, пятница с 08:30 до 16:00, обеденный перерыв с 12:00 до 12:30.

2.3. Абоненты Защищенной сети – организации системы образования Челябинской области, использующие функции Защищенной сети для осуществления уставной деятельности (в том числе органы исполнительной власти Челябинской области и подведомственные им организации, иные организации, осуществляющие образовательную деятельность, организации, осуществляющие обучение).

3. Цель и задачи Защищенной сети.

3.1. Защищенная сеть построена при использовании продуктов компании акционерного общества «Информационные технологии и коммуникационные системы» и имеет номер 3660.

3.2. Защищенная сеть создана с целью защиты информации пользователей Защищенной сети.

3.3. Задачи функционирования Защищенной сети.

3.3.1. Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи пользователей Защищенной сети.

3.3.2. Реализация защищенного удаленного доступа субъектов доступа (пользователей Защищенной сети) к объектам доступа через внешние информационно-телекоммуникационные сети.

4. Права, обязанности и ответственность пользователей Защищенной сети.

4.1. Права Абонента и Оператора Защищенной сети определены положением о Защищенной сети.

4.2. Обязанности Абонента Защищенной сети.

4.2.1. Выполнять обязанности, определенные положением о Защищенной сети.

4.2.2. Выполнять обязанности, предусмотренные главой 4 Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 №152-ФЗ (далее – Закон «О персональных данных»).

4.2.3. Предоставить Оператору Защищенной сети в соответствии с настоящим регламентом и с использованием автоматизированной информационной системы «Мониторинг узлов Защищенной сети» (далее – АИС МУЗС; 192.168.74.9) актуальные и действующие документы, подтверждающие принятие и выполнение Абонентом Защищенной сети следующих мер и требований (далее – Документы) в отношении информационных систем, в состав которых входят объекты информатизации, имеющие подключение к Защищенной сети, предусмотренных:

4.2.3.1. Пунктом 4 части 2 статьи 19 Закона «О персональных данных».

4.2.3.2. Пунктом 6 состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.2.3.3. Пунктом 17 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.2.4. В случае не предоставления оператору Защищенной сети в соответствии с настоящим регламентом и с использованием АИС МУЗС актуальных и действующих Документов, подтверждающих принятие и выполнение в отношении информационных систем в состав которых входят объекты информатизации, имеющие подключение к Защищенной сети, мер и требований предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, оператор Защищенной сети такие сетевые узлы блокирует без права работы с информационными системами, функционирующими с использованием Защищенной сети.

4.2.4.1. Для разблокировки подключения пользователь Защищенной сети проводит работы, предусмотренные пунктами 4.2.3.1 – 4.2.3.3 настоящего документа, после чего пишет обращение на почту support@rcokio.ru, в теме письма указывает «Разблокировка доступа», в тексте письма указывает наименование сетевых узлов ViPNet Client, которые необходимо разблокировать и прикладывает документы, предусмотренные пунктом 4.2.3 настоящего документа.

4.2.5. Рекомендуется проведение работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, в форме аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну в соответствии с порядком, утверждённым приказом ФСТЭК России от 29.04.2021 №77 «Об утверждении организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

4.2.6. Работы, предусмотренные пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, организуются и проводятся Абонентом Защищенной сети самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации (далее – ТЗКИ).

4.2.6.1. При проведении работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, привлекаемые на договорной основе

юридические лица и индивидуальные предприниматели должны иметь лицензию по ТЗКИ на проведение работ и оказание услуг, предусмотренных подпунктом «б» пункта 4 положения о лицензировании деятельности по ТЗКИ, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации» (далее – Положение ТЗКИ).

4.2.6.1.1. Если работы, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, проводятся в форме, определенной пунктом 4.2.5 настоящего Регламента, то привлекаемые на договорной основе юридические лица и индивидуальные предприниматели должны иметь лицензию по ТЗКИ на проведение работ и оказание услуг, предусмотренных подпунктами «б» и «г».

4.2.6.1.2. Если в процессе работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, проводимых в форме, определенной пунктом 4.2.5 настоящего Регламента, запланирована установка и настройка средств защиты информации, то привлекаемые на договорной основе юридические лица и индивидуальные предприниматели должны иметь лицензию по ТЗКИ на проведение работ и оказание услуг, предусмотренных подпунктами «б», «г» и «е».

4.2.6.1.3. Если в процессе работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, запланирована установка, настройка и передача средств криптографической защиты информации, то привлекаемые на договорной основе юридические лица и индивидуальные предприниматели должны иметь лицензию ФСБ России на выполнение работ и оказание услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, предусмотренных пунктами 12, 20, 21 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств», утвержденного Постановлением 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)».

4.2.6.2. При самостоятельном проведении работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 настоящего Регламента, Абонент Защищенной сети обязан учитывать следующее:

4.2.6.2.1. Работы должны проводиться специалистами по защите информации, обладающими знаниями, умениями и навыками, необходимыми для организации и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.6.2.2. Работы должны проводиться специалистами по защите информации, которые периодически проходят повышение квалификации. Повышение квалификации осуществляется в соответствии с постановлением Правительства Российской Федерации от 06.05.2016 №399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса». Подобное повышение квалификации специалисты могут в том числе пройти через программу повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных», которая реализуется ГБУ ДПО «ЧИРО» и согласована с ФСТЭК России.

4.2.7. Как минимум один раз в первую неделю каждого месяца запускать ViPNet Client.

4.3. Обязанности Оператора Защищенной сети.

4.3.1. Выполнять обязанности, определенные положением о Защищенной сети.

4.3.2. В случае невыполнения абонентами Защищенной сети требований законодательства Российской Федерации в области персональных данных, информации и информационной безопасности, требований положения и регламента функционирования Защищенной сети ограничить их доступ к Защищенной сети.

