


Приложение №1 к Приказу № 32
от «22» ноября 2018 г.

УТВЕРЖДЕНО

Директор КУ НАО «НИАЦ»

 П.А. Окладников
«22» ноября 2018 г.

РЕГЛАМЕНТ РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
КАЗЕННОГО УЧРЕЖДЕНИЯ НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА
«НЕНЕЦКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»
НА БАЗЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА (ПАК) «VIPNET»

Нарьян-Мар

2018

1. Термины и определения

Абонентский пункт (АП) – АРМ, на котором установлен либо ViPNet «Координатор» либо ViPNet «Клиент».

Администратор УЦ – ответственный сотрудник КУ НАО НИАЦ, наделенный полномочиями по осуществлению действий по регистрации и управлению пользователями УЦ.

Адресные справочники – набор файлов, содержащих информацию об объектах сети ViPNet.

Защищенная сеть КУ НАО НИАЦ – это совокупность сетевых узлов (абонентских пунктов и координаторов), управляемая КУ НАО НИАЦ и защищаемая с помощью продуктов линейки ViPNet. Сеть №2440.

ИОГВ НАО – исполнительные органы государственной власти Ненецкого автономного округа.

КУ НАО НИАЦ – казенное учреждение Ненецкого автономного округа «Ненецкий информационно-аналитический центр».

Ключевая и справочная информация – закрытый ключ и сертификат открытого ключа, ключи защиты ключей обмена, ключи обмена, справочник сертификатов администраторов своей и доверенных сетей, списки отозванных сертификатов (СОС) своей и доверенной сетей шифруется на действующем персональном ключе пользователя. Персональный ключ шифруется на парольном ключе. Вся сформированная справочная и ключевая информация передается в файле-дистрибутиве.

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Кросс-сертификация — комплекс организационно-технических мероприятий, предпринимаемых удостоверяющими центрами для установления взаимных доверенных отношений. Кросс-сертификация между удостоверяющими центрами обеспечивает прозрачное взаимодействие между пользователями этих УЦ.

Кросс-сертификат — сертификат, владельцем которого является Уполномоченное лицо одного удостоверяющего центра, а издателем – Уполномоченное лицо другого удостоверяющего центра.

ПАК – программно-аппаратный комплекс

Парольная фраза – набор грамматически согласованных между собой слов, выбираемых случайным образом из специальных словарей

Первичная ключевая информация – Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей и к которым доступ имеет только данный пользователь.

Ключи пользователя могут содержать:

– действующий персональный ключ пользователя

- случайный ключ защиты пользователя
- закрытый ключ и соответствующий ему сертификат открытого ключа подписи пользователя
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

ПО – программное обеспечение.

Пользователь УЦ – Лицо, которому Удостоверяющим центром была выдана ключевая информация.

РФ – Российская Федерация

Сертификат (сертификат ключа подписи) – электронный документ, который содержит открытый ключ подписи субъекта и подписан электронной подписью его издателя, сведения о владельце открытого ключа подписи.

Список аннулированных сертификатов (CRL) – Созданный УЦ список сертификатов, аннулированных до окончания срока действия.

Таблица маршрутизации – таблица, согласно которой происходит процесс выбора пути для передачи данных.

УЦ – удостоверяющий центр.

УКЦ – удостоверяющий и ключевой центр.

ФАПСИ – Федеральное агентство правительственной связи и информации

ФЗ – Федеральный закон

ФСБ – Федеральная служба безопасности

2. Общие положения

Настоящий регламент определяет механизмы и условия предоставления и использования услуг Удостоверяющего центра КУ НАО «НИАЦ», включая обязанности пользователей УЦ и администраторов УЦ, протоколы работы, процедуры взаимодействия сторон, принятые форматы документов и данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ.

Регламент разработан в соответствии с ФЗ от 06.04.2011 № 63 «Об электронной подписи», ФЗ от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации», Приказом ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», Приказом ФАПСИ от 13.06.2001 года № 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».

