АКЦИОНЕРНОЕ ОБЩЕСТВО
НАУЧНО-ИНЖЕНЕРНОЕ ПРЕДПРИЯТИЕ «ИНФОРМЗАЩИТА»
наименование организации-разработчика

РУКОВОДСТВО АДМИНИСТРАТОРА ЦЕНРТА СЕРТИФИКАЦИИ

наименование документа

RU.40308570.501430.010.И5.02

На 17 листах

2022 г.

Аннотация

Настоящий документ содержит инструкцию по работе администратора центра сертификации программно-аппаратного комплекса «Юнисерт-ГОСТ. Версия 4.0» (далее – ПАК «Юнисерт-ГОСТ»).

Содержание

Перечень сокращений

Сокращение	Полное наименование
CRL	Certificate revocation list (Список сертификатов, досрочно прекративших действие, сформированный в соответствии со стандартом RFC5280)
АРМ	Автоматизированное рабочее место
ГОСТ	Государственный стандарт
ГУЦ	Головной удостоверяющий центр
ИИ	Интерфейс интеграции
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СКП ЭП, Сертификат	Сертификат ключа проверки электронной подписи
УЗ	Учетная запись
УЦ	Удостоверяющий центр
ЦР	Центр регистрации
ЦС	Центр сертификации
ЭП	Электронная подпись

Перечень терминов

Наименование термина	Определение
Головной удостоверяющий центр	Удостоверяющий центр Министерства связи и массовых коммуникаций, осуществляющий создание и контроль актуальности сертификатов электронной подписи аккредитованных удостоверяющих центров
Запрос на сертификат	Файл, созданный с использованием средств электронной подписи, содержащий ключ проверки электронной подписи и иную информацию о Владельце сертификата
Заявитель	лицо, обратившееся за получением сертификата, фамилия, имя, отчество (если имеется) которого указаны в Запросе на сертификат
Квалифицированный сертификат ключа проверки электронной подписи	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи
Ключ электронной подписи	Уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию
Ключевой носитель	Физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт - диск, Data Key, Smart Card, Touch Memory,

Наименование термина	Определение
	Token и т.п.)
Система	Программно-аппаратный комплекс «Юнисерт-ГОСТ. Версия 4.0»
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. В настоящем Регламенте под сертификатом понимается являющийся квалифицированным сертификат ключа проверки электронной подписи, выданный в соответствии с Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
Список сертификатов, досрочно прекративших действие	Электронный документ с электронной подписью УЦ, включающий в себя список серийных номеров сертификатов, изготовленных данным УЦ, действие которых на указанный в данном документе момент времени было досрочно прекращено
Средства электронной подписи	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи
Удостоверяющий центр	Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом
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

1 Общие положения

1.1 Общая информация

Назначением ПАК «Юнисерт-ГОСТ 4.0» является реализация функций средств УЦ:

- создание по обращениям заявителей ключей ЭП и ключей проверки ЭП (с использованием запросов на издание сертификатов);
- создание сертификатов и выдача таких сертификатов лицам, обратившимся за их получением (заявителям);
- аннулирование выданных сертификатов;
- ведение реестра выданных и аннулированных сертификатов.

ПАК «Юнисерт-ГОСТ» может использоваться для выпуска квалифицированных сертификатов, соответствующих требованиям Приказа ФСБ России от 27.12.2011 № 795 (ред. от 29.01.2021) «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», которые могут использоваться для формирования квалифицированной ЭП в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Основное направление деятельности администратора ЦС – управление ключами УЦ, используемыми для подписи выпускаемых сертификатов и CRL, а именно:

- первичное создание;
- плановая смена;
- вывод из эксплуатации.

Ключи УЦ создаются, хранятся и используются в ПАК ViPNet PKI Service. Программная служба ЦС для доступа к ключу УЦ обращается к ПАК ViPNet PKI Service через API под учётной записью пользователя сервера подписи.

Управление учётными записями пользователей сервера подписи выполняет администратор ЦС.

Администратор ЦС не имеет доступа к web-интерфейсу ЦР ПАК «Юнисерт-ГОСТ».

