Министерство социальной политики и труда Удмуртской Республики
(Минсоцполитики УР)

Удмурт Элькунысь мерлыко политикая но ужъя министерство
(УЭ мерполитикмин)

ПРИКАЗ

«2» августа 2019 г. № 203

г. Ижевск

Об утверждении Регламента защищённой сети передачи данных VipNet № 577 Министерства социальной политики и труда Удмуртской Республики с использованием технологии VipNet

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» п р и к а з ы в а ю:

1. Утвердить прилагаемый Регламент защищённой сети передачи данных VipNet № 577 Министерства социальной политики и труда Удмуртской Республики с использованием технологии VipNet.

2. Признать утратившим силу приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 11 июня 2015 года № 176 «Об утверждении Регламента защищённой сети передачи данных VipNet № 577 Министерства социальной, семейной и демографической политики Удмуртской Республики с использованием технологии VipNet».

3. Контроль за исполнением настоящего приказа возложить на заместителя министра Белоусову М.Е.

Первый заместитель министра О.В. Лубнина

УТВЕРЖДЁН
приказом Министерства
социальной политики и труда
Удмуртской Республики
от «02» 08 2019 года № 203

РЕГЛАМЕНТ
защищённой сети передачи данных VipNet № 577 Министерства социальной политики и труда Удмуртской Республики с использованием технологии VipNet

I. Общие положения

1. Настоящий Регламент разработан в соответствии с:

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

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённым приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66;

Составом и содержанием 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, утверждённым приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378;

Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждённой приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152.

II. Термины и определения

2. В настоящем Регламенте используются следующие термины и

определения:

1) абонентский пункт защищённой сети передачи данных VipNet № 577 Министерства социальной политики и труда Удмуртской Республики (далее соответственно – АП, Министерство) – компьютер, включённый в список АП и пользователей защищённой сети передачи данных VipNet № 577 Министерства, на котором зарегистрирован хотя бы один пользователь, с установленным средством криптографической защиты информации – программным обеспечением (далее – ПО) VipNet Client, реализующим функции шифрования и электронной подписи (далее - ЭП), в том числе:

создание ЭП в электронном документе с использованием закрытого ключа ЭП;

подтверждение подлинности ЭП в электронном документе с использованием открытого ключа ЭП;

создание закрытых и открытых ключей ЭП.

2) автоматизированное рабочее место (далее – АРМ) VipNet Administrator – аппаратно-программный комплекс, представляющий собой компьютер с установленным ПО VipNet Administrator [Центр управления сетью] и VipNet Administrator [Удостоверяющий и ключевой центр], установленный в Министерстве и эксплуатируемый администратором безопасности защищённой сети передачи данных VipNet № 577 Министерства;

3) администратор безопасности защищённой сети передачи данных VipNet № 577 Министерства (далее – администратор безопасности) – должностное лицо Министерства, назначенное для эксплуатации АРМ Administrator; администратор безопасности одновременно является уполномоченным лицом удостоверяющего центра своей сети, удостоверяющим своей электронной подписью (далее – ЭП) сертификаты ключей ЭП всех остальных пользователей защищённой сети передачи данных VipNet № 577 Министерства;

4) защищённая сеть передачи данных VipNet № 577 Министерства (далее – защищённая сеть VipNet № 577) – информационная система, в которой для защиты информации, передаваемой по каналам открытой сети, используется её шифрование, построенная с использованием технологии VipNet; владельцем защищённой сети VipNet № 577 является Министерство;

5) подтверждение подлинности ЭП в электронном документе – положительный результат проверки средствами АП с использованием сертификата ключа ЭП принадлежности ЭП в электронном документе владельцу сертификата ключа ЭП и отсутствия искажений в электронном документе, подписанном данной ЭП;

