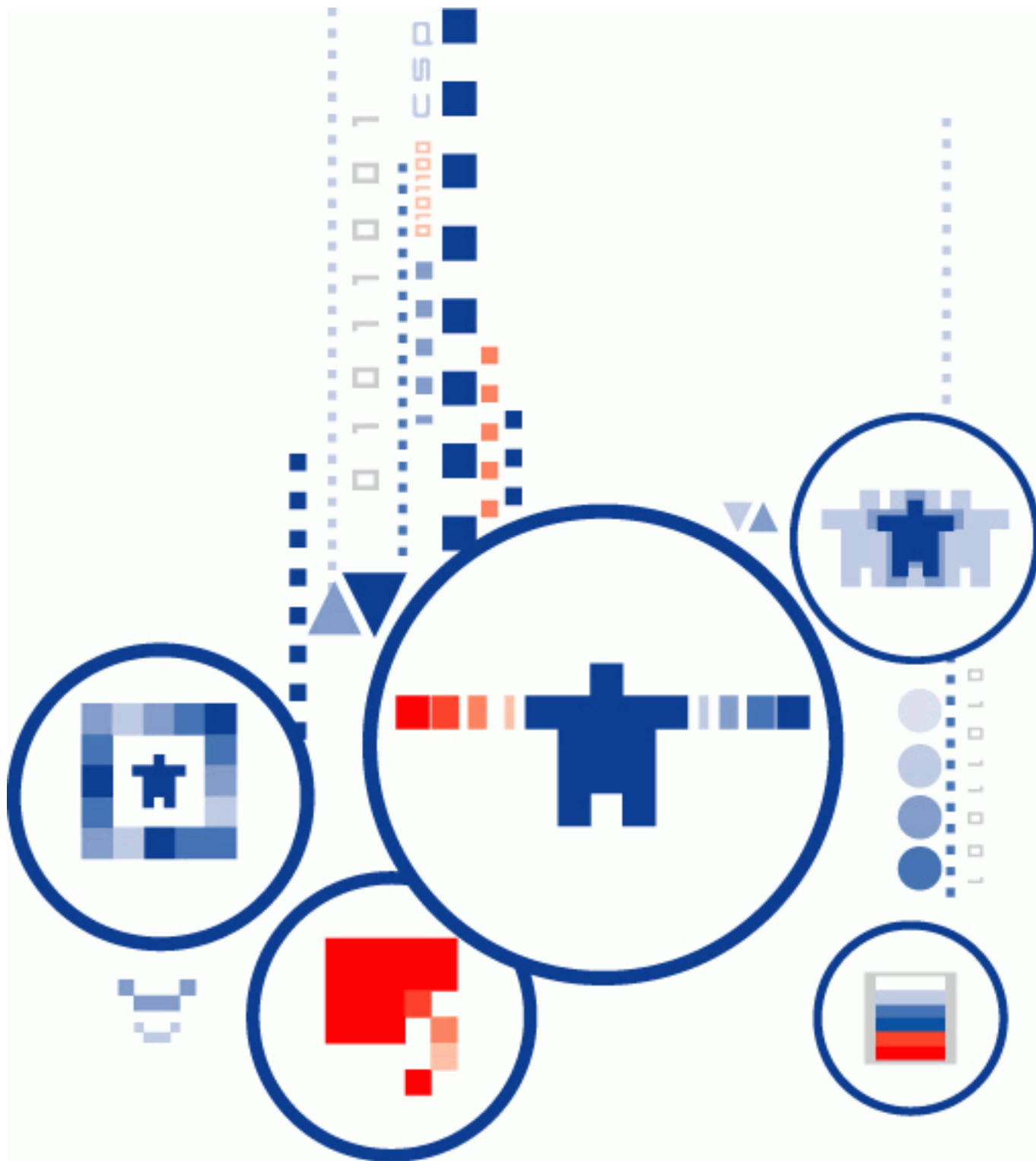




# Службы УЦ

## КриптоПро OCSP Server

Версия 2.0

Руководство администратора

## АННОТАЦИЯ

Настоящий документ содержит описание процесса установки и конфигурации программного комплекса «КриптоПро OSCP Server» (ПК «КриптоПро OSCP Server»), предназначенного для распространения информации о статусах сертификатов по протоколу OSCP.

Документ предназначен для администраторов как руководство по установке и конфигурации ПК «КриптоПро OSCP Server».