4.4. Ответственность пользователей Защищенной сети.

4.4.1. В случае нарушения требований законодательства Российской Федерации в области персональных данных, в области информации и информационной безопасности, требований положения и регламента функционирования Защищенной сети, а также в случае выполнения действий, послуживших причинами сбоя функционирования Защищенной сети и (или) создания условий (предпосылок), направленных на получение лицами неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, нарушения конфиденциальности информации ограниченного доступа и неправомерного ограничения доступа к информации, пользователи Защищенной сети несут персональную ответственность в пределах, определенных действующим законодательством Российской Федерации.

5. Порядок обновления мастер ключей.

5.1. Оператором Защищенной сети в сроки, определенные эксплуатационной документацией к ПО ViPNet Administrator, проводится обновление мастер ключей. Перед началом обновления мастер ключей оператор Защищенной сети направляет информационное письмо (далее - Письмо) всем пользователям Защищенной сети с использованием электронной почты и (или) ViPNet Деловая почта.

5.2. Пользователи Защищенной сети при получении Письма, указанного в пункте 5.1 настоящего документа, обязаны не позднее 3 рабочих дней с момента получения такого Письма запустить ViPNet Client и проверить корректность функционирования Защищенной сети в соответствии с инструкцией проверки функционирования Защищенной сети (Приложение № 2).

5.2.1. Если ViPNet Client функционирует корректно, то пользователям необходимо поддерживать непрерывную рабочую сессию ViPNet Client в сроки, указанные в Письме.

5.2.2. Если ViPNet Client функционирует некорректно, то пользователям Защищенной сети необходимо обратиться в техническую поддержку (п. 8 настоящего Регламента).

5.3. По возникшим вопросам централизованного обновления мастер ключей, необходимо обращаться в отдел обеспечения информационной безопасности ГБУ ДПО «ЧИРО» по электронной почте «support@rcokio.ru», указав в теме письма «Централизованное обновление мастер ключей».

6. Порядок обновления дистрибутивов ключей.

6.1. Дистрибутив ключей обновляется в следующих случаях:

6.1.1. Некорректное функционирование ViPNet Client и его компонентов.

6.1.2. В случае несвоевременного централизованного обновления мастер ключей.

6.1.3. По рекомендациям работников отдела обеспечения информационной безопасности ГБУ ДПО «ЧИРО».

6.1.4. В иных случаях, установленных эксплуатационной и технической документацией к ViPNet Client.

6.2. Обновление дистрибутивов ключей производится путем их генерации и выдачи пользователю Защищенной сети.

6.3. Обновление дистрибутивов ключей производится по одной из двух схем на выбор пользователя Защищенной сети.

6.4. Схема обновления дистрибутивов ключей № 1.

6.4.1. Дистрибутив ключей формируется и выдается в течении 5 (пяти) рабочих дней после получения следующего комплекта документов:

6.4.1.1. Оригинал заявления на генерацию дистрибутива ключей (Приложение № 3).

6.4.1.2. Оригинал заявления на добавление связей (Приложение № 3.1).

6.4.1.3. Заверенная копия приказа об утверждении списка пользователей средств криптографической защиты информации (далее – СКЗИ) (Приложение № 5).

6.4.1.3.1. Если требуется предоставить заверенную копию документа, то необходимо выполнить следующие правила заверения копий документов: проставляется надпись «Копия верна», должность лица, заверившего копию, подпись и расшифровка подписи лица, заверившего копию, дата заверения, печать организации. В многостраничном документе вышеуказанное заверение проставляется на каждой странице или весь документ сшивается, и отметка о заверении проставляются на 1 странице.

6.4.1.4. Оригинал согласия на обработку персональных данных. Согласие на обработку персональных данных предоставляется:

6.4.1.4.1. Лицом, чьи персональные данные указываются в заявлении на генерацию дистрибутива ключей (Приложение № 6).

6.4.1.4.2. Лицом, на которое оформлена доверенность на получение дистрибутива ключей (Приложение № 6.1).

6.4.1.5. Доверенность (Приложение № 7) предоставляется в случае, если получать дистрибутив ключей будет доверенное лицо.

6.4.1.6. Заверенная копия лицензии на право пользования ПК ViPNet Client (далее - Лицензия). Лицензия предоставляется на каждый сетевой узел. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

6.4.1.7. Заверенные копии документов, подтверждающих проведение работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 регламента функционирования Защищенной сети. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

6.4.1.7.1. В случае невозможности проведения работ, предусмотренных пунктами 4.2.3.1 – 4.2.3.3 регламента функционирования Защищенной сети, из-за отсутствия дистрибутива ключей, предоставляются документы, подтверждающие выполнение таких работ в ближайшее время, но не более 30 календарных дней с момента получения дистрибутива ключей (гарантийные письма, договоры на оказание услуг и прочее).

6.4.1.8. Заверенная копия заключения об уровне специальной подготовки пользователя СКЗИ ПК ViPNet Client (далее - Заключение). Заключение пользователи СКЗИ получают после прохождения соответствующего обучения и сдачи зачёта по программе обучения, которое проводится лицензиатом ФСБ России. Заключение пользователи СКЗИ могут получить в том числе в ГБУ ДПО «ЧИРО» после прохождения соответствующего обучения. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

6.4.1.9. Заверенная копия сертификата активации сервиса совместной технической поддержки продуктов ViPNet. Приобретается пользователями Защищенной сети самостоятельно и на каждый сетевой узел, подключенный к Защищенной сети Министерства образования и науки Челябинской области. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

6.4.2. Комплект документов, указанный в пункте 6.4. настоящего Регламента предоставляется очно оператору Защищенной сети. При себе необходимо иметь документ, удостоверяющий личность.

6.4.3. Если комплект документов, указанный в пункте 6.4. настоящего Регламента неполный или неточный, то оператор даёт мотивированный отказ в обновлении дистрибутивов ключей в течении 3 рабочих дней.