Удостоверяющий центр предназначен для обработки информации, не содержащей сведений составляющих государственную тайну.

Удостоверяющий Центр защищенной сети КУ НАО «НИАЦ» осуществляет свою деятельность на безвозмездной основе.

При возникновении вопросов, не урегулированных положениями Регламента, следует руководствоваться законодательством Российской Федерации.

Внесение изменений (дополнений) в регламент, включая приложения к нему, производится в УЦ в одностороннем порядке. Уведомление третьих лиц о внесении изменений (дополнений) в регламент осуществляется путем обязательного размещения очередной редакции настоящего регламента на сайте НИАЦ : <http://niac.adm-nao.ru/pages/about> .

Настоящий Регламент вступает в силу со дня утверждения приказом КУ НАО «НИАЦ». Действие Регламента отменяется приказом КУ НАО «НИАЦ».

3. Порядок присоединения к Регламенту

Деятельность УЦ направлена на организацию защищенной сети исполнительных органов государственной власти Ненецкого автономного округа. При необходимости устанавливается межсетевое взаимодействие с защищёнными сетями учреждений и организаций, с которыми взаимодействует КУ НАО «НИАЦ» или абоненты защищенной сети (ИОГВ НАО). Присоединение к настоящему регламенту (принятие его условий) организациями (за исключением ИОГВ НАО) осуществляется путем заключения соглашения о присоединении к Регламенту по форме, установленной Приложением №1 к настоящему Регламенту.

С момента заключения соглашения к настоящему Регламенту, Сторона соглашается с требованиями регламента и приложениями к нему и обязуется соблюдать все их положения (статья 428 Гражданского кодекса Российской Федерации). Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

Удостоверяющий центр КУ НАО «НИАЦ» вправе отказать любому лицу в приеме и регистрации Соглашения о присоединении к Регламенту с указанием причин отказа.

После присоединения в установленном порядке к Регламенту, Стороны вступают в соответствующие договорные отношения на неопределенный срок. Сторона, присоединившаяся к Регламенту, имеет право в одностороннем порядке прекратить отношения по присоединению к настоящему Регламенту, письменно уведомив об этом Удостоверяющий центр за один месяц до дня прекращения присоединения. Уведомление о прекращении отношений по присоединению к Регламенту, полученное Удостоверяющим центром, является основанием для обязательного аннулирования всех сертификатов данного пользователя УЦ. Датой аннулирования указанных сертификатов будет дата прекращения отношений по присоединению. При этом Стороны до дня прекращения отношений по присоединению к Регламенту обязаны разрешить между собой все вопросы, связанные с требованиями Регламента.

4. Публикация Регламента

С текстом Регламента можно ознакомиться одним из следующих способов:

- 1) в электронной форме на сайте КУ НАО «НИАЦ» по адресу: <http://niac.adm-nao.ru/pages/about>
- 2) сделав запрос на получение копии Регламента по электронной почте на адрес электронной почты niac@adm-nao.ru
- 3) в бумажной форме по адресу 166000, Ненецкий АО, г.Нарьян-Мар, ул.Ленина, д.27В, оф.59

5. Структура УЦ КУ НАО «НИАЦ»:

Структурно УЦ представляет программно-аппаратный комплекс с установленным ПО ViPNet и штатных специалистов, обслуживающих этот ПАК.

Программный комплекс обеспечения реализации целевых функций УЦ включает в себя следующие программные компоненты:

- ViPNet «Администратор»;
- ViPNet «Центр управления сетью»;
- ViPNet «Удостоверяющий и Ключевой центр»;
- ViPNet «Пункт регистрации».

В соответствии со статьей 16 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УЦ использует средства, получившие подтверждение соответствия требованиям приказа ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

Программный комплекс «ViPNet Удостоверяющий центр 4» (ПК «ViPNet УЦ 4»), производитель: ОАО «ИнфоТеКС», г. Москва.