1.2 Описание функций администратора ЦС

На администратора ЦС возлагаются следующие функциональные обязанности:

– уполномоченное лицо по выпуску сертификатов (делегирует ответственность автоматическим сервисам ПАК «Юнисерт-ГОСТ»);
– создание ключа ЭП и соответствующего ему файла запроса на сертификат (PKCS#10), используемого для подписи квалифицированных сертификатов и соответствующих CRL;
– обращение в ГУЦ для получения сертификата, используемого для подписи изготовляемых сертификатов и соответствующих CRL;
– импорт полученного в ГУЦ сертификата, используемого для подписи квалифицированных сертификатов и соответствующих CRL, в хранилище СКЗИ ViPNet PKI Service;
– контроль срока действия ключей ЭП УЦ;
– изменение режима использования ключей ЭП УЦ и вывод их из эксплуатации по истечению срока действия с выпуском финального CRL;
– управление учётной записью пользователя сервера подписи, используемой программным компонентом ЦС для обращения к сервису СКЗИ «ViPNet PKI Service» для выполнения криптографических операций с использованием ключа ЭП и соответсвующего ему сертифката УЦ.

1.3 Уровень подготовки персонала

В рамках подготовки персонала к выполнению своих должностных обязанностей сотрудники, назначенные на роль администратора ЦС, должны ознакомиться со следующей нормативной и эксплуатационной документацией:

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
– Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
– Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
– Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);
– Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и

передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- эксплуатационная документация ПАК «Юнисерт-ГОСТ 4.0»;
- Руководство администратора СКЗИ ViPNet CSP для Linux;
- Руководство администратора СКЗИ ViPNet PKI Client для Linux;
- Руководство администратора ПАК ViPNet PKI Service;
- Руководство разработчика ПАК ViPNet PKI Service;
- Руководство пользователя АПМДЗ;
- Руководство пользователя Astra Linux Special Edition.

2 Подготовка к работе

Для выполнения функциональных обязанностей администратор ЦС должен получить доверенным способом у системного администратора учётные записи на технических средствах, входящих в состав ПАК «Юнисерт-ГОСТ», а именно:

– идентификатор с ключом, обладающий правами Администратора прикладного сервиса в СКЗИ ViPNet PKI Service, который используется в составе ПАК «Юнисерт-ГОСТ» (подробнее об СКЗИ ViPNet PKI Service см. п. 1.5.4 «ViPNet PKI Service» Описания применения ПАК «Юнисерт-ГОСТ» RU.40308570.501430.010.ПФ);
– логин/пароль учётной записи в ОС АРМ, используемого для администрирования СКЗИ ViPNet PKI Service в соответствии с требованиями эксплуатационной документации СКЗИ ViPNet PKI Service (терминала администрирования СКЗИ ViPNet PKI Service);
– логин/пароль учётной записи в ОС сервера с установленным программным компонентом ЦС (подробнее о программном компоненте ЦС см. п. 1.7 «ПО ПАК «Юнисерт-ГОСТ» Описания применения ПАК «Юнисерт-ГОСТ» RU.40308570.501430.010.ПФ).

Администратор ЦС должен сменить пароли всех полученных учётных записей при первом использовании. При работе с парольной информацией администратор ЦС должен руководствоваться требованиями п. 2.3.4 «Парольная политика» Описания применения ПАК «Юнисерт-ГОСТ» RU.40308570.501430.010.ПФ.

Доступ к паролю должен быть обеспечен только администратору ЦС, владельцу соответствующей паролю учётной записи.

3 Описание операций

3.1 Управление пользователем сервера подписи

В рамках инициализации ПАК «Юнисерт-ГОСТ» администратор ЦС должен создать пользователей сервера подписи, чтобы программные службы ЦС смогли подключиться к СКЗИ ViPNet PKI Service.

После получения идентификатора учётной записи с правами администратора прикладного сервиса администратор ЦС должен через веб-интерфейс администрирования СКЗИ ViPNet PKI Service создать учётную запись с правами пользователя сервера подписи для службы программного компонента ЦС.

При работе с ViPNet PKI Service администратор ЦС должен соблюдать требования эксплуатационной документации СКЗИ.

При работе с парольной информацией учётных записей Администратора прикладного сервиса и Пользователя сервера подписи администратор ЦС должен руководствоваться требованиями п. 2.3.4 «Парольная политика» Описания применения ПАК «Юнисерт-ГОСТ» RU.40308570.501430.010.ПФ.

3.2 Работа с сертификатами УЦ

3.2.1 Первичное создание

После создания пользователей сервиса подписи в процессе инициализации ПАК «Юнисерт-ГОСТ» администратор ЦС должен создать ключевую пару и получить сертификат в ГУЦ, используемые для подписи квалифицированных сертификатов и CRL, выпускаемых ПАК «Юнисерт-ГОСТ».

