Приложение к приказу БУЗОО «МИАЦ»

от «\_\_\_» \_\_\_\_\_\_\_\_ 2021 г. № \_\_\_\_\_\_

«Приложение к приказу БУЗОО «МИАЦ»

от «13» мая 2015 г. № 14

##### РЕГЛАМЕНТ

##### удостоверяющего центра бюджетного учреждения здравоохранения

##### Омской области «Медицинский информационно-аналитический центр»

##### (VPN № 798)

###### 1. Общие положения

1.1. Настоящий Регламент удостоверяющего центра бюджетного учреждения здравоохранения Омской области «Медицинский информационно-аналитический центр» (VPN № 798) (далее соответственно − Регламент, БУЗОО «МИАЦ») определяет основные принципы использования электронной подписи (далее − ЭП) при организации управления системой сертификации ключей подписи на базе средства криптографической защиты информации (далее − СКЗИ) ViPNet CSP, реализующего функции шифрования информации и ЭП.

1.2. Целью настоящего Регламента является создание необходимых условий для реализации в защищенной сети передачи данных (далее − ЗСПД) БУЗОО «МИАЦ» требований действующего законодательства Российской Федерации по использованию ЭП, при соблюдении которых ЭП в электронном документе (далее − ЭД) признается равнозначной собственноручной подписи в документе на бумажном носителе.

1.3. Регламент разработан в соответствии с требованиями Федеральных законов от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»,   
от 7 июля 2003 года № 126-ФЗ «О связи», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и является основным руководящим документом для абонентов Удостоверяющего центра (далее − УЦ) БУЗОО «МИАЦ».

1.4. Настоящий Регламент публикуется:

* на официальном сайте БУЗОО «МИАЦ»;

− по запросу через почтовый адрес: г. Омск, 644021, ул. 8-я Линия,   
д. 219а.

###### 2. Термины и определения

Абонент ЗСПД БУЗОО «МИАЦ», абонент − пользователь услугами связи ЗСПД БУЗОО «МИАЦ», с которым заключен договор об оказании таких услуг при выделении для этих целей в качестве уникального кода идентификации ключа электронной подписи.

Абонентский пункт ЗСПД БУЗОО «МИАЦ», абонентский пункт   
(далее – АП) – комплекс технических и программных средств, который предназначен для связи удаленного пользователя с электронной вычислительной машиной (далее – ЭВМ) или другим абонентским пунктом посредством каналов связи ЗСПД БУЗОО «МИАЦ», и имеющий в своем составе СКЗИ ViPNet, компьютер, на котором зарегистрирован хотя бы один абонент, с установленным СКЗИ − программным обеспечением (далее − ПО) ViPNet [Клиент], реализующим функции шифрования и/или ЭП, в том числе:

* подписание ЭД с использованием ключа ЭП;
* подтверждение с использованием открытого ключа ЭП подлинности ЭП в ЭД;
* контроль целостности и достоверности ключей и сертификатов;
* предупреждение о приближающемся истечении срока действия сертификата;
* создание ключей ЭП, ключей проверки ЭП и электронных запросов в УЦ на получение новых сертификатов.

Автоматизированное рабочее место (далее − АРМ) ViPNet [Администратор] − аппаратно-программный комплекс (далее − АПК), представляющий собой ЭВМ/персональную ЭВМ, расположенный на территории БУЗОО «МИАЦ» с установленным ПО ViPNet [Центр управления сетью] (далее − ЦУС) и ViPNet [Удостоверяющий и Ключевой центр] (далее − УКЦ).

Администратор безопасности (далее − АБ) − должностное лицо БУЗОО «МИАЦ», ответственное за защиту АРМ ViPNet [Администратор] и ViPNet [Координатор] от несанкционированного доступа к информации.

Владелец ключевой информации (далее – владелец КИ) − лицо, которому в установленном приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 порядке выдана ключевая информация.