6) VipNet Client – ПО, обеспечивающее установление криптографически защищённых соединений, а также возможность гарантированной доставки подписанных ЭП сообщений (файлов) по назначению с автоматическим подтверждением доставки и прочтения документов, а также надёжную защиту компьютера от несанкционированного доступа к различным информационным и аппаратным ресурсам на нём при работе компьютера в локальных или глобальных сетях, например, интернет, в том числе от сетевых атак;

7) VipNet Coordinator (далее – координатор) – ПО, обеспечивающее маршрутизацию почтовых конвертов и управляющих сообщений при взаимодействии центра управления сетью и объектов сети между собой, регистрацию и предоставление информации о текущих IP-адресах и способах подключения объектов защищённой сети VipNet № 577, выполняющее функции VipNet-Firewall и VipNet-сервер открытого интернета;

8) VipNet Administrator [Удостоверяющий и ключевой центр] (далее – УКЦ) – ПО, состоящее из удостоверяющего центра, практически реализующего выполнение функций удостоверяющего центра, связанных с изданием, заверением, отзывом и хранением сертификатов ключей ЭП, а также других функций, предусмотренных Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», и ключевого центра, обеспечивающего формирование и обновление ключевой информации для взаимодействия между узлами защищённой сети VipNet № 577 в соответствии с заданными связями;

9) VipNet Administrator [Центр управления сетью] (далее – ЦУС) – ПО, предназначенное для создания и управления конфигурацией виртуальной сети на базе распределённой системы персональных и межсетевых экранов с использованием технологии VipNet, обеспечивающей защиту функционирования компьютеров и передаваемой информации в защищённой сети VipNet № 577 и решает следующие основные задачи:

построение инфраструктуры виртуальной сети (узлы и связи между ними, включая межсетевые);

изменение конфигурации защищённой сети VipNet № 577;

формирование и рассылка защищённых адресных справочников, защищённых таблиц маршрутизации;

формирование информации о ключевых связях пользователей для ключевого центра;

определение прав доступа к ресурсам каждого пользователя защищённой сети VipNet № 577;

10) пользователь защищённой сети VipNet № 577 – владелец сертификата ключа ЭП, назначенный приказом Министерства о назначении уполномоченных пользователей защищённой сети VipNet № 577 и зарегистрированный хотя бы на одном из АП защищённой сети VipNet № 577 (для АП, расположенных в Министерстве), либо приказом территориального органа Министерства или подведомственного Министерству организации о назначении уполномоченных пользователей защищённой сети VipNet № 577 (для АП, расположенных в территориальных органах Министерства или подведомственного Министерству организации);

11) узел защищённой сети VipNet № 577 (далее – узел) – это функционирующий АП или координатор;

12) программный координатор – компьютер с установленным ПО VipNet Coordinator Windows, обеспечивающий включение в защищённую сеть VipNet № 577 открытых и защищённых компьютеров, находящихся в этой локальной вычислительной сети (далее – ЛВС), независимо от типа адреса, выделяемого

им, разделение и защиту сетей от сетевых атак, оповещение АП о состоянии других сетевых узлов, связанных с ним;

13) программно-аппаратный координатор – транспортный сервер, комплекс технических и программных средств, обеспечивающих доставку информации получателям в виде пакетов;

14) сертификат ключа ЭП (далее – сертификат) – документ на бумажном носителе или электронный документ с ЭП уполномоченного лица удостоверяющего центра, который включает в себя открытый и закрытый ключ ЭП и выдается удостоверяющим центром пользователю защищённой сети VipNet № 577 для подтверждения подлинности ЭП и идентификации владельца сертификата ключа ЭП;

15) средства криптографической защиты информации (далее – СКЗИ) – программно-аппаратные средства, осуществляющие криптографическое преобразование информации для обеспечения её безопасности;

16) технология VipNet – технология, предназначенная для построения защищённой сети VipNet № 577 путём использования системы персональных и межсетевых экранов на защищаемых элементах распределённой сети (рабочие станции, серверы, локальные сети) и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе СКЗИ «Домен-КС3»;

17) ЭП – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца сертификата ключа ЭП, а также установить отсутствие искажения информации в электронном документе;

18) электронный документ (далее – ЭД) – файл определённого типа и внутренней структуры, содержащий информацию, состав которой регламентируется соглашениями или иными нормативными актами. Юридическая значимость документа подтверждается ЭП.

