МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПРИКАЗ

31 ДЕК 2019 № 03/4829

Челябинск

Об утверждении Положения о защищенной сети Министерства образования и науки Челябинской области

В целях обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, во исполнение Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 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»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение о защищенной сети Министерства образования и науки Челябинской области (далее - Положение).

2. Определить:

владельцем Защищенной сети – Министерство образования и науки Челябинской области;

оператором Защищенной сети – Государственное бюджетное учреждение дополнительного профессионального образования «Региональный центр оценки качества и информатизации образования» (далее - ГБУ ДПО РЦОКИО);

абонентами Защищенной сети – организации системы образования Челябинской области, использующие сервисы Защищенной сети для осуществления уставной деятельности, в том числе органы исполнительной власти Челябинской области и подведомственные им организации, органы

местного самоуправления Челябинской области и подведомственные им организации, иные организации осуществляющие образовательную деятельность, организации, осуществляющие обучение.

3. Назначить ответственным за обеспечение функционирования Защищенной сети Министерства образования и науки Челябинской области начальника Управления начального, основного, среднего общего образования Министерства образования и науки Челябинской области Тюрину Е.А.

4. Рекомендовать абонентам Защищенной сети Министерства образования и науки Челябинской области обеспечить выполнение следующих мероприятий:

назначить ответственного пользователя средств криптографической защиты информации, пользователей средств защиты информации;

обеспечить подготовку пользователей средств криптографической защиты информации;

обеспечить соответствие автоматизированного рабочего места (далее – АРМ), предназначенного для использования в качестве абонентского пункта требованиям, предъявляемым программным обеспечением, устанавливаемым для организации абонентского пункта;

обеспечить наличие на АРМ, предназначенном для использования в качестве абонентского пункта, лицензионного программного обеспечения;

обеспечить безопасность помещений, хранилищ, средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Первый заместитель Министра Е.А. Коузова

Есения Анатольевна Кулагина (351) 2638562

Разослать: в дело, ГБУ ДПО РЦОКИО, МОУО, областные государственные образовательные организации.

Приложение к
приказу от 31 ДЕК 2019
№ 03/4829

Положение о защищенной сети Министерства образования и науки Челябинской области

1. Термины и определения

1.1. VPN (Virtual Private Network, виртуальная частная сеть) - виртуальная защищенная сеть - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть), в том числе защищенных, с использованием инфраструктуры информационно-телекоммуникационных сетей общего пользования.

1.2. ViPNet CUSTOM (технология) - технология, предназначенная для построения виртуальных защищённых сетей, путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами.

1.3. ViPNet Administrator - набор программного обеспечения для администрирования защищенной сети ViPNet и управления ею.

1.4. ViPNet Client - программное обеспечение, выполняющее функции VPN-клиента в сети ViPNet, обеспечивающее защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

1.5. ViPNet Coordinator - программное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet. Абонент

1.6. Информационная система - совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

1.7. Владелец информационной системы и компьютерной сети - организация, осуществляющая владение и пользование информационными системами и компьютерными сетями и реализующая полномочия распоряжения в пределах, установленных законодательством.

1.8. Оператор информационной системы и компьютерной сети - организация, которой Владельцем информационной системы и компьютерной сети переданы полномочия по организации функционирования, содержания и обслуживания информационной системы и компьютерной сети.

2. Общие положения

2.1. Защищённая сеть Министерства образования и науки Челябинской области (далее - Защищенная сеть) – территориально распределённая информационно-телекоммуникационная сеть, объединяющую абонентские пункты организаций системы образования Челябинской области (пользователей Защищенной сети) по технологии ViPNet CUSTOM с целью организации защищенного информационного взаимодействия между ними в соответствии с

нормативными актами Российской Федерации в области обеспечения информационной безопасности.

2.2. Основания разработки Положение о защищенной сети Министерства образования и науки Челябинской области (далее - Положение):

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федеральный закон от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации»;

Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 г. Москва «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Приказ 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»;

«Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994).

2.3. Настоящее Положение определяет назначение, состав и устройство Защищенной сети, устанавливает принципы подключения к Защищенной сети и использования сервисов Защищённой сети, функции и полномочия пользователей Защищённой сети, требования к ним, а также правила информационной безопасности.

3. Назначение Защищенной сети

3.1. Защищённая сеть предназначена для решения следующих задач:

обеспечение защищенного информационного взаимодействия между организациями системы образования Челябинской области в соответствии с нормативными актами Российский Федерации в области обеспечения информационной безопасности.

обеспечение защищенного доступа к сервисам и информационным системам Защищенной сети.

4. Пользователи Защищенной сети

4.1. Владелец Защищенной сети – Министерство образования и науки Челябинской области (МОиН Челябинской области).

4.2. Оператор Защищенной сети – Государственное бюджетное учреждение дополнительного профессионального образования «Региональный центр оценки качества и информатизации образования».