Владелец сертификата ключа проверки электронной подписи (далее − владелец СКПЭП) − лицо, которому в установленном Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки ЭП. Владельцем СКПЭП, изданного УЦ БУЗОО «МИАЦ», может быть только сотрудник учреждения, наделенный полномочиями ведения переписки учреждения согласно уставным документам учреждения или доверенности учреждения на право подписания ЭД.

Доверенное лицо УЦ (главный абонент сети ViPNet) − лицо, уполномоченное руководителем УЦ удостоверять сертификаты ключей проверки ЭП, выдаваемых УЦ от имени УЦ, на своем ключе ЭП.

Доверенный способ передачи информации − способ передачи информации, принятый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности и обеспечивающий требуемую степень её защищенности.

Дублер − человек, исполняющий обязанности абонента на время его отсутствия (отпуск, командировка и.т.п.).

Защищенная сеть связи − информационно-телекоммуникационная сеть, в которой обеспечивается, в том числе с использование СКЗИ, защита от несанкционированного доступа к передаваемой информации

Защищенная сеть передачи данных БУЗОО «МИАЦ» − защищенная сеть связи специального назначения, оператором которой является БУЗОО «МИАЦ».

Ключ проверки электронной подписи − уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее − проверка ЭП).

Ключ электронной подписи − уникальная последовательность символов, предназначенная для создания ЭП.

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

Ключевой дистрибутив − файл с расширением .DST, создаваемый в ПО УКЦ для каждого абонента сетевого узла, в котором в зашифрованном на парольном ключе виде помещена необходимая адресная и ключевая информация для обеспечения первичного запуска на компьютере ПО ViPNet [Клиент] или ViPNet [Координатор].

Компрометация ключа − утрата доверия к тому, что используемые ключи шифрования и/или ЭП обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Конфликтная ситуация − ситуация, при которой у владельца СКПЭП возникает необходимость разрешения вопросов признания или не признания авторства и/или подлинности ЭД, обработанных с помощью средств ЭП.

Коллектив – это совокупность абонентов одного сетевого узла, имеющих одинаковые ключи для шифрования конфиденциальной информации.

ПО ViPNet [Центр управления сетью] − ПО, предназначенное для создания и управления конфигурацией виртуальной сети на базе распределенной системы персональных и межсетевых экранов на базе технологии ViPNet, обеспечивающей защиту функционирования компьютеров и передаваемой информации в ЗСПД БУЗОО «МИАЦ», и решает следующие основные задачи:

* построение инфраструктуры виртуальной сети (узлы защищенной сети и связи между ними, включая межсетевые);
* изменение конфигурации сети;
* формирование и рассылка защищенных адресных справочников, защищенных таблиц маршрутизации;
* формирование информации о ключевых связях абонентов для ключевого центра;
* определение прав доступа к ресурсам каждого абонента.

Плановая смена ключей − смена ключей с установленной периодичностью, не вызванная компрометацией ключей.

Подтверждение подлинности электронной подписи в электронном документе − положительный результат проверки средствами АП с использованием СКПЭП принадлежности ЭП в ЭД владельцу сертификата ключа проверки ЭП и отсутствия искажений в подписанном данной ЭП ЭД.

Регламент − настоящий Регламент УЦ БУЗОО МИАЦ» (VPN № 798).

Сертификат ключа проверки электронной подписи − ЭД или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

Список отозванных сертификатов (далее − СОС) − список сертификатов ключей проверки электронной подписи, действие которых было прекращено или которые были отозваны (аннулированы) доверенным лицом УЦ БУЗОО МИАЦ» в ПО УКЦ (до окончания срока их действия) и на данный момент недействительны.

Средства криптографической защиты информации (СКЗИ) − программные и программно-аппаратные средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства удостоверяющего центра − программные и/или аппаратные средства, используемые для реализации функций УЦ.

Средства электронной подписи − шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Технология ViPNet − технология, предназначенная для построения защищенной сети путем использования системы персональных и межсетевых экранов на защищаемых элементах распределенной сети (рабочие станции, сервера, локальные сети), и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе СКЗИ «ViPNet CSP».