### **Информация о разработчике ПК «КриптоПро OSCP Server»:**

ООО «КРИПТО-ПРО»

127018, г. Москва, ул. Суцевский вал, д. 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

<https://www.cryptopro.ru>

E-mail: info@cryptopro.ru

# СОДЕРЖАНИЕ

|                                                                                                                                      |           |
|--------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Требования к аппаратному и программному обеспечению .....</b>                                                                  | <b>4</b>  |
| <b>2. Установка КриптоПро OSCP Server .....</b>                                                                                      | <b>5</b>  |
| 2.1. Особенности установки КриптоПро OSCP Server под управлением ОС Linux .....                                                      | 5         |
| 2.2. Установка КриптоПро OSCP Client .....                                                                                           | 5         |
| <b>3. Конфигурационные файлы КриптоПро OSCP Server .....</b>                                                                         | <b>7</b>  |
| <b>4. Запуск и проверка работоспособности Службы .....</b>                                                                           | <b>10</b> |
| 4.1. Управление операторами Службы .....                                                                                             | 10        |
| 4.2. Настройка Службы .....                                                                                                          | 11        |
| 4.3. Автоматический запуск Службы .....                                                                                              | 22        |
| 4.4. Развертывание веб-сервера .....                                                                                                 | 23        |
| <b>5. Перечень сокращений .....</b>                                                                                                  | <b>25</b> |
| <b>6. Перечень ссылочных документов .....</b>                                                                                        | <b>26</b> |
| <b>Приложение А. Заполнение полей thisUpdate и nextUpdate службой<br/>    актуальных статусов при различных режимах работы .....</b> | <b>27</b> |
| <b>Приложение В. Пример командного файла, обновляющего файлы СОС .....</b>                                                           | <b>28</b> |

## 1. Требования к аппаратному и программному обеспечению

Для ПАК «Службы УЦ 2.0» варианта исполнения 7 должно быть установлено СКЗИ «КриптоПро CSP» версии 5.0 R2 KC2 варианта исполнения 2-Base и/или ПАКМ «КриптоПро HSM» версии 2.0.

Для ПАК «Службы УЦ 2.0» варианта исполнения 8 должно быть установлено СКЗИ «КриптоПро CSP» версии 5.0 R2 KC3 варианта исполнения 3-Base и/или ПАКМ «КриптоПро HSM» версии 2.0.

Использование ПК «КриптоПро OSCP Server» должно осуществляться только совместно с ПАК «Удостоверяющий центр «КриптоПро УЦ» версия 2.0, имеющим действующий сертификат (заключение) ФСБ России.

## 2. Установка КриптоПро OCSF Server

Перед началом установки КриптоПро OCSF Server необходимо выполнить установку СКЗИ «КриптоПро CSP». Установка «КриптоПро CSP» должна выполняться в соответствии с указаниями эксплуатационной документации на используемую версию СКЗИ в соответствии с используемой ОС.

Установка ПО КриптоПро OCSF Server осуществляется в следующем порядке:

1. Выполните установку дистрибутива, расположенного на компакт-диске.
2. Укажите название организации и серийный номер лицензии (в конфигурационном файле, см. раздел 3).
3. Установите КриптоПро OCSF Client и введите серийный номер лицензии для него (см. раздел 2.2). Если не ввести лицензию на КриптоПро OCSF Client, то будет установлена временная лицензия сроком на 3 месяца.
4. Следующим шагом необходимо получить сертификат Оператора Службы OCSF. Подробно требования к сертификату оператора и процесс создания такого сертификата описан в разделе 4.1 настоящего Руководства.
5. Настройте Службу для работы в выбранном режиме. Подробное описание настроек Службы представлено в разделе 4.2 настоящего Руководства.
6. Проверьте работоспособность Службы, как указано в разделе 4.2.7 настоящего Руководства.

### 2.1. Особенности установки КриптоПро OCSF Server под управлением ОС Linux

Установка дистрибутива КриптоПро OCSF Server выполняется простым копированием. Необходимо дать права на выполнение следующего файла:

```
chmod u+x ocspsvc
```

### 2.2. Установка КриптоПро OCSF Client

Модуль КриптоПро OCSF Client предназначен для установки на рабочем месте клиента и позволяет решить каждую из следующих задач:

- Создать запрос на проверку статуса сертификата.
- Подписать запрос.
- Отправить запрос службе и получить ответ.
- Проверить сертификат подписи ответа.
- Проверить подпись ответа на заданном сертификате.

#### 2.2.1. Установка КриптоПро OCSF Client на компьютер под управлением ОС Windows

Модуль КриптоПро OCSF Client входит в состав КриптоПро OCSFUTIL из состава КриптоПро ЭЦП SDK. Для его установки следует установить следующий дистрибутив:

```
ocsputil.msi
```

### 2.2.2. Установка КриптоПро OSCP Client на компьютер под управлением ОС Linux

Модуль КриптоПро OSCP Client входит в пакет **cprocsp-pki-cares** из состава КриптоПро PKI SDK. Для его установки следует выполнить следующие команды:

```
> tar xvf cares_linux_amd64.tar.gz
> cd cares_linux_amd64
> apt install ./cprocsp-pki-cares*.deb
```

### 2.2.3. Ввод лицензии на КриптоПро OSCP Client

Лицензия на КриптоПро OSCP Client может быть введена при помощи `ocsputil`. Для этого нужно выполнить следующую команду с повышенными правами:

```
> ocsputil license -s <серийный номер>
```

### 3. Конфигурационные файлы КриптоПро OCSF Server

Параметры функционирования Службы указываются с помощью конфигурационных файлов. Пример конфигурационного файла (см. Рисунок 1) **ocsp\_2012.json** можно найти в той же директории, в которую была выполнена установка КриптоПро OCSF Server.