III. Назначение Регламента и область применения

3. Настоящий Регламент устанавливает и определяет режимы работы всех узлов защищённой сети VipNet № 577 в Министерстве и территориальных органах Министерства. Форматы и режимы обмена информацией в защищённой сети VipNet № 577 определены в технологии обмена информацией по телекоммуникационным каналам связи в защищённой сети VipNet № 577.

4. VipNet Administrator устанавливается на АРМ администратора защищённой сети VipNet № 577, утверждённого приказом о назначении ответственными за эксплуатацию защищённой сети VipNet № 577. АРМ VipNet Administrator расположен в помещении, в котором охрана и организация режима соответствуют установленным требованиям.

5. ПО VipNet Coordinator Windows устанавливается на АРМ, выполняющем функции программного координатора в автоматическом режиме.

6. ПО VipNet Client устанавливается на АРМ уполномоченных пользователей защищённой сети VipNet № 577, утверждённых приказом о назначении уполномоченных пользователей защищённой сети VipNet № 577.

7. Все АРМ защищённой сети VipNet № 577 располагаются в помещениях, в которых охрана и организация режима, а также условия хранения установочных дистрибутивов, эксплуатационно-технической документации, ключевых документов, соответствуют установленным требованиям.

8. Пользователи защищённой сети VipNet № 577 признают, что полученные ими ЭД, заверенные ЭП уполномоченных лиц, эквивалентны документам на бумажных носителях, заверенным соответствующими подписями и оттиском печати.

9. Пользователи защищённой сети VipNet № 577 признают, что использование в системе СКЗИ, которые реализуют шифрование и ЭП, достаточно для обеспечения конфиденциальности информационного взаимодействия узлов по защите от несанкционированного доступа и безопасности обработки информации, а также для подтверждения следующих обстоятельств:

ЭД исходит от пользователя защищённой сети VipNet № 577, его передающего (подтверждение авторства документа);

ЭД не претерпел изменений при информационном взаимодействии (подтверждение целостности и подлинности документа);

фактом доставки ЭД является формирование квитанции о доставке ЭД на АП пользователя защищённой сети VipNet № 577, принявшего ЭД.

IV. Регистрация пользователей защищённой сети VipNet № 577 в качестве узлов и АП

10. Регистрация пользователей защищённой сети VipNet № 577 в качестве узлов и АП осуществляется администратором безопасности в АРМ [Администратор] на основании приказа об утверждении перечня абонентских пунктов защищённой сети VipNet № 577 в соответствии с эксплуатационно-технической документацией. На основании введённых данных о пользователе защищённой сети VipNet № 577 и разрешённых связях между узлами формируется ключевой дистрибутив для каждого конкретного пользователя защищённой сети VipNet № 577. Одновременно для каждого конкретного пользователя защищённой сети VipNet № 577 формируется резервный набор персональных ключей, необходимый для дистанционного обновления ключей АП при их компрометации.

11. Регистрация и подключение пользователей территориальных органов Министерства защищённой сети VipNet № 577 осуществляется администратором безопасности в АРМ [Администратор] на основании приказа территориального органа Министерства о назначении уполномоченными пользователями защищённой сети VipNet № 577.

12. В соответствии с заключенными соглашениями со сторонними организациями создаётся межсетевое взаимодействие защищённой сети VipNet № 577 и защищённой сети сторонней организацией, а также устанавливается связь между пользователями.

13. Ключевой дистрибутив вместе с паролем доступа к нему, резервным набором персональных ключей и эксплуатационно-технической документацией ПО VipNet [Клиент] передаётся лично пользователю защищённой сети VipNet № 577 или по защищённому каналу связи.