Удостоверяющий центр − юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче СКПЭП, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Узел защищенной сети, узел − это функционирующий абонентский пункт или координатор ViPNet.

Уполномоченное лицо − физическое лицо, являющееся сотрудником юридического лица и наделенное полномочиями ведения переписки учреждения согласно уставным документам учреждения или доверенности учреждения на право подписания ЭД.

Учреждение − медицинские организации или иные организации, которым необходим информационный обмен с БУЗОО «МИАЦ» и медицинскими организациями, находящимся на территории Омской области.

Электронная подпись − информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронный документ − документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием ЭВМ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

ViPNet [Координатор] − ЭВМ с установленным ПО ViPNet Coordinator или программно-аппаратный комплекс ViPNet Coordinator, который устанавливается на границе локальной вычислительной сети (далее − ЛВС) и обеспечивает:

* включение в защищенную сеть открытых и защищенных компьютеров, находящихся в этой ЛВС, независимо от типа адреса, выделяемого им;
* разделение и защиту сетей от сетевых атак;
* оповещение АП о состоянии других сетевых узлов, связанных с ним.

###### 3. Статус и область действия УЦ

* 1. Функции УЦ для Учреждений (VPN № 798) выполняет БУЗОО «МИАЦ».
  2. УЦ БУЗОО «МИАЦ» вправе выдавать усиленную неквалифицированную ЭП.

При необходимости организуется защищенный юридически значимый электронный документооборот с внешними организациями согласно Регламенту регистрации и подключения к УЦ БУЗОО «МИАЦ» абонентов сторонних организаций (Приложение № 2 к настоящему Регламенту) с заключением Соглашения об обмене ЭД между Учреждениями и внешней организацией (Приложение № 1 к настоящему Регламенту).

###### 4. Условия признания равнозначности ЭП и собственноручной подписи

4.1. Информация в электронной форме, полученная абонентом ЗСПД БУЗОО «МИАЦ», подписанная неквалифицированной ЭП, признается ЭД, равнозначным эквивалентным такому же документу на бумажном носителе, заверенному собственноручной подписью должностного лица, от имени которого получен документ и печатью организации, на основании Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и настоящего Регламента при условии соблюдения следующих условий:

* отсутствует информация о внесении изменений в подписанный электронной подписью электронный документ;
* СКПЭП, соответствующий ЭП полученного ЭД, не утратил силу (действует) на момент получения документа средствами АП, указанный в соответствующем журнале регистрации АП, или на момент подписания данного документа, указанный при проверке его свойств, средствами АП в соответствующем реквизите;
* подлинность ЭП в ЭД подтверждена средствами АП;
* ЭП в ЭД используется в соответствии со сведениями, указанными в СКПЭП;
* СКПЭП, относящийся к ЭП полученного документа, издан в УЦ БУЗОО «МИАЦ» или во внешнем УЦ, если с указанным сторонним УЦ соответствующим договором (соглашением) установлены доверительные отношения.

4.2. При одновременном наличии ЭД, подлинность ЭП которого подтверждается с помощью средств АП, и эквивалентного ему документа на бумажном носителе, заверенного собственноручной подписью и печатью, подлинником документа считается ЭД, а документ на бумажном носителе − его бумажной копией.

###### 5. Функции УЦ

5.1. Функции УЦ БУЗОО «МИАЦ» (VPN № 798):

* создание ключевых дистрибутивов при регистрации новых   
  АП ЗСПД БУЗОО «МИАЦ», а также при регистрации на АП ЗСПД   
  БУЗОО «МИАЦ» новых абонентов с гарантией конфиденциальности   
  ключа ЭП;
* формирование СКПЭП и/или ключевой информации должностных лиц Учреждений;
* создание АП и допустимых связей между ними;
* рассылка всем узлам сети справочно-ключевой информации;
* организация межсетевого взаимодействия с целью установления защищенных связей между Абонентами;
* установление сроков действия СКПЭП;
* приостановление и возобновление действия СКПЭП (ключевой информации) должностных лиц Учреждений, а также их отзыв (аннулирование);
* ведение реестра изданных СКПЭП, обеспечение его актуальности и возможности доступа к нему абонентов ЗСПД БУЗОО «МИАЦ» и взаимодействующих информационных систем;
* проверка уникальности ключей проверки ЭП в реестре СКПЭП;
* выдача СКПЭП в форме документов на бумажных носителях и/или в форме ЭД с информацией об их действии;
* подтверждение по обращениям владельцев СКПЭП подлинности ЭП в ЭД в отношении выданных УЦ СКПЭП;
* осуществление иной, связанной с использованием ЭП, деятельности.