Сопровождение программно-аппаратного комплекса осуществляется отделом по защите информации КУ НАО «НИАЦ», для чего приказом назначаются Администраторы УЦ с указанием их прав и обязанностей в должностных инструкциях.

Удостоверяющий центр предназначен для выполнения следующих основных функций:

- Формирование и хранение первичной ключевой информации;
- Формирование и обновление справочно-ключевой информации для организации защищенного обмена информации в рамках защищенной сети КУ НАО «НИАЦ»;
- Выработка персональных ключей защиты пользователей и криптографически надежных парольных фраз;
- Запись персональных ключей пользователей на внешние устройства – аппаратные носители ключей;
- Установление сроков действия сертификатов;
- Хранение конфиденциальной информации в форме, позволяющей проверить ее целостность и достоверность в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации;
- Выполнение операций по отзыву, приостановлению и возобновлению сертификатов, рассылка списков аннулированных сертификатов;
- осуществление иных функций, необходимых для осуществления деятельности, связанной с организацией защищенной сети КУ НАО «НИАЦ».

6. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ

Способ создания и передачи ключевого дистрибутива

Администратор УЦ, в соответствии подписанным соглашением о присоединении к Регламенту, на своем специализированном рабочем месте УЦ регистрирует новый абонентский пункт, формирует адресные справочники, таблицы маршрутизации, справочники для УКЦ, создаёт справочно-ключевую информацию.

Ключевой дистрибутив вместе с паролем доступа к нему, резервным набором персональных ключей передается одним из способов:

- лично абоненту

- доверенному лицу по доверенности (Приложение №2) под роспись в журнале учёта выдачи дистрибутивов ключей (Приложение №3)
- по защищенным каналам связи в соответствии с инструкциями разработчика СКЗИ с регистрацией в журнале. В этом случае в журнале учета выдачи ключевых дистрибутивов УЦ (приложение №3) ставится подпись сотрудника УЦ, производившего передачу.

При создании ключевой информации администратор УЦ должен выполнять требования по обеспечению безопасности информации, соответствующие законодательству Российской Федерации по технической защите конфиденциальной информации.

Регистрацию абонентских пунктов и установку ключевых дистрибутивов для исполнительных органов государственной власти выполняют сотрудники УЦ в соответствии со своими должностными инструкциями.

Установка ПО ViPNet на абонентские пункты организациям отличным от ИОГВ НАО производится с использованием выданных ключевых дистрибутивов пользователем Удостоверяющего центра защищенной сети самостоятельно.

Аннулирование сертификата

Заявление на аннулирование сертификата в письменной форме подается пользователем в УЦ лично.

Заявление на аннулирование сертификата в письменной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью пользователя.

Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные пользователя;
- серийный номер отзываемого сертификата;
- причину отзыва сертификата;
- дата и подпись пользователя.

Срок рассмотрения заявления на аннулирование сертификата составляет один рабочий день с момента его поступления в УЦ.

УЦ может по собственной инициативе аннулировать сертификат пользователя УЦ в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата указанием обоснованных причин отзыва.

Администратор УЦ формирует запрос на отзыв сертификата, подписывает его и отправляет в ViPNet УКЦ, где запрос обрабатывается и сертификат попадет в список аннулированных сертификатов Администратора УЦ (издателя сертификата) и будет иметь статус Отозван. Данный CRL поступает в программу ViPNet Registration Point вместе с ответом на запрос об отзыве сертификата. С момента получения остальными пользователями обновленного CRL аннулированный сертификат станет недействительным.

7. Взаимодействие с удостоверяющими центрами внешних организаций

Для организации обмена информацией по защищенным каналам связи между пользователями защищённой сети КУ НАО НИАЦ и внешними организациями производится установление доверительных отношений с внешними удостоверяющими центрами, обслуживающими эти организации.