Обратите внимание, что конфигурационные файлы должны быть сохранены в кодировке UTF-8.

**Рисунок 1. Пример конфигурационного файла**

```
{
  "AllowedHosts": "*",
  "Serilog": {
    "Using": [ "Serilog.Expressions", "Serilog.Sinks.File" ],
    "MinimumLevel": {
      "Default": "Warning",
      "Override": {
        "Microsoft": "Information",
        "Microsoft.Hosting.Lifetime": "Information",
        "ocspsvc.OcspService": "Information",
        "ocspsvc.Audit": "Information"
      }
    },
    "WriteTo": [
      {
        "Name": "Console",
        "Args": {
          "outputTemplate": "[{Timestamp:HH:mm:ss.fff} {Level:u3}] {Message:l}"
        }
      },
      {
        "Name": "File",
        "Args": {
          "path": "/tmp/ocspsvc_2012_log.txt",
          "rollingInterval": "Day",
          "outputTemplate": "[{Timestamp:HH:mm:ss.fff} {Level:u3}] {Message:l}"
        }
      }
    ],
    "configureLogger": {
      "Filter": [
        {
          "Name": "ByIncludingOnly",
          "Args": {
            "expression": "StartsWith(SourceContext, 'ocspsvc.Audit')"
          }
        }
      ]
    },
    "WriteTo": [
      {
        "Name": "File",
        "Args": {
          "path": "/tmp/ocspsvc 2012 audit.txt",
```

```

        "outputTemplate": "[{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} {Level:u3}] {Message:l}{NewLine}{Exception}",
        "rollingInterval": "Day",
        "retainedFileCountLimit": 7
    }
}
]
},
"urls": "http://localhost:2012;",
"OCSP": {
    "OperatorThumbprint": "0953de8e25a1f26556964baa7e3c75b815d09525",
    "OperatorPin": "",
    "OperatorStore": "My",
    "ResponderType": "ByHash",
    "Ocsptype": "db", // "db" "crl"
    "Algorithm": "1.2.643.7.1.1.3.2",
    "CRLFolderPath": "/crl",
    "CRLUseCurrentTime": false,
    "RequireNonce": true,
    "RequireSignedOcsprequest": false,
    "RequestMaxSize": 2500,
    "ResponseMaxSize": 5000,
    "CAConnection": {
        "URL": "https://astra-ca:444/api/certRegistry/certStatus/",
        "TLSThumbprint": "f1301807778006abd05a835340389d4f41029a41",
        "TLSStore": "My"
    }
},
"License": {
    "SerialNumber": "",
    "Company": ""
}
}

```

Описание основных параметров конфигурационного файла представлено в таблице:

**Таблица 1. Описание параметров конфигурационного файла**

| Название параметра | Значение                                                              | Описание параметра                                                                                                                                                                  |
|--------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "AllowedHosts"     | "*", "example.com;localhost"                                          | Имена узлов, для которых будет доступна Служба. Если узлов несколько, то для их разделения используют символ ";". Значение "*" означает, что Служба будет доступна для любых узлов. |
| "Serilog"          | Набор параметров для управления настройками журнала Службы            | Подробное описание параметров см. в разделе 4.2.2                                                                                                                                   |
| "urls"             | "http://*:5000"<br>"http://localhost:5001"<br>"https://hostname:5002" | Адрес и порт, по которому происходит обращение к Службе. В случае задания нескольких адресов их нужно разделять при помощи символа ";"                                              |
| "OCSP"             | Набор параметров для управления настройками режима работы Службы      | Подробное описание параметров см. в разделе 4.2.                                                                                                                                    |

| Название параметра | Значение                                    | Описание параметра                                                                                                                                                                                                                                                                                                             |
|--------------------|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "License"          | Название компании и серийный номер лицензии | <p>Название компании указывается в поле "Company", серийный номер лицензии – в поле "SerialNumber".</p> <p>Обратите внимание, что специальные символы в названии компании, такие как кавычки, должны быть экранированы.</p> <p>Например: "Company": "ООО \"КРИПТО-ПРО\""</p> <p>Все символы должны быть в кодировке UTF-8.</p> |

## 4. Запуск и проверка работоспособности Службы

### 4.1. Управление операторами Службы

Служба КриптоПро OSCP Server работает от имени Оператора. Оператор – это уполномоченное лицо, обладающее сертификатом и ключом подписи OSCP-ответов, и имеющее право на управление Службой, т.е. осуществлять её запуск и остановку.

Таким образом, запуск службы должен осуществляться из-под учётной записи, соответствующей роли Оператора Службы. Учётная запись может быть локальной или доменной, если компьютер, на котором установлена Служба, является членом домена.



Обратите внимание, что сертификат Оператора должен быть установлен в хранилище (со ссылкой на закрытый ключ) и учётная запись Оператора должна иметь доступ к этому хранилищу и сертификату.

#### 4.1.1. Требования к сертификату оператора

Создание сертификатов ключей проверки ЭП для ПО «КриптоПро OSCP» должно осуществляться в соответствии с требованиями законодательства Российской Федерации в области использования электронной подписи, регулирующими автоматическое создание и автоматическую проверку электронной подписи в информационных системах.