5.2. Обязанности УЦ БУЗОО «МИАЦ» (VPN № 798):

* информировать в письменной форме заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки;
* обеспечивать актуальность информации, содержащейся в реестре СКПЭП, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
* безвозмездно предоставлять любому абоненту по его официальному запросу в УЦ информацию, содержащуюся в реестре СКПЭП, в том числе информацию об аннулировании СКПЭП;
* обеспечивать конфиденциальность УЦ ключей ЭП и ключевой информации.

6. Присоединение к Регламенту УЦ БУЗОО «МИАЦ» (VPN № 798)

1. БУЗОО «МИАЦ» считается присоединившимся к регламенту априори.
2. Любая организация, желающая присоединиться к регламенту УЦ БУЗОО «МИАЦ», должна выполнить ряд определенных условий:
   * приобрести, если не имеет в наличии в нужном количестве, необходимое ПО (или АПК), поддерживаемое УЦ БУЗОО «МИАЦ» (ViPNet [Клиент] и/или ViPNet [Координатор]);
   * обеспечить своевременную синхронизацию версии программного обеспечения ViPNet на своих узлах сети путем обновления программного обеспечения специалистами, имеющими навыки и соответствующий уровень квалификации;
   * иметь действующую непрерывную техническую поддержку на свои узлы сети ViPNet, обеспечивающую стабильную работу ЗСПД;
   * обеспечить эксплуатацию используемого ПО, в соответствии с эксплуатационно-технической документацией, законодательными и руководящими документами на СКЗИ и ЭП, действующими в Российской Федерации;
   * подать заявление о присоединении к Регламенту УЦ БУЗОО «МИАЦ» по форме согласно приложению № 7 к настоящему Регламенту.

БУЗОО «МИАЦ» вправе запросить, а организация (уже присоединившаяся или присоединяющаяся к Регламенту) обязана предоставить подтверждение выполнения требований, указанных в п. 6.2 настоящего Регламента.

6.3. УЦ вправе запросить, а сторона, присоединившаяся к Регламенту, обязана представить документы, подтверждающие достоверность информации для включения в СКПЭП или при создании ключевой информации, либо их надлежащим образом заверенные копии:

* устав организации, положение или иной уставной документ в соответствии с законом;
* учредительный договор (при наличии);
* документ, подтверждающий государственную регистрацию организации или факт внесения записи о юридическом лице (индивидуальном предпринимателе) в Единый государственный реестр юридических лиц (индивидуальных предпринимателей);
* свидетельство о постановке на учет в налоговом органе;
* документ, удостоверяющий личность заявителя;
* доверенность или иной документ, подтверждающий право заявителя действовать от присоединившейся стороны;
* копии протоколов, либо иных документов, о назначении полномочных представителей организации и/или надлежащим образом оформленные доверенности;
* надлежащим образом заверенный перевод на русский язык легализованных в установленном порядке документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);
* документы, указывающие на ограничения использования СКПЭП (если такие ограничения устанавливаются).

###### 7. Регистрация должностных лиц Учреждений

###### в качестве абонентов ЗСПД БУЗОО «МИАЦ»

7.1. Для регистрации абонентов в УЦ БУЗОО «МИАЦ» представляется заявление на изготовление СКПЭП по форме согласно приложению № 8 или заявление на изготовление ключевой информации по форме согласно приложению № 9 к настоящему Регламенту, согласие на обработку персональных данных по форме согласно приложению № 13.