6.5. Схема обновления дистрибутивов ключей №2.

6.5.1. Необходимо подготовить комплект документов, указанный в пункте 6.4 настоящего Регламента, и подписать его усиленной квалифицированной электронной подписью (далее – УКЭП) руководителя организации или иного уполномоченного лица в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ. Подписанный УКЭП комплект документов загружается в специально организованную систему с децентрализованным снабжением криптоключами – АИС МУЗС, используя раздел «ЗАПРОС DST». Дополнительно пользователь АИС МУЗС предоставляет квалифицированный сертификат ключа проверки электронной подписи, выданный на уполномоченное лицо или пользователя СКЗИ.

6.5.1.1. В случае принятия решения об отказе в генерации дистрибутива ключей оператор Защищенной сети направляет, пользователю АИС МУЗС мотивированный отказ.

6.5.1.2. В случае принятия положительного решения в выдаче дистрибутива ключей оператор Защищенной сети генерирует его и направляет пользователю Защищенной сети в зашифрованном на предоставленном квалифицированном сертификате ключа проверки электронной подписи, используя АИС МУЗС.

6.5.2. Направленный дистрибутив ключей доступен для скачивания в АИС МУЗС в течении 5 рабочих дней, по истечении указанного срока скачать его будет невозможно.

6.5.3. После успешного получения дистрибутивов ключей с использованием АИС МУЗС они удаляются с АИС МУЗС автоматически через 24 часа.

6.5.3.1. Пользователь СКЗИ обязан в срок, не превышающий 1 календарного дня, уведомить оператора Защищенной сети о получении дистрибутива ключей с использованием АИС МУЗС путем отправки электронного сообщения на почту support@rcokio.ru с указанием в теме письма «Дистрибутив ключей», а в тексте наименование и ИНН организации, и информацию о получении дистрибутива ключей.

6.5.3.1.1. В случае не предоставления информации, указанной в пункте 6.5.3.1 настоящего Регламента, оператор Защищенной сети оставляет за собой право такие учреждения отключать от Защищенной сети.

7. Порядок подключения к Защищенной сети.

7.1. Подключение к Защищенной сети производится только после ознакомления и принятия соответствующего Договора оферты присоединения. (Приложение № 1).

7.2. Подключение к Защищенной сети проводится путем генерации и выдачи пользователю дистрибутива ключей.

7.3. Дистрибутив ключей генерируется оператором Защищенной сети после получения и проверки следующего комплекта документов:

7.3.1. Оригинал заявления на генерацию дистрибутива ключей (Приложение № 3).

7.3.2. Оригинал заявления на добавление связей (Приложение № 3.1).

7.3.3. Оригинал заявления на подключение к Защищенной сети (Приложение № 4).

7.3.4. Заверенная копия документа подтверждающего полномочия руководителя организации или иного уполномоченного лица. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.3.5. Заверенная копия приказа об утверждении списка пользователей СКЗИ (Приложение № 5). Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.3.6. Оригинал согласия на обработку персональных данных. Согласие на обработку персональных данных предоставляется:

7.3.6.1. Лицом, чьи персональные данные указываются в заявлении на генерацию дистрибутива ключей (Приложение № 6).

7.3.6.2. Лицом, на которое оформлена доверенность на получение дистрибутива ключей (Приложение № 6.1).

7.3.7. Доверенность (Приложение № 7) предоставляется, если дистрибутив ключей будет получать доверенное лицо.

7.3.8. Заверенная копия Лицензии на ПК ViPNet Client. Лицензия предоставляется на каждый сетевой узел. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.3.9. Заверенные копии документов, подтверждающих проведение работ, предусмотренных пунктами 4.2.3.1-4.2.3.3 Регламента функционирования

Защищенной сети. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.3.9.1. В случае невозможности проведения работ, предусмотренных пунктами 4.2.3.1-4.2.3.3 регламента функционирования Защищенной сети, из-за отсутствия дистрибутива ключей, предоставляются документы, подтверждающие выполнение таких работ в ближайшее время, но не более 30 календарных дней с момента получения дистрибутива ключей (гарантийные письма, договоры на оказание услуг и прочее).

7.3.10. Заверенная копия заключения об уровне специальной подготовки пользователя СКЗИ. Данный документ получают после прохождения соответствующего обучения и сдачи зачёта по программе обучения, которое проводится лицензиатом ФСБ России. Заключение пользователи СКЗИ могут получить в том числе в ГБУ ДПО «ЧИРО» после прохождения соответствующего обучения. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.3.11. Заверенная копия сертификата активации сервиса совместной технической поддержки продуктов ViPNet. Приобретается пользователями Защищенной сети самостоятельно и на каждый сетевой узел, подключенный к Защищенной сети Министерства образования и науки Челябинской области. Документы заверяются согласно пункту 6.4.1.3.1 настоящего Регламента.

7.4. Комплект документов, указанный в п. 7 настоящего Регламента, предоставляется очно оператору Защищенной сети. При себе необходимо иметь документ, удостоверяющий личность.

7.5. После рассмотрения предоставленного комплекта документов Оператор Защищенной сети принимает решение о подключении к Защищенной сети и выдаче дистрибутива ключей или об отказе о подключении к Защищенной сети и выдачи дистрибутива ключей. В случае отказа в выдаче дистрибутива ключей оператор Защищенной сети в устной или письменной форме с использованием электронной почты разъясняет причину отказа.

7.6. В случае принятия решения о подключении к Защищенной сети и выдаче дистрибутива ключей, оператор Защищенной сети в течении 5 (пяти) рабочих дней через электронную почту, указанную в заявлении на генерацию

дистрибутива ключей, информирует о принятии такого решения Пользователя СКЗИ и назначает возможную дату выдачи дистрибутива ключей.