Каждый оператор должен иметь один или несколько сертификатов ключа проверки электронной подписи OSCP-ответов. Процедура запуска Службы предусматривает загрузку ключа подписи OSCP-ответов Оператора, который осуществляет запуск.

В [1] определён ряд требований, необходимых для признания OSCP-ответа действительным. В соответствии с этими требованиями, клиентское ПО проверяет по сертификату, которым подписан полученный OSCP-ответ, уполномочен ли данный OSCP-сервер Удостоверяющим Центром, издавшим сертификат, чей статус запрашивался, выдавать информацию о статусе данного сертификата (см. [1], подраздел 4.2.2.2).

OCSP-сервер считается уполномоченным, если он подписал OSCP-ответ тем же ключом, которым подписан сертификат, чей статус запрашивался, или если сертификат OSCP-сервера подписан этим ключом и содержит в расширении ECU назначение **Подпись ответов службы OSCP (id-kp-OCSPSigning – OID 1.3.6.1.5.5.7.3.9)**.

При использовании КриптоПро OSCP Client возможен альтернативный вариант признания OSCP-сервера уполномоченным. Для этого сертификат Службы должен быть перечислен в групповой политике **Службы OSCP: сертификаты уполномоченных служб OSCP**. Данную политику нужно установить на том компьютере, где производится проверка OSCP-ответа.

Сертификат оператора службы OSCP должен удовлетворять требованиям [2] с учетом [3].

Удостоверяющий Центр в соответствии со своим регламентом и настройками ПО может добавить в сертификат оператора **Признак доверия службе OSCP (id-pkix-ocsp-nocheck – OID 1.3.6.1.5.5.7.48.1.5)**. В зависимости от возможностей ПО Удостоверяющего Центра может потребоваться добавить данное расширение в создаваемый запрос на сертификат. Наличие данного расширения в сертификате, на котором подписан OSCP-ответ, отменяет его проверку на отзыв клиентскими приложениями.



Отсутствие расширения **Признак доверия службе OSCP (id-pkix-ocsp-nocheck)** в сертификате оператора приведёт к тому, что клиентские приложения будут проверять статус данного сертификата. Данная проверка может быть произведена по СОС, однако это может нивелировать многие преимущества от использования протокола OSCP.

В связи с этим рекомендуется включать в сертификат оператора данное расширение, при этом принимая во внимание, что в данном случае компрометация ключа оператора почти также нежелательна по своим последствиям, как и компрометация ключа УЦ.

#### 4.1.2. Управление сертификатами оператора

Для того, чтобы назначить новый сертификат Оператора Службы, его отпечаток следует указать в конфигурационном файле (см. раздел 4.2 настоящего Руководства). Кроме этого, нужно указать хранилище, в котором установлен данный сертификат (со ссылкой на закрытый ключ).

Учётная запись, из-под которой планируется осуществлять запуск Службы, должна иметь доступ к этому хранилищу и к этому сертификату.

### 4.2. Настройка Службы

Помимо создания сертификата оператора Службы и назначения сертификата подписи OSCP-ответов, в Службе необходимо настроить один из режимов работы, которые определяются источником получения информации о статусах сертификатов:

- Режим работы с базой данных Центра Сертификации или Центра Регистрации КриптоПро УЦ;
- Режим работы со списками отзыва сертификатов.

Для настройки режимов работы служит конфигурационный файл (см. раздел 3 настоящего Руководства). Описание параметров настройки режимов работы Службы приведено в таблице (см. Таблица 2).

**Таблица 2. Описание параметров настройки режима работы Службы**

| Название параметра   | Возможные значения                                                                            | Описание параметра                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| "OperatorThumbprint" | Поле thumbprint сертификата Оператора. Шестнадцатеричные цифры нижним регистром без пробелов. | Отпечаток сертификата Оператора.                                                                                                       |
| "OperatorPin"        |                                                                                               | PIN-код для доступа к контейнеру закрытого ключа Оператора Службы.                                                                     |
| "OperatorStore"      | Название хранилища, например "My"                                                             | Хранилище сертификатов для поиска сертификата Оператора. Хранилище будет открыто для текущей учётной записи.                           |
| "ResponderType"      | "ByHash" "ByName"                                                                             | На основании этого параметра будет заполнено поле ResponderID выдаваемых службой OSCP-ответов.                                         |
| "Ocsptype"           | "db", "CRL"                                                                                   | Режим работы Службы – по базе данных Центра сертификации или Центра регистрации КриптоПро УЦ или по спискам отзыва сертификатов (CRL). |