4.3. Абонент Защищенной сети – организации системы образования Челябинской области, использующие сервисы Защищенной сети для осуществления уставной деятельности (в том числе органы исполнительной власти Челябинской области и подведомственные им организации, органы местного самоуправления Челябинской области и подведомственные им организации, иные организации осуществляющие образовательную деятельность, организации, осуществляющие обучение).

5. Структура, состав и сервисы Защищенной сети

5.1. Защищенная сеть формируется из следующих структурных компонентов:

5.1.1. центр управления защищенной сети, включающий:

сетевые узлы, представляющие собой компьютеры с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс;

сетевые узлы, представляющие собой компьютеры с установленным программным обеспечением VipNet Administrator;

ViPNet IDS - программно-аппаратный комплекс для обнаружения вторжений в информационные системы;

5.1.2. абонентские пункты - сетевые узлы, представляющие собой компьютеры с установленным программным обеспечением ViPNet Client;

5.2. Основными активами Защищенной сети являются серверы и абонентские пункты.

5.3. В составе Защищённой сети функционируют информационные системы и следующие основные виды серверов:

файловые серверы – серверы, предназначенный для выполнения файловых операций ввода-вывода и хранящий файлы любого типа;

FTP-серверы – серверы, работающие по протоколу передачи файлов FTP (File Transfer Protocol), обеспечивающие обмен файлами между компьютерами по локальной сети и сети Интернет;

Web-серверы – серверы, принимающий запросы от клиентов, обычно веб-браузеров, и выдающие им ответы по протоколу HTTP (HyperHyperText Transfer Protocol - протокол передачи гипертекста), как правило, в виде гипертекстовых документов в формате HTML (в виде Web-сайтов);

серверы баз данных – серверы, выполняющий обслуживание и управление базами данных, отвечающие за целостность и сохранность данных, а также обеспечивающие операции ввода-вывода при работе с базами данных.

5.4. Режим работы Защищённой сети: серверы и структурные компоненты Защищенной сети, за исключением Абонентских пунктов, работают круглосуточно, 7 дней в неделю, за исключением перерывов для проведения аварийно-ремонтных и планово-профилактических работ.

5.5. Центр управления Защищенной сети расположен в Государственном бюджетном учреждении дополнительного профессионального образования «Региональный центр оценки качества и информатизации образования» (далее – ГБУ ДПО РЦОКИО).

5.6. Абонентские пункты расположены в организациях системы образования Челябинской области.

5.7. Абоненты получают доступ к следующим сервисным службам Защищенной сети:

защищенная электронная почта (на базе модуля «Деловая почта» (далее - ПО “Деловая почта”), входящего в состав ПО ViPNet Client, выполняющего функции почтового клиента защищённой почтовой службы, функционирующей в рамках Защищённой сети; основными функциями модуля «Деловая почта» являются передача электронных сообщений, а также прикреплённых к ним файлов по открытым каналам связи с защитой на всём маршруте следования от отправителя до получателя, подтверждение получения и использования сообщений, а также даты, времени получения и личности получателей);

защищенный файловый обмен (сервис, позволяющий Абонентам обмениваться файлами без установки дополнительного программного обеспечения или использования функций операционной системы; основными функциями защищённого файлового обмена являются обмен файлами между абонентами через защищённую транспортную сеть ViPNet, гарантированная доставка и возобновление передачи файлов при обрыве связи);

защищенный обмен мгновенными сообщениями (предназначен для обмена сообщениями в режиме реального времени между абонентами Защищённой сети; основными функциями защищенного обмена мгновенными сообщениями являются передача сообщений между абонентами в защищённом виде, исключающем постороннее вмешательство, обмен сообщениями в режиме конференции, сохранение результатов в протокол);

доступ к информационным ресурсам и информационным системам, функционирующим в рамках Защищенной сети с обеспечением защиты сетевого трафика при обращении к серверам Защищенной сети, разграничения доступа к информационным ресурсам и система Защищенной сети.

6. Функции и полномочия пользователей Защищенной сети

6.1. Обязанности оператора:

разработка единых правил формирования, развития Защищённой сети;

разработка регламента функционирования Защищенной сети, определяющего порядок создания, выдачи, получения и использования дистрибутивов ключевой и справочной информации для подключения пользователей к Защищенной сети (далее - Регламент функционирования Защищенной сети);

разработка регламентирующих документов использования информационных систем, доступ к которым предоставляется с использованием Защищённой сети (совместно с владельцами информационных систем и Защищенной сети);

разработка предложений Владельцу Защищенной сети по формированию и внедрению компонентов Защищённой сети;

проведение мероприятий по модернизации и развитию Защищённой сети;

контроль соблюдения всеми категориями пользователей правил работы и использования компонентов Защищённой сети;

управление режимами работы компьютерного и коммутационного оборудования Защищённой сети и поддержка работоспособности Защищенной сети, в том числе оборудование файловых серверов, серверов ViPNet, серверов баз данных источниками бесперебойного питания, мощность которых в случае отключения электропитания обеспечивает возможность корректного завершения выполняемых задач;

предоставление пользователям Защищенной сети доступа к информационным системам Защищённой сети;