7.7. Руководитель организации, пользователь СКЗИ или доверенное лицо после получения информации о выдачи дистрибутива ключей обязан(о) получить его в назначенное оператором Защищенной сети время.

7.8. После установки дистрибутива ключей пользователь СКЗИ обязан в течении 5 рабочих дней:

7.8.1. Выполнить действия, предусмотренные пунктом 4.2.3 настоящего документа.

7.8.2. Сообщить о выполнении пункта 4.2.3 на почту support@rcokio.ru, в теме письма необходимо указать «Разблокировка сетевого узла (указать имя сетевого узла)».

7.8.3. В случае невыполнения пользователем СКЗИ требований, предусмотренных пунктами 7.8.1 - 7.8.2 настоящего документа, оператор Защищенной сети оставляет за собой право такое подключение заблокировать.

7.8.3.1. Для разблокировки подключения пользователь Защищенной сети проводит работы, предусмотренные пунктами 4.2.3.1 – 4.2.3.3 настоящего документа, после чего пишет обращение на почту support@rcokio.ru, в теме письма указывает «Разблокировка доступа», в тексте письма наименование сетевых узлов ViPNet Client, которые необходимо разблокировать и прикладывает документы, предусмотренные пунктом 4.2.3 настоящего документа.

7.9. В случае возникновения вопросов по подключению к Защищенной сети, необходимо писать на почту support@rcokio.ru с указанием темы письма «Вопросы по подключению к Защищенной сети».

8. Техническая поддержка и консультация пользователей Защищенной сети.

8.1. Техническая поддержка пользователей Защищенной сети оказывается организацией, у которой пользователи Защищенной сети приобрели сертификат активации сервиса совместной технической поддержки продуктов ViPNet.

8.2. Получить консультацию по работе с Защищенной сетью её пользователи могут по адресу электронной почты support@rcokio.ru или по номеру телефона +7 (351) 217-30-94.

9. Межсетевое взаимодействие.

9.1. Если требуется организовать канал для защищенного обмена информацией между Защищённой сетью и иными сетями, построенными с использованием продуктов компании АО «ИНФОТЕКС» (далее – Доверенная сеть), то такой канал организуется путём установки межсетевого взаимодействия между такими сетями. Для организации межсетевого взаимодействия необходимо:

9.1.1. Если инициатором межсетевого взаимодействия является владелец или оператор Защищенной сети, то владелец или оператор Защищенной сети направляет официальное письмо в адрес руководителя администратора Доверенной сети или иных уполномоченных лиц, ответственных за функционирование Доверенной сети, с просьбой рассмотреть возможность организации такого межсетевого взаимодействия.

9.1.2. Если инициатором является администратор Доверенной сети или иные уполномоченные лица, ответственные за функционирование Доверенной сети, то такие лица направляют официальное письмо в адрес руководителя Министерства образования и науки Челябинской области с просьбой рассмотреть возможность организации такого межсетевого взаимодействия.

9.1.3. В случае положительного ответа на письма, указанные в пунктах 9.1.1 или 9.1.2, администраторы Защищенной сети и Доверенной сети последовательно выполняют следующие действия:

9.1.3.1. Разрабатывают регламент межсетевого взаимодействия между Защищенной сетью и Доверенной сетью, в котором указывается следующая информация:

9.1.3.1.1. Полное наименование организаций администратора Защищенной сети и администратора Доверенной сети, а также наименования Защищенной сети и Доверенной сети.

9.1.3.1.2. Номер Защищенной сети и Доверенной сети.

9.1.3.1.3. Фамилия, имя, отчество, должность, адрес электронной почты и контактные номера телефонов администратора Защищенной сети и Доверенной сети.

9.1.3.1.4. Наименование сетевых узлов шлюзовых координаторов Защищенной сети и Доверенной сети, версия используемого программного обеспечения шлюзовых координаторов и ПО ViPNet Administrator.

9.1.3.1.5. Цель установки межсетевого взаимодействия.

9.1.3.1.6. Реквизиты документов, подтверждающих проведение аттестации на соответствие требованиям по защите информации объектов информатизации администраторов Защищенной сети и Доверенной сети, в состав которых входят все компоненты ViPNet Administrator.

9.1.3.1.7. Перечень (наименование) сетевых узлов, участвующих в защищенном соединении между Защищенной сетью и Доверенной сетью с указанием наименования и адреса информационных систем, с которыми планируют работать такие сетевые узлы.

9.1.3.1.7.1. Порядок изменения, добавления и (или) удаления сетевых узлов, участвующих в защищенном соединении между Защищенной сетью и Доверенной сетью, а также перечня информационных систем, с которыми необходимо работать таким сетевым узлам.

9.1.3.1.7.2. Перечень нормативных правовых актов, требования которых обязаны выполнить сетевые узлы, участвующие в защищенном соединении между Защищенной сетью и Доверенной сетью, и порядок предоставления подтверждающих документов.

9.1.3.2. После разработки регламента межсетевого взаимодействия между Защищенной сетью и Доверенной сетью, такой регламент печатается для каждой из сторон межсетевого взаимодействия и подписывается руководителем или иным уполномоченным лицом. Регламент межсетевого взаимодействия между Защищенной сетью и Доверенной сетью может быть утвержден в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

9.1.3.3. После подписания и обмена экземплярами регламента межсетевого взаимодействия между Защищенной сетью и Доверенной сетью, администраторы Защищенной сети и Доверенной сети проводят работы по организации межсетевого взаимодействия между такими сетями,

руководствуясь эксплуатационной документацией и формулярами на ПО ViPNet Administrator.

10. Порядок отключения от защищённой сети.

10.1. В случае принятия решения об отключении от Защищенной сети, пользователь Защищенной сети обязан уничтожить дистрибутивы ключей и предоставить оператору Защищенной сети:

10.1.1. Заявление о прекращении использования Защищенной сети (Приложение № 8).