14. Установка ПО VipNet [Клиент] на АП производится с использованием выданных ключевых дистрибутивов, одновременно организуется допуск пользователя защищённой сети VipNet № 577 к работе с АП. Резервные наборы персональных ключей пользователей защищённой сети VipNet № 577, необходимые для дистанционного обновления ключей АП при их компрометации, хранятся у администратора безопасности для АП, расположенных в Министерстве, или уполномоченных пользователей защищённой сети VipNet № 577, расположенных в территориальных органах Министерства, на съёмном носителе.

15. ЭП из состава ключевого дистрибутива, сформированного УКЦ, применяется только для постоянного функционирования защищённого канала защищённой сети VipNet № 577.

16. Использование ключей ЭП пользователя защищённой сети VipNet № 577 из состава его ключевого дистрибутива допускается в процессе обучения и допуска пользователя защищённой сети VipNet № 577 к работе с АП.

17. Пользователи защищённой сети VipNet № 577 должны подписывать ЭД только ключом ЭП, выданным Удостоверяющим центром аккредитованным в соответствии с требованиями Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и имеющим лицензию Федеральной службы безопасности Российской Федерации на осуществление работ по защите информации (не содержащей сведений, составляющих государственную тайну) с использованием шифровальных (криптографических) средств (далее – аккредитованный УЦ).

18. Дистрибутивы ПО VipNet, действующие и отозванные сертификаты ключей ЭП АП, расположенных в Министерстве, хранятся в сейфе администратора безопасности. Дистрибутивы ПО VipNet, действующие и отозванные сертификаты ключей ЭП АП, расположенных в территориальных органах Министерства, хранятся в сейфе руководителя территориального органа Министерства. Лица, ответственные за хранение дистрибутивов и средств ЭП ведут журнал учёта по форме согласно приложению 1 к настоящему Регламенту.

19. По окончании срока действия сертификатов ЭП, а также бумажные копии сертификатов ЭП, изымаются и передаются в архив. Срок архивного хранения составляет не менее чем пять лет. По истечении срока хранения ключи ЭП уничтожаются по акту об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов, оформленному согласно приложению 2 к настоящему Регламенту.

V. Издание и плановая замена сертификатов пользователям защищённой сети VipNet № 577

20. Издание сертификата пользователям защищённой сети VipNet № 577, сформированного УКЦ, осуществляется администратором безопасности в АРМ VipNet [Администратор].

21. Для юридически значимого информационного обмена ЭД издание сертификата пользователям защищённой сети VipNet № 577 осуществляется аккредитованным УЦ.

22. Сертификат, полученный аккредитованным УЦ, вводится в действие администратором безопасности в ПО VipNet [Клиент].

23. Срок действия сертификата устанавливается в один год. Администратор безопасности производит периодическую (плановую) замену используемых ключей ЭП не реже указанного срока. ПО АП заблаговременно информирует пользователя защищённой сети VipNet № 577 о необходимости проведения данной процедуры.

24. Замена ключа ЭП осуществляется в обязательном порядке, если изменился любой из реквизитов, указанных в сертификате. При этом владелец сертификата обязан заблаговременно известить администратора безопасности о характере изменения реквизитов и согласовать с ним дату и порядок замены ключа ЭП.

25. Замена сертификата пользователя защищённой сети VipNet № 577, сформированного УКЦ, производится автоматизировано непосредственного на АП путём формирования нового сертификата администратором безопасности в АРМ VipNet [Администратор].

26. Замена сертификата пользователя защищённой сети VipNet № 577, полученного из аккредитованного УЦ, до истечения срока его действия осуществляется администратором безопасности непосредственно на АП путём установки контейнера ключа ЭП в ПО VipNet [Клиент] со съёмного носителя (eToken).