| Название параметра        | Возможные значения                                                    | Описание параметра                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "CAConnection"            | Набор параметров для подключения к Реестру сертификатов КриптоПро УЦ. | Подробное описание параметров представлено в разделе 4.2.1 настоящего Руководства.                                                                                                                                                 |
| "Algorithm"               | OID алгоритма подписи, например "1.2.643.7.1.1.3.2"                   | Алгоритм подписи, используемый при создании OSCP-ответа. Должен соответствовать алгоритму в сертификате Оператора.                                                                                                                 |
| "CRLUseCurrentTime"       | true или false                                                        | Заменять время последнего обновления списка отозванных сертификатов (CRL) текущим временем. Используется в режиме работы со списками отзыва сертификатов. Подробное описание данного параметра представлено в разделе 4.2.1.       |
| "CRLFolderPath"           | Локальный путь к директории, например "F:\\CRLFolder", "/crl"         | Путь к директории со списками отзыва сертификатов (CRL).                                                                                                                                                                           |
| "RequireNonce"            | true или false                                                        | Требовать наличие поля 'Nonce' в запросах. Если запрос не содержит поля 'Nonce', то OSCP-ответ выдан не будет.<br>Отключать требование 'Nonce' допускается только при необходимости обеспечить совместимость со старыми системами. |
| "RequireSignedOcsRequest" | true или false                                                        | Если данный параметр установлен в true, то служба будет обрабатывать только подписанные запросы.                                                                                                                                   |

Применение сервисов онлайн-проверки статусов сертификатов разрешено только в отношении сертификатов, созданных и выданных УЦ, в составе которого применяются указанные сервисы.

#### 4.2.1. Параметры режимов работы Службы

##### Режим работы с базой данных Реестра сертификатов КриптоПро УЦ

Данный режим обеспечивает наибольшую актуальность информации в OSCP-ответах, поскольку работа идёт непосредственно с базой данных, хранящей информацию о статусах сертификатов.

**Таблица 3. Описание параметров подключения к Реестру отозванных сертификатов**

| Название параметра | Возможные значения                                                                 | Описание параметра                                                                                 |
|--------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| "URL"              | "https://<имя_сайта:порт>/api/certregistry/certstatus/"                            | Строка подключения к Реестру сертификатов Центра сертификации или Центра регистрации КриптоПро УЦ. |
| "TLSThumbprint"    | Поле thumbprint сертификата, шестнадцатеричные цифры нижним регистром без пробелов | Отпечаток сертификата, который будет использоваться для подключения к Реестру сертификатов         |

| Название параметра | Возможные значения                | Описание параметра                                                                                                                                                                     |
|--------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | лов.                              | тов КриптоПро УЦ по протоколу TLS.                                                                                                                                                     |
| "TLSStore"         | Название хранилища, например "My" | Хранилище сертификатов для поиска сертификата, используемого для подключения к Реестру сертификатов КриптоПро УЦ по протоколу TLS. Хранилище будет открыто для текущей учётной записи. |

В режиме работы по базе данных Реестра сертификатов КриптоПро УЦ, КриптоПро OSCP Server в издаваемых OSCP-ответах проставляет текущее время в **thisUpdate** и не включает время **nextUpdate**.

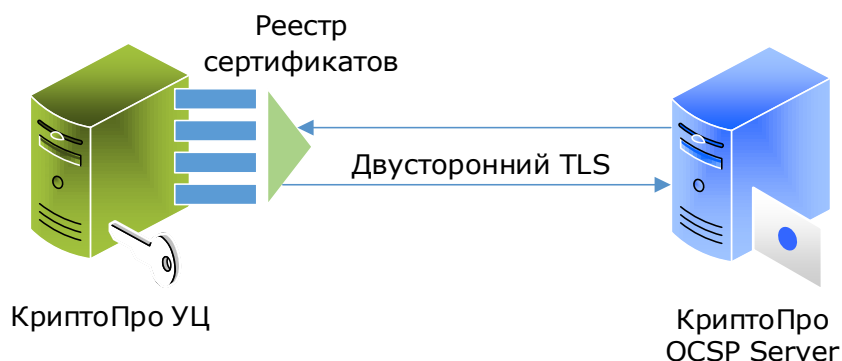


Установка КриптоПро OSCP Server и КриптоПро УЦ на одном компьютере допустима исключительно в целях тестирования, так как при данной конфигурации ставится под угрозу информационная безопасность УЦ. При эксплуатации системы в рабочем режиме необходимо устанавливать КриптоПро OSCP Server на отличном от КриптоПро УЦ компьютере.

Для настройки режима работы по БД Реестра сертификатов КриптоПро УЦ, в конфигурационном файле КриптоПро OSCP Server настраивается строка подключения к Реестру сертификатов КриптоПро УЦ. Строка подключения имеет вид:

```
https://<имя_сайта:порт>/api/certregistry/certstatus/
```

**Рисунок 2. Схема доступа к Реестру сертификатов КриптоПро УЦ**



В качестве транспортного соединения между КриптоПро OSCP Server и компьютером с Реестром сертификатов КриптоПро УЦ используется протокол HTTPS.



В целях противодействия атакам типа «отказ в обслуживании» со стороны удаленных пользователей «КриптоПро OSCP Server», при встраивании в информационные системы, организация инфраструктуры взаимодействия «КриптоПро OSCP Server» и Удостоверяющего центра должна осуществляться с учетом предъявляемых нагрузок на «КриптоПро OSCP Server».