10.1.2. Доверенность (Приложение № 7) предоставляется в случае, если Заявление о прекращении использования Защищенной сети предоставляет доверенное лицо пользователя СКЗИ.

10.1.3. Если пользователем СКЗИ принято решение о передачи документов на отключение от Защищенной сети доверенным лицом, то предоставляется согласие на обработку персональных данных доверенного лица (Приложение № 10).

10.2. Дистрибутивы ключей уничтожаются путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования) в соответствии с Приказом ФАПСИ от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

10.3. Комплект документов, указанный в пункте 10.1 настоящего Регламента по отключению от Защищенной сети, предоставляется в отдел обеспечения информационной безопасности ГБУ ДПО «ЧИРО» одним из следующих способов:

10.3.1. Очно по адресу: 454111, Челябинская область, г. Челябинск, ул. Комсомольская, д. 20а, кабинет № 311.

10.3.2. На электронную почту support@rcokio.ru. В данном случае комплект документов необходимо подписать усиленной квалифицированной электронной подписью, выданной аккредитованным удостоверяющим центром,

в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

11. Порядок действий при компрометации дистрибутивов ключей.

11.1. В случае возникновения компрометации дистрибутивов ключей, в том числе любого из его компонентов (справочники, ключи, пароль и прочее) пользователь СКЗИ уведомляет об этом оператора Защищенной сети посредством телефонного звонка на номер +7 (351) 217-30-94 и направляет заявление о компрометации дистрибутивов ключей (Приложение № 9) на почту support@rcokio.ru с указанием темы письма «Компрометация дистрибутивов ключей».

11.2. После получения информации о компрометации дистрибутивов ключей оператор Защищенной сети проводит процедуру по декомпрометации дистрибутивов ключей. После завершения процедуры декомпрометации дистрибутивов ключей Пользователь Защищенной сети (о завершении декомпрометации пользователь Защищенной сети узнает от оператора Защищенной сети) обязан провести расследование и устранить причины компрометации дистрибутивов ключей и их предпосылки. Результаты расследования высылаются на почту support@rcokio.ru с указанием темы письма «Результаты расследования причин компрометации ключевой информации». В случае невозможности устранения причин и предпосылок компрометации дистрибутивов ключей пользователь Защищенной сети обращается за консультацией в отдел обеспечения информационной безопасности ГБУ ДПО «ЧИРО», направив на почту support@rcokio.ru.

11.3. После устранения причины компрометации дистрибутивов ключей для возобновления работы с Защищенной сетью пользователь Защищенной сети выполняет процедуру обновления дистрибутивов ключей в соответствии с пунктом 6 настоящего Регламента.

Приложение № 1 к Регламенту

Договор оферты присоединения
к Регламенту функционирования Защищенной сети Министерства образования и науки Челябинской области

_____ _____
(населенный пункт) (дата составления договора)

Государственное бюджетное учреждение дополнительного профессионального образования «Челябинский институт развития образования», именуемое в дальнейшем «Администратор сети», в лице ректора Барабаса Андрея Александровича, действующего на основании Устава, с одной стороны и организация, именуемая в дальнейшем «Пользователь сети», в лице его руководителя с другой стороны, совместно именуемые «Стороны» и каждый в отдельности также «Сторона» заключили настоящий договор присоединения к Регламенту функционирования Защищенной сети образовательных организаций (далее по тексту – «Договор») о нижеследующем.

1. Предмет договора

1.1. Настоящий договор оферты является публичным предложением ГБУ ДПО «ЧИРО» присоединиться Пользователям сети к Регламенту функционирования Защищенной сети Министерства образования и науки Челябинской области (далее – Регламент) в порядке, предусмотренном ст. 428, ст. 432, ст. 435, ст. 438 Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ.

2. Условия договора

2.1. Договор считается заключенным, если между сторонами достигнуто соглашение по всем существенным условиям договора.

2.2. Существенными являются условия о предмете договора, условия, которые названы в законе или иных правовых актах как существенные, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение.

2.3. Договор заключается посредством направления оферты (предложения заключить договор) одной из сторон и ее акцепта (принятия предложения) другой стороной.

2.4. Направлением оферты считается размещение данного договора на официальном сайте ГБУ ДПО «ЧИРО».

2.5. Акцепт оферты считается осуществленным, а Договор считается заключенным, если Пользователь сети направил Администратору сети заявления на подключение к Защищенной сети и заявления на генерацию дистрибутива ключей.

3. Права, обязанности и ответственность Сторон

3.1. Права, обязанности и ответственность Сторон определяются регламентом и положением о Защищенной сети Министерства образования и науки Челябинской области, и настоящим договором.

3.2. Обязанности Пользователя сети:

3.2.1. Своевременно (не позднее одного рабочего дня с момента принятия решения о внесении изменений) информировать Администратора сети об изменении реквизитов Пользователя сети, пользователей средств криптографической защиты информации (в том числе о расторжении трудовых договоров с пользователями средств криптографической защиты информации);

3.2.2. Принимать все вносимые в Регламент изменения с момента их вступления в силу.

3.2.3. В случае, если пользователь сети не согласен с изменениями Регламента, то он обязан отключиться от Защищенной сети в соответствии с пунктом 10 Регламента.

3.2.4. С момента принятия оферты выполнять условия настоящей оферты.

3.2.5. С момента принятия оферты выполнять требования регламента Защищенной сети Министерства образования и науки Челябинской области.

3.3. Права Администратора сети:

3.3.1. Приостанавливать исполнение настоящего договора и Регламента в случае выявления нарушений со стороны Пользователя сети до момента устранения таких нарушений;

3.3.2. Вносить изменения в Регламент без дополнительного уведомления Пользователя сети.