своевременное реагирование на поступившие в систему технической поддержки заявки о неисправностях в работе компонентов Защищённой сети и принятие необходимых мер по их устранению;

восстановление работоспособности компонентов Защищённой сети в технологически возможный короткий срок;

периодические проверки состояния Защищённой сети и своевременное реагирование на попытки несанкционированного доступа;

предоставление Владельцу информации о компонентах Защищённой сети;

информирование Пользователей Защищенной сети о порядке работы и ответственности за нарушение настоящего Положения и Регламента функционирования Защищенной сети;

информирование Пользователей о проводимых работах по обслуживанию и возможных перебоях в работе Защищённой сети;

6.2. Права оператора:

информировать Пользователей о невыполнении их сотрудниками требований безопасности и несоблюдении других требований по обеспечению бесперебойного функционирования Защищённой сети;

запрашивать информацию у Пользователей Защищенной сети о компонентах Защищённой сети;

принимать решение об отключении или ограничении доступа Пользователей к Защищённой сети и информационным системам Защищенной сети в случаях нарушения Пользователями Защищенной сети требований настоящего Положения и Регламента функционирования Защищённой сети.

6.3. Обязанности Абонента Защищенной сети:

выполнять требования настоящего Положения и Регламента функционирования Защищенной сети;

обеспечивать требования действующего законодательства Российской Федерации в области обеспечения информационной безопасности;

проводить мероприятия по оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы, взаимодействующей с Защищенной сетью.

6.4. Права Абонентов Защищенной сети:

использовать сервисы Защищенной сети для осуществления своей уставной деятельности;

обращаться в адрес Оператора Защищенной сети посредством системы технической поддержки по вопросам функционирования, устранения

неисправностей, обеспечения информационной безопасности и развития Защищенной сети.

7. Требования к организациям, в которых расположены абонентские пункты Защищенной сети

7.1. Организации, в которых создаются абонентские пункты Защищенной сети, обязаны соблюдать законодательство Российской Федерации в сфере информационной безопасности, в частности:

назначить ответственного пользователя средств криптографической защиты информации, пользователей средств защиты информации;

обеспечить подготовку пользователей в соответствии с Приказом ФАПСИ от 13 июня 2001 г. N 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»;

обеспечить соответствие АРМ, предназначенного для использования в качестве абонентского пункта требованиям, предъявляемым ПО, устанавливаемым для организации абонентского пункта;

обеспечить наличие на АРМ, предназначенном для использования в качестве абонентского пункта, лицензионного программного обеспечения, необходимого для исполнения требований, предусмотренных Приказом ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва «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»;

обеспечить безопасность помещений, хранилищ, средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в соответствии с Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378 г. Москва «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», Приказом ФАПСИ от 13 июня 2001 г. N 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»;

7.2. Организации, в которых создаются Абонентские пункты Защищенной сети, берут на себя обязательство о проведении комплекса мероприятий по оценки

эффективности принимаемых мер по обеспечению безопасности персональных данных в соответствии с Федеральным законом от 27.07.2006 г. №152 «О персональных данных» и Приказом ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» до ввода в эксплуатацию информационной системы взаимодействующей с Защищенной сетью.

7.2.1. Оценка эффективности принимаемых мер по обеспечению информационной безопасности персональных данных может быть проведена в форме аттестации объекта информатизации в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994), а также в других формах.

7.2.3. Решение о типе оценки эффективности принимаемых мер по обеспечению информационной безопасности персональных данных принимается руководителем Абонентского пункта самостоятельно.

8. Технические мероприятия

8.1. Технические мероприятия по обслуживанию компонентов Защищенной сети и информационных систем проводятся оператором Защищенной сети, при необходимости с привлечением соответствующего пользователя Защищенной сети.

8.2. В случае возникновения производственной необходимости проведения аварийных и планово-профилактических работ Защищённая сеть может быть закрыта для доступа.

8.3. Плановые работы проводятся по графику разрабатываемому Оператором защищенной сети. К плановым работам относятся:

реконфигурирование Защищённой сети;

установка/обновление системного и прикладного программного обеспечения, функционирующего в составе защищенной сети;

техническое обслуживание компонентов Защищённой сети;

другие виды работ, необходимость которых определяется Оператором по согласованию с Владельцем сети.

8.4. О проведение плановых работ Оператор уведомляет Пользователей Защищённой сети не менее чем за 24 часа до начала работ по электронной почте, а также путём размещения соответствующего сообщения на официальном сайте Оператора.

9. Ответственность

9.1. В случае нарушения требований данного Положения, послуживших причиной сбоя функционирования Защищенной сети или несанкционированного доступа к информации циркулирующей в Защищённой сети, все категории пользователей несут ответственность в соответствии с действующим законодательством.

10. Заключительные положения

10.1. Изменения и дополнения в настоящее Положение вносятся соответствующим приказом Министерства образования и науки Челябинской области и доводятся до сведения всех Пользователей при публикации на сайте ГБУ ДПО РЦОКИО в течении 3 рабочих дней со дня издания приказа.