7.2. Регистрация АП и абонентов ЗСПД БУЗОО «МИАЦ» в качестве узлов и абонентов сети ViPNet (VPN № 798) осуществляется доверенным лицом УЦ в АРМ ViPNet [Администратор] (согласно доверенности по форме согласно приложению № 10 к настоящему Регламенту) в соответствии с эксплуатационно-технической документацией организации-разработчика ПО ViPNet. На основании введенных данных об АП, абонентах и разрешенных связях между узлами формируется ключевой дистрибутив для каждого конкретного абонента. Одновременно для каждого конкретного абонента формируется резервный набор персональных ключей, необходимый для дистанционного обновления ключей абонента при их компрометации.

7.3. Ключевой дистрибутив с паролем доступа к нему, резервным набором персональных ключей передается лично абоненту (или его доверенному лицу согласно доверенности по форме согласно приложению   
№ 12 к настоящему Регламенту) одним из установленных доверенных способов, о чем делается отметка в журнале учета выдачи ключевой информации (приложение № 3 к настоящему Регламенту). Журнал ведется доверенным лицом УЦ БУЗОО «МИАЦ».

7.4. Установка ПО ViPNet [Клиент] на АП производится с использованием выданных ключевых дистрибутивов абонентов, одновременно организуется допуск абонентов к работе с АП. Съемный носитель (например, флэш-накопитель) с выданным резервным набором персональных ключей абонента, необходимым для дистанционного обновления ключей абонента при их компрометации, должен храниться в безопасном месте, например, в опечатываемом сейфе, отдельно от ключевых дистрибутивов абонентов.

7.5. Абонент ЗСПД БУЗОО «МИАЦ» имеет право:

7.5.1. Обратиться в УЦ:

* для получения СКПЭП и ключа ЭП с записью их на ключевой носитель;
* за подтверждением статуса СКПЭП в реестре СКПЭП и подлинности ЭП в ЭД;
* для аннулирования СКПЭП.

7.5.2. Получить список отозванных СКПЭП.

7.5.3. Получить в электронной форме копии СКПЭП уполномоченных лиц Абонента системы, внесенных в реестр СКПЭП.

7.5.4. Применять копии открытых ключей ЭП в электронной форме для проверки ЭП ЭД в соответствии со сведениями, указанными в СКПЭП.

7.5.5. Применять список отозванных СКПЭП для проверки статуса СКПЭП.

7.6. Абонент ЗСПД БУЗОО «МИАЦ» обязан:

7.6.1. Предоставить в УЦ в соответствии с пунктом 6 настоящего Регламента сведения, необходимые для их регистрации в УЦ и выдачи СКПЭП.

7.6.2. Хранить в тайне пароль, используемый для подписания ЭД закрытым ключом ЭП, в течение срока действия СКПЭП.

7.6.3. Хранить в тайне закрытый ключ ЭП в течение срока действия СКПЭП, принимать все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования.

7.6.4. Обеспечивать сохранность, целостность и работоспособность АП.

7.6.5. Своевременно информировать УЦ о компрометации ключей ЭП.

7.5.6. Не использовать ключи ЭП, если Абоненту ЗСПД БУЗОО «МИАЦ» известно, что эти ключи используются или использовались ранее другими лицами.

7.6.7. Обратиться в УЦ для плановой замены СКПЭП не ранее чем за четырнадцать и не позднее чем за три календарных дня до окончания срока его действия.

7.6.8. Незамедлительно обратиться в УЦ с заявлением об аннулировании (отзыв) СКПЭП по форме согласно приложению № 11 при наличии оснований полагать, что тайна закрытого ключа ЭП нарушена.

7.6.9. Предоставлять отчеты об уничтоженных ключевых документах, полученных в УЦ, в течении трех дней после оформления соответствующего акта об их уничтожении. Отчеты предоставляются в УЦ в форме сканированных копий актов об уничтожении ключевых документов.

7.6.10. Соблюдать настоящий Регламент.