VI. Замена ключей ЭП пользователям защищённой сети VipNet № 577 в случае их компрометации

27. Если возникает сомнение в неизвестности посторонним лицам пароля доступа пользователя защищённой сети VipNet № 577 при старте модуля VipNet, но доступ к компьютеру этих посторонних лиц был невозможен, пользователю защищённой сети VipNet № 577 следует сменить пароль и продолжить работу. Если доступ к компьютеру посторонних лиц был возможен, то ключи ЭП пользователя защищённой сети VipNet № 577 считаются скомпрометированными.

28. К событиям компрометации, когда ключи ЭП пользователя защищённой сети VipNet № 577 считаются скомпрометированными, также относятся следующие случаи:

посторонним лицам мог стать доступным файл ключевого дистрибутива пользователя защищённой сети VipNet № 577;

посторонним лицам мог стать доступным съемный носитель с ключевой информацией пользователя защищённой сети VipNet № 577;

посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере пользователя защищённой сети VipNet № 577;

на АП отсутствовал (был отключен) модуль VipNet [Клиент] или он устанавливался в 4-й или 5-й режим работы, и в ЛВС считается возможным присутствие посторонних лиц;

на АП отсутствовал (был отключен) модуль VipNet [Клиент] или он устанавливался в 4-й или 5-й режим работы, и на границе ЛВС отсутствовал (был отключен) сертифицированный межсетевой экран VipNet [Координатор], или он устанавливался в 4-й или 5-й режим работы;

на сейфе с ключевыми документами (резервным набором персональных ключей) нарушена печать;

в ЭП под входящим ЭД имеется сертификат, находящийся в списке отозванных сертификатов;

во входящем документе, полученном по защищённой сети VipNet № 577 и имеющем ЭП, навязывается заведомо ложная информация;

случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в т.ч. когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошёл в результате несанкционированных действий злоумышленника).

29. В случае наступления любого из событий, связанных с компрометацией ключевой информации, пользователь защищённой сети VipNet № 577 немедленно прекращает связь с другими АП и сообщает о факте компрометации (или предполагаемом факте компрометации) администратору безопасности.

30. Администратор безопасности при получении сообщения о компрометации ключевой информации определяет объём скомпрометированной ключевой информации, в том числе факт компрометации резервного набора персональных ключей ЭП, исходя из следующих правил:

в случае признания факта компрометации любого из секретных ключей ЭП, записанных на съёмном носителе, признаются непосредственно скомпрометированными все ключи ЭП на данной съёмном носителе. Данный пользователь защищённой сети VipNet № 577 признается непосредственно скомпрометированным;

в случае признания факта непосредственной компрометации любого из ключей ЭП у любого АП защищённой сети VipNet № 577 однозначно признаются скомпрометированными все ключи ЭП общие для АП; АП, не подвергшиеся непосредственной компрометации, признаются косвенно скомпрометированными; у АП, не подвергшихся непосредственной

компрометации, не скомпрометированными могут быть признаны только индивидуальные ключи ЭП (например, секретный ключ ЭП);

в случае признания факта компрометации любого из секретных ключей ЭП, записанных на жестком диске, признаются скомпрометированными все ключи ЭП данного АП.

31. Администратор безопасности при получении сообщения о компрометации ключевой информации в течение одного рабочего дня:

в ПО ЦУС объявляет ключи ЭП скомпрометированного АП скомпрометированными и создает средствами ПО ЦУС справочники связей при компрометациях с необходимой информацией для УКЦ: файлы связей для полной замены индивидуальной ключевой информации скомпрометированных пользователей защищённой сети VipNet № 577 и замены ключей ЭП АП, где зарегистрированы скомпрометированные пользователей защищённой сети VipNet № 577; файлы связей для частичного обновления ключевой информации для всех АП, с которыми связаны АП, где зарегистрированы скомпрометированные пользователи защищённой сети VipNet № 577; файлы связей для частичного обновления индивидуальной ключевой информации для АП с нескомпрометированными ключами ЭП, зарегистрированных в защищённой сети VipNet № 577, где имеются скомпрометированные пользователи защищённой сети VipNet № 577;