Для первичного создания сертификата УЦ администратор ЦС должен выполнить следующие действия:

– подключиться локально к интерфейсу командной строки сервера ЦС под своей учётной записью и перейти в каталог приложения консоли управления ЦС:

```
cd /usr/unicert/uc-cs-console
```

– установить адрес сервера подписи СКЗИ «ViPNet PKI Service» через приложение консоли ЦС:

```
dotnet uc-cs-console.dll --setParameter –n “HSMApiUrl” –v “http://<ip-адрес>:9000/api”
```

– установить логин и пароль пользователя сервера подписи, созданного в СКЗИ «ViPNet PKI Service» (см. п. 3.1 настоящего Руководства) следующими командами:

```
dotnet uc-cs-console.dll --setParameter –n “HSMLogin” –v “логинПользователя”
dotnet uc-cs-console.dll --setParameter –n “HSMPassword” –v “парольПользователя”
```

– сформировать файл запроса pkcs#10 на основании JSON или TBS файла:

```
dotnet uc-cs-console.dll –createRootCertRequest -rp <JSONФайлПараметров>  -rf <путьФайлаЗапроса>
```

или

```
dotnet uc-cs-console.dll –createRootCertRequest -tbs <TBSФайлПараметров>  -rf <путьФайлаЗапроса>
```

где:

-rp <JSONФайлПараметров> - JSON-файл с параметрами запроса[1];

-tbs <TBSФайлПараметров> - TBS-файл с параметрами запроса[2];

-rf <путьФайлаЗапроса> - путь к файлу для сохранения pkcs#10 файла запроса;

Описание JSON файла приведено в Руководстве разработчика ViPNet PKI Service ФРКЕ.00184-01 33 01

– выгрузить из файловой системы сервера ЦС на съемный носитель информации изготовленный файл запроса pkcs#10;

– передать изготовленный файл запроса pkcs#10 в ГУЦ и получить подчиненный сертификат на основании сформированного файла запроса в порядке, предусмотренном Регламентом ГУЦ;

– загрузить в файловую систему сервера ЦС со съемного носителя

[1] Данные, используемые для заполнения полей JSON файла, должны позволить выпустить сертификат, соответствующий требованиям к квалифицированному сертификату юридического лица, содержащимся в Приказе ФСБ России №795 от 27.12.2011 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»

[2] Данные, используемые для заполнения полей TBS файла, должны позволить выпустить сертификат, соответствующий требованиям к квалифицированному сертификату юридического лица, содержащимся в Приказе ФСБ России №795 от 27.12.2011 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»

информации изготовленный сертификат;

– установить сертификат через приложение консоли управления ЦС:

```
dotnet uc-cs-console.dll –installRootCertificate -rc <файлСертификата>
```

– подключиться локально к интерфейсу командной строки сервера ЦР под своей учётной записью;

– загрузить в файловую систему сервера ЦР со съемного носителя информации изготовленный сертификат;

– перейти в каталог приложения консоли ЦР:

```
cd /usr/unicert/uc-rs-console
```

– установить сертификат через приложение консоли сервера ЦР:

```
dotnet uc-rs-console.dll --setParameter –n “RootCertificate” -c-f <файлСертификата>
```

3.2.2 Плановая смена

Срок действия ключей ЭП УЦ – не более 3 (трёх) лет, при этом для подписи создаваемых сертификатов ключи УЦ должны использоваться не более 1 (одного) года и 3 (трёх) месяцев.

Администратор ЦС должен следить за длительностью использования ключей ЭП УЦ. За месяц до окончания срока действия ключа ЭП сертификата УЦ администратор ЦС должен начать процедуру плановой смены сертификата УЦ.

Для плановой смены сертификата УЦ администратор ЦС должен выполнить следующие действия:

– повторить действия, описанные в 3.2.1 настоящего Руководства;

– подключиться локально к интерфейсу командной строки сервера ЦС под своей учётной записью и перейти в каталог приложения консоли ЦС:

```
cd /usr/unicert/uc-cs-console
```

– с помощью приложения консоли ЦС перевести новый сертификат УЦ в режим «Используется»:

```
dotnet uc-cs-console.dll –setRootCertificateMode -ski <ИдентификаторКлючаКорневогоСертификата>
-m <режимИспользованияКорневогоСертификата>
```

Режим использования корневого сертификата:

1 – Используется,

2 – Выведен из эксплуатации,

3 – Выпуск CRL.