###### 8. Издание СКПЭП абонентов

8.1. Издание СКПЭП абонента осуществляется доверенным лицом УЦ БУЗОО «МИАЦ» в АРМ ViPNet [Администратор] на основании электронного запроса абонента на сертификат и/или его заявления на сертификат. Электронный запрос формируется ПО АП, при этом автоматически вырабатываются новые ключи подписи абонента.

В заявлении абонента на сертификат при необходимости уточняются реквизиты абонента, указанные в электронном запросе, и иные сведения, включаемые в СКПЭП.

Заявление подписывается собственноручной подписью абонента. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

БУЗОО «МИАЦ» в установленном порядке идентифицирует абонента. Идентификация абонента проводится при его личном присутствии, при предъявлении документа удостоверяющего личность.

8.2. Все изданные СКПЭП учитываются в Реестре изданных (действующих) СКПЭП (приложение № 4 к настоящему Регламенту). Реестр ведется доверенным лицом УЦ БУЗОО «МИАЦ».

8.3. Электронные запросы на СКПЭП и изданные СКПЭП абонентов хранятся в АРМ ViPNet [Администратор] и на АП абонентов в электронном виде. Доверенное лицо УЦ БУЗОО «МИАЦ» распечатывает на бумажном носителе два экземпляра СКПЭП (приложение № 5 к настоящему Регламенту), которые заверяются собственноручной подписью доверенного лица УЦ и печатью УЦ БУЗОО «МИАЦ». СКПЭП на бумажном носителе заверяется собственноручной подписью его владельца. Один экземпляр оформленных документов выдается владельцу СКПЭП.

Второй экземпляр подшивается доверенным лицом УЦ БУЗОО «МИАЦ» к Реестру действующих СКПЭП, изданных УЦ БУЗОО «МИАЦ», и хранится в течение всего срока действия СКПЭП.

8.4. После ввода полученного в виде ЭД СКПЭП на своем АП в действие и ознакомления с инструкцией абонента УЦ (приложение № 14 к настоящему Регламенту) его владелец может приступать к юридически значимому информационному обмену ЭД.

###### 9. Порядок плановой смены ключей подписи

9.1. Срок действия сертификата ключа проверки ЭП в ЗСПД БУЗОО «МИАЦ» устанавливается в один календарный год. Владельцы сертификатов ключей подписи обязаны производить периодическую (плановую) замену используемых ключей ЭП не реже указанного срока. ПО АП заблаговременно информирует абонента о необходимости проведения данной процедуры.

9.2. Замена ключей ЭП осуществляется в обязательном порядке, если изменился любой из реквизитов, указанных в сертификате ключа ЭП. При этом владелец сертификата обязан известить доверенное лицо УЦ БУЗОО «МИАЦ» о характере изменения реквизитов и согласовать с ним дату и порядок смены ключей ЭП.

9.3. Смена ключей ЭП до истечения срока их действия осуществляется абонентом автоматизировано непосредственно на АП путем формирования новых ключей подписи и отправки электронного запроса на сертификат. Изготовление нового сертификата ключа проверки ЭП при необходимости получения ключевого дистрибутива осуществляется согласно п. 10.8.

9.4. Доверенное лицо УЦ БУЗОО «МИАЦ» должно осуществлять сертификацию ключа ЭП абонента по возможности в день получения электронного запроса, но не позднее дня истечения срока действия действующего СКПЭП. После ввода сертификата ключа проверки ЭП в действие абонент осуществляет информационный обмен с ЭП на новых ключах.

9.5. Если абонент не выполнил смену ключей ЭП до истечения срока действия сертификата, то изготовление нового сертификата ключа проверки ЭП и ключевого дистрибутива осуществляется согласно п. 10.8 настоящего Регламента.

###### 10. Смена ключей в случае их компрометации

10.1. Если возникает сомнение в неизвестности посторонним лицам пароля доступа абонента при старте модуля ViPNet (этот пароль совпадает с паролем доступа к ключам ЭП и шифрования абонента), но доступ к компьютеру этих посторонних лиц был невозможен, абоненту следует сменить пароль и продолжить работу. Если доступ к компьютеру посторонних лиц был возможен, то ключи абонента считаются скомпрометированными.