## Режим работы со списком отзыва сертификатов

Режим работы с СОС подразумевает два настраиваемых параметра:

- путь к папке с СОС,
- критерий определения издателя СОС.

Путь к папке с СОС определяет папку, в которой Служба будет искать один или несколько СОС, из которых она будет черпать информацию о статусах сертификатов. Этот параметр может указывать локальную или сетевую (UNC) папку, в которую осуществляется регулярная публикация выпускаемых УЦ СОС.

Несколько СОС необходимы Службе, например, если УЦ имеет несколько ключей. Такая ситуация возникает, например, после плановой смены ключа УЦ. Кроме этого случая, Служба может одновременно выдавать ответы о статусах сертификатов нескольких разных УЦ. Для этого также необходимы несколько СОС.

Служба при запуске загружает все найденные в данной папке СОС по расширению **.crl**, действующие на момент запуска. Во время работы Служба отслеживает изменения файлов в заданной папке – создание новых, удаление старых и изменение существующих файлов. Все изменения немедленно отражаются в Службе, таким образом в OSCP-ответах отражается в точности та информация, которая содержится в СОС в заданной папке в данный момент.

Чтобы Служба могла загружать СОС из папки, необходимо убедиться, что учётная запись, под которой работает Служба, имеет права на обзор папки и чтение файлов в ней.



При решении задачи распространения СОС нужные файлы необходимо копировать в папку назначения, а не перемещать. Это связано с тем, что на большинстве ОС при копировании файла, права доступа к нему наследуются из свойств папки, а при перемещении остаются прежними и Служба может не получить доступ к такому файлу.

Убедитесь, что используемая для копирования утилита поддерживает наследование прав доступа из свойств папки.

Если СОС не издаётся на компьютере, где установлена Служба, то необходимо обеспечить своевременное обновление СОС в Службе. При использовании КриптоПро УЦ, это можно обеспечить путём публикации СОС в сетевую папку, доступную с компьютера Службы, либо путём настройки задач распространения СОС.



Для обеспечения бесперебойной работы Службы необходимо обновлять папку с СОС следующим образом: поместить в папку новые файлы СОС, не удаляя и не заменяя имеющихся файлов; после помещения новых файлов можно удалить ненужные.

Пример командного файла, реализующего необходимый алгоритм обновления файлов СОС, приведён в приложении (см. Приложение В).

Если СОС издаётся на компьютере, где установлена Служба, то нельзя в качестве папки с СОС указывать папку, в которую публикуются СОС Удостоверяющим Центром. В этом случае необходимо завести отдельную папку и обеспечить обновление СОС в ней по алгоритму, описанному в замечании выше.

В режиме работы по СОС Служба в издаваемых OSCP-ответах проставляет времена **thisUpdate** и **nextUpdate** в соответствии с СОС. Это приводит к тому, что некоторые реализации клиентов OSCP могут считать такой ответ недостаточно свежим. В частности, КриптоПро OSCP Client по умолчанию считает ответ неактуальным, если время **thisUpdate** отличается от текущего времени на 1 день. Если период публикации СОС превышает это время, то для того, чтобы КриптоПро OSCP Client принимал ответы, издаваемые Службой в режиме работы по СОС, необходимо настроить групповую политику **Ответ: Максимальная давность поля 'ThisUpdate'** и установить в ней время, равное или превышающее период публикации СОС.

Если по каким-то причинам требуется, чтобы OCSP-ответы содержали в поле **thisUpdate** текущее время, можно воспользоваться параметром "CRLUseCurrentTime" = true, но в данном случае необходимо учитывать возможность выдачи недостоверных ответов – в случае, если сертификат уже отозван, а соответствующий СОС (содержащий отозванный сертификат) ещё не выпущен. В этом случае Служба выдаст OCSP-ответ на основании предыдущего (но ещё действующего СОС), в котором сертификат ещё не был отозван.

#### 4.2.2. Параметры управления журналом Службы

Журнал позволяет вести учёт всех событий, происходящих в Службе, а также полученных запросов и отправленных ответов.

К отслеживаемым событиям, происходящим в Службе, относятся:

- запуск и останов Службы;
- информация о событиях (загрузка ключа, обновление CRL, подключение к базе данных и т.д.);
- сообщения о предупреждениях и об ошибках;
- полученный OCSP-запрос;
- отправленный OCSP-ответ;
- отправленное в качестве ответа сообщение об ошибке.

Файлы журнала создаются при наличии свободного места на диске. В связи с этим, во избежание переполнения диска, необходимо предусмотреть своевременную запись файлов журнала на другие носители (при необходимости). Или следует предусмотреть автоматическую очистку старых журналов, если отсутствует необходимость их хранения.

Параметры управления журналом Службы настраиваются в конфигурационном файле Службы и описаны в таблице (см. Таблица 4).