оповещает о факте компрометации ключей всех АП, связанных со скомпрометированным пользователем защищённой сети VipNet № 577, после получения данного сообщения АП не должны использовать скомпрометированные ключи ЭП;

формирует средствами УКЦ для генерации ключей ЭП при компрометации новую ключевую информацию; все сформированные файлы с новой ключевой информацией зашифрованы на нескомпрометированных ключах ЭП из резервного набора персональных ключей ЭП, поэтому могут передаваться на скомпрометированный АП и скомпрометированному пользователю защищённой сети VipNet № 577 по любым каналам связи, в том числе и открытым;

производит рассылку сформированных обновлений ключей ЭП на узлы, в том числе и скомпрометированному пользователю защищённой сети VipNet № 577 при наличии у него нескомпрометированного резервного набора персональных ключей ЭП;

в случае признания факта компрометации секретного ключа ЭП пользователей защищённой сети VipNet № 577, средствами УКЦ отзывает (аннулирует) сертификат этого АП; производит рассылку списка отозванных сертификатов всем АП защищённой сети VipNet № 577, а также во все взаимодействующие УЦ.

32. Отозванные сертификаты пользователя защищённой сети VipNet № 577 не удаляются из базы УКЦ и хранятся в течение всего срока действия УЦ для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

33. Информация, содержащаяся на скомпрометированных съёмных ключевых носителях, после проведения служебного расследования должна быть уничтожена с использованием штатных средств ПО VipNet.

34. В случае признания факта компрометации резервного набора персональных ключей ЭП скомпрометированного пользователя защищённой сети VipNet № 577, для него средствами УКЦ создается ключевая дискета с новыми ключами ЭП.

35. В случае компрометации ключей ЭП администратора безопасности считается скомпрометированной вся ключевая информация в защищённой сети VipNet № 577, т.е. ключи ЭП всех АП. В этом случае должна быть немедленно остановлена работа на симметричных ключах шифрования и оповещены администраторы безопасности сторонних организаций. Для восстановления работы системы необходимо:

удалить с жёсткого диска УКЦ все ключи с использованием штатных средств ПО УКЦ;

начать формирование ключевой системы с нулевой отметки согласно эксплуатационной документации на ПО УКЦ.

VII. Отзыв (аннулирование) сертификатов пользователей защищённой сети VipNet № 577

36. Отзыв (аннулирование) сертификата осуществляется администратором безопасности при окончании срока действия сертификата или увольнении пользователя защищённой сети VipNet № 577.

37. Администратор безопасности в течение одного рабочего дня отзывает (аннулирует) сертификат.

38. Отозванные сертификаты пользователя защищённой сети VipNet № 577 не удаляются из базы УКЦ и хранятся в течение всего срока действия УЦ для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

VIII. Режимы работы программно-аппаратных средств защищённой сети VipNet № 577

39. Режим работы программно-аппаратного координатора HW-1000 и программного координатора VipNet: 365/24/7.

40. Отключение программно-аппаратного координатора HW-1000 и программного координатора VipNet выполняется при возникновении следующих обстоятельств:

выполнение профилактических работ;

отключение электричества в здании Министерства более чем на 30 минут;

технические неисправности;

возникновение обстоятельств непреодолимой силы, т.е. чрезвычайных и непредотвратимых при данных условиях обстоятельств, в том числе

объявленная или фактическая война, гражданские волнения, эпидемии, блокада, эмбарго, пожары, землетрясения, наводнения и другие стихийные природные бедствия, а также издание актов государственных органов.

41. Включение программно-аппаратных координаторов HW-1000 и компьютеров с установленным ПО VipNet [Клиент] выполняется до 09.00 часов в рабочие дни.

42. Отключение программно-аппаратных координаторов HW-1000 и компьютеров с установленным ПО VipNet [Клиент] выполняется перед выходом из служебного помещения в конце рабочего дня.