К событиям компрометации, когда ключи абонента считаются скомпрометированными, также относятся следующие случаи:

* посторонним лицам мог стать доступным файл ключевого дистрибутива абонента;
* посторонним лицам мог стать доступным съемный носитель с ключевой информацией абонента;
* посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере абонента;
* увольнение должностного лица, являющегося владельцем ЭП и зарегистрированного как абонент ЗСПД (в т.ч. его дублера), или сотрудника подразделения автоматизации (информационных технологий, защиты информации) Учреждения, имевшего доступ к паролям и ключам;
* на сейфе с ключевыми документами (резервным набором персональных ключей) нарушена печать;
* в подписи под входящим электронным документом наличествует сертификат, находящийся в списке отозванных сертификатов;
* во входящем документе, полученном по защищенной сети 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 произошел в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения на предмет происшествия компрометации ключевой информации, относится возникновение подозрений в утечке информации при ее передаче посредством защищенной сети.

В случае увольнения абонента, зарегистрированного на одном или нескольких АП, считаются скомпрометированными ключи всех абонентов, зарегистрированных на этом (этих) АП.

В случае увольнения сотрудника подразделения автоматизации (информационных технологий, защиты информации) Учреждения, считаются скомпрометированными ключи всех абонентов данного Учреждения.

В случае увольнения действующего доверенного лица УЦ БУЗОО «МИАЦ» или его действующего дублера, считается скомпрометированной вся ключевая информация в ведомственной информационной системе Учреждения, т.е. ключи всех абонентов во всех Учреждениях.

10.2. В случае наступления любого из событий, связанных с компрометацией ключевой информации, абонент немедленно прекращает связь с другими абонентами и сообщает о факте компрометации (или предполагаемом факте компрометации) доверенному лицу УЦ БУЗОО «МИАЦ».

10.3. Доверенное лицо УЦ БУЗОО «МИАЦ» при получении сообщения о компрометации ключевой информации определяет объем скомпрометированной ключевой информации, в том числе факт компрометации резервного набора персональных ключей, исходя из следующих правил:

* в случае признания факта компрометации любого из секретных ключей, записанных на ключевой дискете (или ином съемном носителе ключевой информации) абонента, признаются непосредственно скомпрометированными все ключи на данной дискете (носителе). Данный абонент признается непосредственно скомпрометированным;
* в случае признания факта непосредственной компрометации любого из ключей у любого абонента коллектива, однозначно признаются скомпрометированными все ключи, общие для абонентов данного коллектива. Абоненты коллектива, не подвергшиеся непосредственной компрометации, признаются косвенно скомпрометированными. У абонентов коллектива, не подвергшихся непосредственной компрометации, не скомпрометированными могут быть признаны только индивидуальные ключи (например, ключ ЭП);
* в случае признания факта компрометации любого из ключей ЭП, записанных на жестком диске, признаются скомпрометированными все ключи данного АП.

10.4. Доверенное лицо УЦ БУЗОО «МИАЦ» при получении сообщения о компрометации ключевой информации в течение одного рабочего дня:

* в ПО ViPNet [Центр управления сетью] объявляет ключи скомпрометированного абонента (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 абонентов и замены ключей АП, где зарегистрированы скомпрометированные абоненты; файлы связей для частичного обновления ключевой информации для всех АП, с которыми связаны АП, где зарегистрированы скомпрометированные абоненты; файлы связей для частичного обновления индивидуальной ключевой информации для абонентов с не скомпрометированными ключами, зарегистрированных в коллективах, где имеются скомпрометированные абоненты;
* оповещает о факте компрометации ключей всех абонентов, связанных со скомпрометированным абонентом. После получения данного сообщения абоненты не должны использовать скомпрометированные ключи;
* формирует средствами УКЦ для генерации ключей при компрометации новую ключевую информацию. Все сформированные файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный АП и скомпрометированному абоненту по любым каналам связи, в том числе и открытым;
* производит рассылку сформированных обновлений ключей на узлы сети VPN № 798, в том числе и скомпрометированному абоненту при наличии у него не скомпрометированного резервного набора персональных ключей, выданного ему при получении ключевого дистрибутива;
* в случае признания факта компрометации ключа подписи абонента, средствами УКЦ отзывает (аннулирует) сертификат этого абонента. Производит рассылку списка отозванных сертификатов всем абонентам сети VPN № 798, а также во все взаимодействующие УЦ.