4. Порядок разрешения споров

4.1. Разногласия, возникающие между Сторонами при заключении, изменении и расторжении настоящего договора, рассматриваются в установленном действующим Законодательством порядке.

4.2. Все споры между Сторонами, по которым не было достигнуто соглашение, разрешаются в соответствии с законодательством Российской Федерации.

5. Дополнительные условия

5.1. Настоящий договор вступает в силу и становится обязательным для сторон с момента его заключения.

5.2. Отношения Сторон, не урегулированные настоящим договором, регулируются действующим Законодательством.

5.3. Условия настоящего договора могут быть изменены по взаимному согласию Сторон с обязательным составлением письменного документа, являющегося неотъемлемой частью настоящего договора.

6. Реквизиты Администратора сети

Государственное бюджетное учреждение дополнительного профессионального образования «Челябинский институт развития образования»

ИНН	-	7447080584
ОГРН	-	1057421508430
КПП	-	745101001
ОКПО	-	75423310
ОКТМО	-	75701000
Юридический (почтовый) адрес	-	454111, Челябинская область, г. Челябинск, ул. Комсомольская, д. 20а
Адрес электронной почты	-	info@rcokio.ru
Контактный номер телефона	-	+7 (351) 217-30-89

Приложение № 2 к Регламенту

Инструкция
проверки функционирования Защищенной сети

Проверка функционирования Защищенной сети осуществляется по следующему алгоритму:

1. Запустить программное обеспечение ViPNet Client.
2. Выбрать пункт «Защищенная сеть» в панели навигации ViPNet Client.
3. Убедиться, что в списках Защищенной сети имеются следующие сетевые узлы:

- Челябинск РЦОКИО Координатор;
- Челябинск РЦОКИО Координатор HW2000.

4. В случае, если «Челябинск РЦОКИО Координатор» или «Челябинск РЦОКИО Координатор HW2000» отсутствуют в списках Защищенной сети, то необходимо выполнить действия по обновлению дистрибутива ключей в соответствии с пунктом 6 Регламента функционирования Защищенной сети.
5. Проверить соединение с сетевыми узлами, указанными в п. 3 настоящей инструкции.
6. Проверка соединения осуществляется путем выделения сетевых узлов, указанных в п. 3 настоящей инструкции и нажатия иконки «Проверить».
7. В случае, если с «Челябинск РЦОКИО Координатор» или «Челябинск РЦОКИО Координатор HW2000» будет отсутствовать соединение (отсутствие соединения определяется статусом «недоступен» в окне проверке соединения), то необходимо обратиться в первую линию технической поддержки в соответствии с пунктом 8 Регламента функционирования Защищенной сети.
8. Если сетевые узлы, указанные в пункте 3 настоящей инструкции, доступны, то это подтверждает корректное функционирование Защищенной сети.

Приложение № 3 к Регламенту

Оформляется на официальном бланке исходящего письма организации, с указанием номера письма и даты!
*пунктирную линию и текст выше неё не печатать!

Ректору ГБУ ДПО «ЧИРО»
А.А. Барабасу

Заявление
на генерацию дистрибутива ключей[1]

С целью обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны нашей организации, в том числе беспроводным каналам связи с использованием защищенной сети Министерства образования и науки Челябинской области «***Наименование организации***» в лице «***Должность и ФИО руководителя организации или иного уполномоченного лица***» просит произвести работы по генерации, записи на носитель (если документы предоставляются очно оператору Защищенной сети) и передачи дистрибутива ключей.

Сведения необходимые для генерации дистрибутива ключей:

Сведения о пользователе СКЗИ	
Фамилия Имя Отчество	*Данное поле обязательно для заполнения*
Должность	*Данное поле обязательно для заполнения*
Контактный номер телефона	*Данное поле обязательно для заполнения*
Адрес электронной почты	*Данное поле обязательно для заполнения*
Сведения об автоматизированном рабочем месте (далее - АРМ)	
Адрес подключения АРМ[2]	*Данное поле обязательно для заполнения.*
Количество АРМ	*Данное поле обязательно для заполнения. Необходимо указать количество обновляемых или новых сетевых узлов.*
Операционная система	*Данное поле обязательно для заполнения. Необходимо указать наименование операционной системы.*
Наименование сетевого узла № 1[3]	*Данное поле обязательно для заполнения.*[4]
Наименование сетевого узла № 2	*Данное поле обязательно для заполнения, только если выбрано 2 или более 2 обновляемых или новых сетевых узлов.*
Сертификат активации сервиса совместной технической поддержки продуктов ViPNet (Сертификат)	*Данное поле обязательно для заполнения. Необходимо указать номер и дату Сертификата.*
	Данное поле обязательно для заполнения Необходимо указать количество лицензий/оборудования.

Подавая настоящее заявление, я подтверждаю, что полученные дистрибутивы ключей будут эксплуатироваться на объектах информатизации, входящих в состав информационной системы нашей организации, для которой выполняются требования, предусмотренные пунктами 4.2.3.1-4.2.3.3 регламента функционирования Защищенной сети и подтверждающие документы загружены в АИС МУЗС.

_____ _____ / _____

(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

[1] Заявление на подключение к защищенной сети при необходимости печатается двусторонней печатью.

[2] Указывается фактический адрес здания организации, в котором установлен ViPNet Client.

[3] В случае, если сетевых узлов более 2-ух (n-кол-во) необходимо добавить n – количество строк с наименованием сетевого узла

[4] Если это новое подключение, то в данном поле указывается прочерк.

Приложение № 3.1 к Регламенту

Оформляется на официальном бланке исходящего письма организации, с указанием номера письма и даты!
*пунктирную линию и текст выше неё не печатать!