IX. Порядок осуществления обмена ЭД

43. Пользователи защищённой сети VipNet № 577 имеют право передавать:

ЭД, содержащие персональные данные;

ЭД, касающиеся деятельности Министерства и его территориальных органов в сфере информационно-коммуникационных технологий.

Контроль поступления ЭД в защищённую сеть VipNet № 577 ведётся пользователями с интервалом 30 минут в течение рабочего дня. Поступившие ЭД, требующие регистрации, регистрируются в Министерстве и территориальных органах Министерства в соответствии с инструкцией по делопроизводству.

44. Отправленные и полученные ЭД сохраняются в зашифрованном виде внутри ПО VipNet [Клиент] в течение календарного года, затем архивируются в соответствии с инструкцией ПО VipNet [Клиент] и хранятся в течение сроков, предусмотренных номенклатурами дел Министерства и территориальных органов Министерства.

45. Пользователи защищённой сети VipNet № 577 обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учётных данных, содержащихся в электронных журналах регистрации ЭД, которые ведутся автоматизированным способом внутри ПО VipNet [Клиент].

46. Пользователи защищённой сети VipNet № 577 обязаны письменно не позднее чем за 2 (два) рабочих дня известить друг друга о начале и окончании обстоятельств форс-мажора, препятствующих выполнению обмена ЭД и предоставить необходимые документы или доказать, что эти обстоятельства действительно имели место, в противном случае все пункты настоящего Регламента выполняются без изменений.

X. Перечень эксплуатационно-технической документации

47. Администратор безопасности должен руководствоваться следующей эксплуатационно-технической документацией:

VipNet Центр Управлению Сетью (Руководство Администратора);

VipNet Administrator [Удостоверяющий и Ключевой Центр] (Руководство Администратора);

48. Пользователь защищённой сети VipNet № 577 в своей работе с ПО VipNet [Клиент] должен руководствоваться следующей эксплуатационно-технической документацией:

VipNet Client [Монитор] (Руководство Пользователя);

VipNet Client [Деловая Почта] (Руководство Пользователя).

XI. Порядок разбора конфликтных ситуаций

49. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения пользователями защищённой сети VipNet № 577 и/или внешней организации ЭД, а также использованием в данных документах ЭП, а также корректной работы ПО VipNet [Клиент].

50. Разбор конфликтных ситуаций осуществляется в два этапа. Сначала путём взаимодействия на пользователя защищённой сети VipNet № 577 Стороны, у которой возникли претензии, с администратором безопасности или уполномоченным представителем аккредитованного УЦ. В случае если пользователь защищённой сети VipNet № 577 не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза.

XII. Ответственность участников защищённой сети VipNet № 577

51. Пользователь защищённой сети VipNet № 577 несёт ответственность за достоверность сведений, указанных им в сертификате пользователя защищённой сети VipNet № 577, а также обязан сообщать администратору безопасности обо всех изменениях этих сведений.

52. Пользователь защищённой сети VipNet № 577 несёт ответственность за сохранность и правильность эксплуатации СКЗИ и своих закрытых ключей ЭП.

53. В случае несвоевременного сообщения о факте компрометации ключей ЭП, пользователь защищённой сети VipNet № 577, допустивший компрометацию ключей ЭП, несёт ответственность в полном объёме за ущерб, причинённый им другим пользователям защищённой сети VipNet № 577.

54. Администратор безопасности не несёт ответственности за последствия и убытки в случае нарушения пользователями защищённой сети VipNet № 577 положений настоящего Регламента.

55. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту пользователи защищённой сети VipNet № 577 несут ответственность в соответствии с действующим законодательством Российской Федерации.

XIII. Взаимодействие сторон при нештатных ситуациях

56. При возникновении нештатных ситуаций, таких как: выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств ЭП и др., пользователь защищённой сети VipNet № 577 обязан:

руководствоваться положениями и инструкциями эксплуатационной документации;

сообщить о возникшей ситуации администратору безопасности;

выполнять указания администратора безопасности, касающиеся выхода из данной внештатной ситуации.