10.5. Отозванные СКПЭП абонента 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.

10.6. Информация, содержащаяся на скомпрометированных съемных ключевых носителях, после проведения служебного расследования должна быть уничтожена с использованием штатных средств ПО ViPNet с отметкой в Журнале учета выдачи ключевой информации.

10.7. В случае признания факта компрометации резервного набора персональных ключей скомпрометированного абонента, для него средствами УКЦ создается ключевая дискета с новыми ключами.

10.8. Изготовление нового СКПЭП и, при необходимости, ключевого дистрибутива происходит согласно процедурам, указанным в разделе 4, с оформлением для абонентов соответствующих документов на бумажном носителе. Абонент обязан лично прибыть к доверенному лицу УЦ БУЗОО «МИАЦ» для получения нового СКПЭП, ключевого дистрибутива (ключевой дискеты) из рук в руки.

10.9. В случае компрометации ключей действующего доверенного лица УЦ БУЗОО «МИАЦ» или его действующего дублера, считается скомпрометированной вся ключевая информация в ведомственной информационной системе Учреждения, т.е. ключи всех абонентов ЗСПД БУЗОО «МИАЦ». В этом случае должна быть немедленно остановлена работа на симметричных ключах шифрования и оповещены администраторы безопасности (доверенные лица УЦ) взаимодействующих УЦ. Для восстановления работы системы ЭД необходимо:

* удалить с жесткого диска УКЦ все ключи с использованием штатных средств ПО УКЦ;
* начать формирование ключевой системы с нулевой отметки согласно эксплуатационной документации на ПО УКЦ.

До полного развертывания ключевой системы ключевая информация передается абонентам посредством личной встречи с доверенным лицом УЦ, использования доверенных нарочных с документальным подтверждением отправки и приема и т.п.

###### 11. Отзыв (аннулирование) сертификата ключа проверки электронной подписи

11.1. Заявление на аннулирование (отзыв) СКПЭП направляется на бумажном носителе (заверяется рукописной подписью абонента по форме согласно приложению № 11 к настоящему Регламенту) с сопроводительным письмом за подписью руководителя Учреждения.

11.2. Доверенное лицо УЦ БУЗОО «МИАЦ» согласно заявке на отзыв СКПЭП в течение одного рабочего дня отзывает (аннулирует) СКПЭП.

11.3. Отозванные СКПЭП абонента 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.

11.4. Все отозванные СКПЭП учитываются в Реестре сертификатов ключей проверки электронной подписи (действующих, отозванных), изданных УЦ БУЗОО «МИАЦ» (приложение № 4 к настоящему Регламенту). Реестр ведется доверенным лицом УЦ БУЗОО «МИАЦ». Отозванные СКПЭП на бумажных носителях извлекаются из подшивки действующих СКПЭП, о чем делается соответствующая отметка в Реестре СКПЭП, после чего подшиваются к отозванным СКПЭП на бумажных носителях, и хранятся в течение всего срока функционирования УЦ БУЗОО «МИАЦ».

###### 12. Порядок разбора конфликтных ситуаций

12.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения абонентами Учреждения и/или внешней организации ЭД, а также использованием в данных документах ЭП.

12.2. Разбор конфликтных ситуаций осуществляется в два этапа. Сначала, путем взаимодействия абонента стороны, у которой возникли претензии, с доверенным лицом УЦ БУЗОО «МИАЦ». В случае если абонент не удовлетворен полученной информацией, для разрешения конфликтной ситуации проводится техническая экспертиза в соответствии с Порядком разрешения конфликтных ситуаций (приложение № 6 к настоящему Регламенту).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_».