Ректору ГБУ ДПО «ЧИРО»
А.А. Барабасу

Заявление[5]
на добавление связей[6]

С целью обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны нашей организации, в том числе беспроводным каналам связи с использованием защищенной сети Министерства образования и науки Челябинской области «***Наименование организации***» в лице «***Должность и ФИО руководителя организации или иного уполномоченного лица***» просит произвести работы по добавлению следующих связей с «***Наименование сетевого узла, с которым нужно установит связь***»:

Со следующими организациями	
Наименование организации	**Цель добавления связи**
…	…
С следующими информационными системами	
Наименование информационной системы	**Цель добавления связи**
…	…

_____ _____ / _____

(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

[5] Заявление на подключение к защищенной сети при необходимости печатается двусторонней печатью.

[6] В данном заявлении указывается наименование организаций или информационных систем, с которыми необходимо установить связь и цель.

Приложение № 4 к Регламенту

Оформляется на официальном бланке исходящего письма организации, с указанием номера письма и даты!
*пунктирную линию и текст выше неё не печатать!

Ректору ГБУ ДПО «ЧИРО»
А.А. Барабасу

Заявление
на подключение к Защищенной сети

С целью защиты информации «***Наименование организации***» в лице «***Должность и ФИО руководителя организации или иного уполномоченного лица***», действующего на основании «***Наименование документа, подтверждающего полномочия руководителя организации или иного уполномоченного лица***» просит произвести подключение нашей организации к Защищенной сети Министерства образования и науки Челябинской области (далее – защищенная сеть).

Сведения о подключаемой к Защищенной сети организации:

Полное наименование организации	*Данное поле обязательно для заполнения*
Сокращенное наименование организации	*Данное поле обязательно для заполнения*
ИНН организации	*Данное поле обязательно для заполнения*
Уровень образования[7]	*Данное поле обязательно для заполнения (указывается в соответствии с лицензией на осуществление образовательной деятельности)*
Юридический адрес организации	*Данное поле обязательно для заполнения*
Номер телефона	*Данное поле обязательно для заполнения*
Адрес электронной почты	*Данное поле обязательно для заполнения*

Подавая настоящее заявление в ГБУ ДПО «ЧИРО», я принимаю условия регламента функционирования Защищенной сети Министерства образования и науки Челябинской области и договора оферты присоединения к Регламенту функционирования Защищенной сети Министерства образования и науки Челябинской области.

Подавая настоящее заявление в ГБУ ДПО «ЧИРО», я подтверждаю присоединение «***Наименование организации***» к Регламенту функционирования Защищенной сети Министерства образования и науки Челябинской области.

_____ _____ / _____

(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

М.П.

[7] Если организация не имеет лицензии на осуществление образовательной деятельности, то данное поле не заполняется.

Приложение № 5 к Регламенту

Оформляется на официальном бланке приказа организации, с указанием номера приказа и даты!
*пунктирную линию и текст выше неё не печатать!

ПРИКАЗ

_____ _____
(населенный пункт) (дата составления приказа)

Об утверждении списка пользователей
средств криптографической защиты
информации

С целью исполнения требований 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, утвержденной приказом ФАПСИ от 13 июня 2001 г. № 152

ПРИКАЗЫВАЮ:

1. Утвердить перечень пользователей средств криптографической защиты информации ***«Наименование организации»***:

№	Должность	Фамилия Имя Отчество
1.		
2.		

2. Контроль за исполнением настоящего приказа оставляю за собой.

_____ _____ / _____
(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

М.П.

Приложение № 6 к Регламенту

Оператор:
ГБУ ДПО «Челябинский институт развития образования»
г. Челябинск, ул. Комсомольская, 20 А
Субъект:_____
_____,
(Фамилия Имя Отчество)
_____

_____,
(адрес)

Паспорт_____,
(номер)
выдан _____
(наименование органа, выдавшего паспорт)
_____

(дата выдачи)

Согласие субъекта персональных данных
на обработку его персональных данных

Я_____,
(Фамилия Имя Отчество)

даю согласие ГБУ ДПО «Челябинский институт развития образования» на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- должность;
- контактный номер телефона;
- адрес электронной почты,

для обработки в целях получения дистрибутивов ключей.

Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных в порядке, предусмотренном законодательством РФ.

Способ обработки персональных данных: смешанный.

Я ознакомлен(а) с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Данное согласие действует до достижения поставленных целей. Согласие может быть отозвано субъектом персональных данных или его уполномоченным представителем в порядке и форме в соответствии с законодательством Российской Федерации в области персональных данных.

_____ _____ _____

фамилия, имя, отчество дата подпись

Приложение № 6.1 к Регламенту

Оператор:
ГБУ ДПО «Челябинский институт развития образования»
г. Челябинск, ул. Комсомольская, 20 А
Субъект:_____
_____,
(Фамилия Имя Отчество)
_____

_____,
(адрес)

Паспорт_____,
(номер)
выдан _____
(наименование органа, выдавшего паспорт)
_____

(дата выдачи)

Согласие субъекта персональных данных
на обработку его персональных данных

Я_____,
(Фамилия Имя Отчество)

даю согласие ГБУ ДПО «Челябинский институт развития образования» на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- должность;
- серия и номер документа, удостоверяющего личность;
- сведения об органе, выдавшем документ, удостоверяющий личность, и дата его выдачи для обработки в целях получения дистрибутива ключей по доверенности.

Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных в порядке, предусмотренном законодательством РФ.

Способ обработки персональных данных: смешанный.

Я ознакомлен(а) с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Данное согласие действует до достижения поставленных целей. Согласие может быть отозвано субъектом персональных данных или его уполномоченным представителем в порядке и форме в соответствии с законодательством Российской Федерации в области персональных данных.