**Таблица 4. Параметры управления журналом Службы**

| Название параметра | Назначение                                                                                                                                                                                                              | Возможные значения                             | Описание значения                                                                                                                                              |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "Using"            | Список используемых модулей Serilog                                                                                                                                                                                     | "Serilog.Expressions",<br>"Serilog.Sinks.File" | Информацию о модулях Serilog и их функциях можно получить <a href="#">на официальной странице проекта</a> .                                                    |
| "MinimumLevel"     | Задаёт минимальный уровень логирования, означающий, насколько подробная информация должна попасть в журнал.<br><br>В журнал будет выводиться информация, соответствующая выбранному уровню и всем более низким уровням. | "Verbose"                                      | Наиболее подробная информация, включающая вспомогательные записи.                                                                                              |
|                    |                                                                                                                                                                                                                         | "Debug"                                        | Информация о значениях переменных.                                                                                                                             |
|                    |                                                                                                                                                                                                                         | "Information"                                  | Информация о событиях: старт службы, загрузка ключа, обновление CRL. Информация о полученных запросах и отправленных ответах, включая время получения запроса. |
|                    |                                                                                                                                                                                                                         | "Warning"                                      | Информация о предупреждениях.                                                                                                                                  |
|                    |                                                                                                                                                                                                                         | "Error"                                        | Информация об ошибках.                                                                                                                                         |
|                    |                                                                                                                                                                                                                         | "Fatal"                                        | Информация о критических ошибках.                                                                                                                              |

|           |                                                                                                                           |        |                                                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "WriteTo" | Представляет собой массив, каждый из элементов которого задаёт метод вывода информации. Можно указать несколько значений. | "Name" | Название метода вывода. "Console" - вывод информации в консоль, "File" – вывод информации в файл, "Logger" – вывод информации в файл с возможностью гибкой настройки. |
|           |                                                                                                                           | "Args" | Параметры для выбранного метода вывода. Подробное описание параметров приведено ниже.                                                                                 |

Для разных методов вывода задаются следующие значения параметров:

- "path": путь к файлу журнала. Если файл не существует, он будет автоматически создан.
- "rollingInterval": период, в течение которого события записываются в файл. По истечении указанного периода, создаётся новый файл журнала.
- "retainedFileCountLimit": максимальное число хранимых файлов журнала. При достижении максимального числа файлов, старые файлы будут автоматически удалены.
- "outputTemplate": шаблон вывода записи журнала. В шаблоне записи можно использовать следующие выражения (см. Таблица 5).

**Таблица 5. Описание шаблона вывода журнала Службы**

| Формат записи            | Описание                                                                                                                                                                                                                                                                                                            |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {Timestamp:HH:mm:ss.fff} | Формат вывода в журнал времени наступления события.                                                                                                                                                                                                                                                                 |
| {Level:u3}               | Формат вывода в журнал уровня логирования, на котором произошло событие. Для сокращённого написания в журнале имени уровня, строчными или заглавными буквами, следует использовать сочетание символов «u+цифра» или «w+цифра» соответственно. Цифра означает, сколько символов имени уровня нужно вывести в журнал. |
| {Message:lj}             | Формат вывода сообщений в журнал. Символ «l» отвечает за способ вывода строк с кавычками. Символ «j» используется для задания формата вывода структурированных данных в виде JSON-объектов.                                                                                                                         |
| <s:{SourceContext}>      | Вывод в журнал информации об источнике сообщения                                                                                                                                                                                                                                                                    |
| {NewLine}                | Перевод строки                                                                                                                                                                                                                                                                                                      |
| {Exception}              | Вывод информации об исключении                                                                                                                                                                                                                                                                                      |

Для метода вывода Logger предусмотрены дополнительные настройки (поле "configureLogger"), позволяющие выбрать информацию, которая будет выведена в журнал:

- "Filter": фильтр событий, информация о которых будет добавляться в журнал. Представляет собой массив, каждый из элементов которого задаёт определённый тип событий. Для каждого значения указывается название фильтра (поле "Name") и параметры (поле "Args"), в которых задаётся выражение для поиска нужных событий. Например: "expression": "StartsWith(SourceContext, 'ocspsvc.Audit')"
- "WriteTo": метод вывода информации. Данный параметр, полностью аналогичен описанному в таблице (см. Таблица 4. Параметры управления журналом Службы).

## 4.2.3. Параметры производительности

Таблица 6. Описание параметров производительности

|                   |                                                    |                                                                                                                                                                                           |
|-------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "RequestMaxSize"  | Максимальный допустимый размер запроса (в байтах). | Если размер запроса превышает значение, указанное в данном параметре, то запрос декодироваться и обрабатываться не будет.<br>Предназначен для защиты от атак типа "Отказ в обслуживании". |
| "ResponseMaxSize" | Максимальный размер OSCP-ответа (в байтах).        | Если размер OSCP-ответа превышает значение, указанное в данном параметре, то такой OSCP-ответ выдан не будет.<br>Предназначен для защиты от атак типа "Отказ в обслуживании".             |

## 4.2.4. Групповые политики КриптоПро OSCP Client

Интерфейс клиентских приложений КриптоПро OSCP может настраиваться с помощью групповых политик (group policy), описанных в файле административного шаблона **ocspcli.adm**. На компьютере, где установлен КриптоПро OSCP Client, этот файл располагается в папке **%SystemDir%\GroupPolicy\Adm** и уже подключен в оснастке **Групповая политика**. Для настройки политик в домене потребуется скопировать шаблон на контроллер домена и подключить его в оснастке Групповая политика.