После выше указанных действия, ключ УЦ и соответствующий ему сертификат УЦ, который ранее использовался для подписи создаваемых сертификатов и CRL в конфигурации ЦС перейдет в режим «Выпуск CRL», т.е. ЦС его сможет использовать только для подписи CRL, в который помещаются досрочно прекратившие действие сертификаты, подписанные с использованием ключа УЦ, который переведен в режим «Выпуск CRL». При этом сертификаты, подписанные новым ключом УЦ, при досрочном прекращении действия попадают в CRL, подписываемый новым ключом УЦ.

3.2.3 Вывод из эксплуатации

В период после 2 (двух) лет и 6 (шести) месяцев и до 3 (трёх) лет ключ УЦ, используемый в режиме «Выпуск CRL» должен быть выведен из эксплуатации. Для этого администратор ЦС должен:

– подключиться локально к интерфейсу командной строки сервера ЦС под своей учётной записью и перейти в каталог приложения консоли ЦС:

```
cd /usr/unicert/uc-cs-console
```

– с помощью приложения консоли ЦС перевести все сертификаты УЦ в режим «Выведен из эксплуатации», кроме того сертификата, который требуется вывести из эксплуатации:

```
dotnet uc-cs-console.dll –setRootCertificateMode -ski <ИдентификаторКлючаКорневогоСертификата>
-m <режимИспользованияКорневогоСертификата>
```

Режим использования корневого сертификата:

1 – Используется,

2 – Выведен из эксплуатации,

3 – Выпуск CRL.

– изменить срок действия финального CRL в задаче выпуска CRL на срок больше срока действия сертификата УЦ, который планируется вывести из эксплуатации (система автоматически ограничит срок действия, выпускаемого CRL сроком действия сертификата УЦ);

```
dotnet uc-cs-console.dll --setParameter -n "FullCrlExpirationPeriod" -v  < Длительность (в сек)>
```

– инициировать внеплановый выпуск CRL, выполнив команду:

```
dotnet uc-cs-console.dll --crlRelease -out <Путь к файлу в файловой системе сервера ЦС>
```

– вернуть срок действия финального CRL в задаче выпуска CRL на значение срока действия CRL в соответствии с принятым регламентом УЦ;

```
dotnet uc-cs-console.dll --setParameter -n "FullCrlExpirationPeriod" -v  <Длительность (в сек)>
```

– перевести сертификат УЦ, который требуется вывести из эксплуатации в режим «Выведен из эксплуатации», для других сертификатов УЦ вернуть режим использования, который был установлен до выпуска финального CRL:

```
dotnet uc-cs-console.dll –setRootCertificateMode -ski <ИдентификаторКлючаКорневогоСертификата>
-m <режимИспользованияКорневогоСертификата>
```

Режим использования корневого сертификата:

1 – Используется,

2 – Выведен из эксплуатации,

3 – Выпуск CRL.

– выгрузить на съемный носитель информации финальный CRL с файловой системы сервера ЦС и передать его системному администратору для его публикации на сервере точки распространения CRL.

4 Администратору ЦС запрещается

Администратору ЦС запрещено:

- использовать интерфейс консоли аудита ЦС;
- подключаться к серверу с консолью управления ЦС удаленно;
- разглашать аутентифицирующую информацию;
- в параметре «sing_type» запроса на генерацию ключевой пары и pkcs#10 запроса сертификата УЦ указывать значение, обозначающее использование устаревшего алгоритма ЭП ГОСТ Р 34.10-2001 (см. 3.2 настоящего Руководства).
- совмещать роль администратора ЦС с другими ролями персонала УЦ;
- использование ключа ЭП УЦ для подписи выпускаемых сертификатов дольше 1 года и 3 месяцев.
- использование ключа ЭП УЦ для подписи выпускаемых CRL дольше 3 лет.
- менять режимы использования ключа УЦ консоли ЦС кроме случаев, указанных в п. 3.2 настоящего Руководства, в частности:
    - ключ, переведенный из режима «используется» в режим «Выпуск CRL», запрещено переводить обратно в режим «Используется».
    - ключ, переведенный из режима «Выпуск CRL» в режим «Выведен из эксплуатации», запрещено переводить обратно в режим «Выпуск CRL» или в режим «Используется».

Лист регистрации изменений

№ версии док-та	Дата изменения	Изменения
1.0	05.09.2022	Начальная версия документа