Установление доверительных отношений между УЦ КУ НАО «НИАЦ» и иными удостоверяющими центрами осуществляется либо напрямую, на основе Соглашений с внешними Удостоверяющими центрами и Регламентом (Временным Регламентом) взаимодействия (установления доверительных отношений) УЦ КУ НАО «НИАЦ» с Удостоверяющим центром внешней организации, либо косвенным образом путем получения кросс-сертификатов.

Технологическое взаимодействие по установлению доверительных отношений между УЦ КУ НАО «НИАЦ» и иными удостоверяющими центрами осуществляется в соответствии с технической документацией на УКЦ VipNet и ПАК, используемый иными Удостоверяющими центрами.

Удостоверяющий центр осуществляет регистрацию абонентских пунктов и абонентов защищенной сети в качестве узлов и абонентов сети VipNet №2440, только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с разделом Настоящего Регламента.

8. Политика конфиденциальности

Ключевая и парольная информация является конфиденциальной информацией.

Информация, хранящаяся в журналах аудита УЦ, считается конфиденциальной и не подлежит разглашению.

Информация, не являющаяся конфиденциальной, является открытой информацией. К открытой информации относятся списки отозванных сертификатов, издаваемые УЦ, данный Регламент.

Открытая информация может публиковаться по решению УЦ.

Обработка персональных данных не осуществляется ввиду того что ключевая информация генерируется не для субъектов персональных данных, а для объектов (организаций) на которых она используется в программном или программно-аппаратном комплексе для установления защищенного канала связи.

9. Ответственность

Удостоверяющий центр не несет никакой ответственности в случае нарушения пользователями УЦ положений настоящего Регламента. Претензии к Удостоверяющему центру ограничиваются указанием на несоответствие его действий настоящему Регламенту.

Соглашение о присоединении к Регламенту Удостоверяющего центра защищенной
сети КУ НАО «НИАЦ»

_____ (наименование организации, включая организационно-правовую форму)

в лице _____

_____ (должность)

_____ (Фамилия, имя, отчество)

действующего на основании _____

в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра защищенной сети КУ НАО «НИАЦ», условия которого определены КУ НАО «НИАЦ» и опубликованы на сайте Удостоверяющего центра защищенной сети КУ НАО «НИАЦ» по адресу: <http://niac.adm-nao.ru/pages/about>

с Регламентом Удостоверяющего центра защищенной сети КУ НАО «НИАЦ» и приложениями к нему ознакомлен (-а) и обязуюсь соблюдать все положения указанного документа.

Руководитель организации _____

_____ (подпись)

_____ (Фамилия, инициалы)

«__» _____ 20__ г.

Печать организации

_____ (заполняется сотрудником Удостоверяющего центра)

Данное Соглашение о присоединении к Регламенту зарегистрировано в реестре Удостоверяющего центра защищенной сети КУ НАО «НИАЦ».

Регистрационный номер № _____ от «__» _____ 20__ г.

Уполномоченный сотрудник

Удостоверяющего центра

защищенной сети КУ НАО «НИАЦ» _____

_____ (подпись)

_____ (Ф.И.О.)

Доверенность

г. _____

« ____ » _____ 20__ г

(наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

(Фамилия, имя, отчество)

действующего на основании _____

уполномочивает представителя _____
(Фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

Получить дистрибутив справочно-ключевой информации в УЦ и выполнить все необходимые действия, связанные с исполнением настоящего поручения, в т.ч. с правом подписи в журнале поэкземплярного учёта СКЗИ и прочих учётных документах.

Настоящая доверенность выдана сроком на 1 (один) месяц без права передоверия.

Руководитель организации _____
(подпись)

М.П.

(Фамилия, инициалы)

Журнал учета выдачи ключевых дистрибутивов

№ п/п	Дата выдачи	Организация	Идентификатор дистрибутива	Тип носителя	Способ передачи (лично, по доверенности, по защищенным каналам связи...)	Подпись получившего

Пройито, продумеровано

и скреплено печатью

листа (08)