_____ _____ _____

фамилия, имя, отчество дата подпись

Приложение № 7 к Регламенту

ДОВЕРЕННОСТЬ[8]

_____ _____
(населенный пункт) (дата составления доверенности)

Настоящей доверенностью, _____
_____
(полное наименование организации)
в лице _____,
(должность пользователя СКЗИ (доверитель), ФИО)
действующего на основании _____,
(документ, подтверждающий полномочия доверителя)
уполномочивает _____
(должность, ФИО доверенного лица)
Документ, удостоверяющий личность: серия _____№ _____
выдан _____
_____
(кем и когда выдан документ удостоверяющий личность)
обращаться в отдел обеспечения информационной безопасности ГБУ ДПО «Челябинский институт развития образования» с целью совершения следующих действий:

1. Передача комплекта документов в отдел обеспечения информационной безопасности ГБУ ДПО «Челябинский институт развития образования», предусмотренного регламентом функционирования Защищенной сети Министерства образования и науки Челябинской области.

2. Получение от отдела обеспечения информационной безопасности ГБУ ДПО «Челябинский институт развития образования» дистрибутива ключей.

3. Проставление отметки (подписи) о получении дистрибутивов ключей в документах ГБУ ДПО «Челябинский институт развития образования» поэкземплярного учета средств криптографической защиты информации.

Настоящая доверенность выдана сроком до «____»_____20___г.

_____ (должность доверенного лица)	_____ (подпись)	/ _____ (Фамилия Имя Отчество)
_____ (должность доверителя)	_____ (подпись)	/ _____ (Фамилия Имя Отчество)
_____ (должность руководителя или иного уполномоченного лица)	_____ (подпись)	/ _____ (Фамилия Имя Отчество)

М.П.

[8] Оформляется на официальном бланке организации

Приложение № 8 к Регламенту

Оформляется на официальном бланке письма организации, с указанием номера письма и даты!
*пунктирную линию и текст выше неё не печатать!

Ректору ГБУ ДПО «ЧИРО»
А.А. Барабасу

Заявление
о прекращении использования Защищенной сети

В связи с _____ ***«Наименование организации»*** в лице ***«Должность и ФИО руководителя организации или иного уполномоченного лица»*** просит произвести работы по отключению вышеуказанной организации от Защищенной сети.

Сведения об отключаемой организации:

Полное наименование организации	*Данное поле обязательно для заполнения*
Сокращенное наименование организации	*Данное поле обязательно для заполнения*
ИНН организации	*Данное поле обязательно для заполнения*
Уровень образования[9]	*Данное поле обязательно для заполнения (указывается в соответствии с лицензией на образовательную деятельность)*
Юридический адрес организации	*Данное поле обязательно для заполнения*
Номер телефона	*Данное поле обязательно для заполнения*
Адрес электронной почты	*Данное поле обязательно для заполнения*
Наименование сетевого узла № 1	*Данное поле обязательно для заполнения*
Наименование сетевого узла № 2[10]	*Данное поле обязательно для заполнения Только если выбрано 2 или более обновляемых или новых сетевых узлов.*

_____ _____ / _____

(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

М.П.

[9] Если организация не имеет лицензии на осуществление образовательной деятельности, то данное поле не заполняется.

[10] В случае, если сетевых узлов более 2-ух (n-кол-во) необходимо добавить n – количество строк с наименованием сетевого узла.

Приложение № 9 к Регламенту

Оформляется на официальном бланке письма организации, с указанием номера письма и от какой даты!
*пунктирную линию и текст выше неё не печатать!

Ректору ГБУ ДПО «ЧИРО»
А.А. Барабасу

Заявление
О компрометации дистрибутивов ключей

«Наименование организации» в лице ***«должность и ФИО руководителя организации или иного уполномоченного лица»*** информирует вас о том, что ключевая информация для Защищенной сети Министерства образования и науки Челябинской области была скомпрометирована.

Эксплуатация средства криптографической защиты информации приостановлена.

Сведения о скомпрометированном сетевом узле:

Полное наименование организации	*Данное поле обязательно для заполнения*
Сокращенное наименование организации	*Данное поле обязательно для заполнения*
ИНН организации	*Данное поле обязательно для заполнения*
Юридический адрес организации	*Данное поле обязательно для заполнения*
Номер телефона	*Данное поле обязательно для заполнения*
Адрес электронной почты	*Данное поле обязательно для заполнения*
Наименование сетевого узла № 1	*Данное поле обязательно для заполнения*
Наименование сетевого узла № 2[11]	*Данное поле обязательно для заполнения Только если выбрано 2 или более обновляемых или новых сетевых узлов.*

_____ _____ / _____

(должность руководителя организации или иного уполномоченного лица) (подпись) (Фамилия Имя Отчество)

М.П.

[11] В случае, если скомпрометированных сетевых узлов более 2-ух (n-кол-во) необходимо добавить n – количество строк с наименованием сетевых узлов.

Приложение № 10 к Регламенту

Оператор:
ГБУ ДПО «Челябинский институт развития образования»
г. Челябинск, ул. Комсомольская, 20 А
Субъект:_____
_____,
(Фамилия Имя Отчество)
_____

_____,
(адрес)

Паспорт_____,
(номер)
выдан _____
(наименование органа, выдавшего паспорт)
_____

(дата выдачи)

Согласие субъекта персональных данных
на обработку его персональных данных

Я_____,
(Фамилия Имя Отчество)

даю согласие ГБУ ДПО «Челябинский институт развития образования» на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- должность;
- серия и номер документа, удостоверяющего личность;
- сведения об органе, выдавшем документ, удостоверяющий личность, и дата его выдачи для обработки в целях отключения от защищенной сети.

Настоящее согласие дается на осуществление следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных в порядке, предусмотренном законодательством РФ.

Способ обработки персональных данных: смешанный.

Я ознакомлен(а) с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Данное согласие действует до достижения поставленных целей. Согласие может быть отозвано субъектом персональных данных или его уполномоченным представителем в порядке и форме в соответствии с законодательством Российской Федерации в области персональных данных.

_____ _____ _____

фамилия, имя, отчество дата подпись