Все политики могут задаваться как для пользователя, так и для компьютера, причем политика компьютера имеет преимущество перед политикой пользователя. Политики располагаются в узле **Крипто-Про\Клиент службы актуальных статусов сертификатов**. В настоящем разделе приводится описание этих групповых политик.

Для Unix-систем значения групповых политик задаются в конфигурационном файле. Задать или прочитать значение политики можно с помощью утилиты `srconfig` из состава КриптоПро CSP:

```
srconfig -ini "\config\cades\ocspolicy" -add <тип значения> "<имя политики>"
"<значение>"
```

Таблица 7. Описание групповых политик

| Название политики                                            | Описание политики                                                                                                                 |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Nonce: включать расширение 'nonce' в запрос по умолчанию     | Определяет, будет ли клиент по умолчанию включать расширение 'nonce' в OSCP-запросы.<br>Имя в Unix: UseNonceByDefault, тип: bool. |
| Nonce: запретить использование расширения 'nonce' в запросах | Позволяет запретить клиенту включать расширение 'nonce' в запросы на OSCP-запросы.<br>Имя в Unix: DisableNonce, тип: bool.        |
| Nonce: размер значения расширения 'nonce' в запросах         | Определяет размер значения расширения 'nonce' (в байтах), включаемого клиентом в запросы.<br>Имя в Unix: NonceLength, тип: long.  |
| Nonce: требовать использование расширения 'nonce' в запросах | Позволяет запретить клиенту отправлять OSCP-запросы не имеющие расширения 'nonce'.<br>Имя в Unix: RequireNonce, тип: bool.        |

| Название политики                                                       | Описание политики                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Аутентификация (прокси-сервер): запрещённые типы                        | Определяет типы аутентификации, которые запрещено использовать для подключения к прокси-серверу.<br>Не поддерживается в Unix.                                                                                                                            |
| Аутентификация (прокси-сервер): запрещённые типы (с использованием TLS) | Определяет типы аутентификации, которые запрещено использовать для подключения к прокси-серверу при использовании TLS-соединения.<br>Не поддерживается в Unix.                                                                                           |
| Аутентификация (прокси-сервер): тип по умолчанию                        | Позволяет задать тип аутентификации, используемый по умолчанию при соединении с прокси-сервером. Если данная политика не задана, то при соединении с прокси-сервером будет использоваться анонимная аутентификация.<br>Не поддерживается в Unix.         |
| Аутентификация (прокси-сервер): тип по умолчанию (с использованием TLS) | Позволяет задать тип аутентификации (с TLS), используемый по умолчанию при соединении с прокси-сервером. Если данная политика не задана, то при соединении с прокси-сервером будет использоваться анонимная аутентификация.<br>Не поддерживается в Unix. |
| Аутентификация: запрещённые типы                                        | Определяет типы аутентификации, которые запрещено использовать для подключения к службе OCSP.<br>Не поддерживается в Unix.                                                                                                                               |
| Аутентификация: запрещённые типы (с использованием TLS)                 | Определяет типы аутентификации, которые запрещено использовать для подключения к службе OCSP при использовании TLS.<br>Не поддерживается в Unix.                                                                                                         |
| Аутентификация: тип по умолчанию                                        | Позволяет задать тип аутентификации, используемый по умолчанию для подключения к службе OCSP. Если данная политика не задана, то при подключении будет использоваться анонимная аутентификация.<br>Не поддерживается в Unix.                             |
| Аутентификация: тип по умолчанию (с использованием TLS)                 | Позволяет задать тип аутентификации (с TLS), используемый по умолчанию для подключения к службе OCSP. Если данная политика не задана, то при подключении будет использоваться анонимная аутентификация.<br>Не поддерживается в Unix.                     |
| Запрос: алгоритм, используемый для хеширования данных                   | Определяет идентификатор (OID) алгоритма хеширования, используемого клиентом для хеширования различных полей при создании OCSP-запроса.<br>Имя в Unix: CertIDHashAlg, тип: string.                                                                       |
| Запрос: запретить неподписанные запросы                                 | Позволяет запретить отправку неподписанных OCSP-запросов.<br>Имя в Unix: DisableUnsignedRequests, тип: bool.                                                                                                                                             |
| Запрос: запретить подписанные запросы                                   | Позволяет запретить отправку подписанных OCSP-запросов.<br>Имя в Unix: DisableSignedRequests, тип: bool.                                                                                                                                                 |

| Название политики                                                          | Описание политики                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Запрос: сертификаты, включаемые в OSCP-запрос                              | <p>Определяет, какие сертификаты включать в OSCP-запрос. Эти сертификаты могут понадобиться службе OSCP для проверки подписи запроса. Возможные варианты:</p> <ul style="list-style-type: none"> <li>- не включать сертификаты (значение в Unix: 0);</li> <li>- сертификат подписчика (значение в Unix: 1);</li> <li>- цепочку кроме корневого сертификата (значение в Unix: 2);</li> <li>- цепочку сертификатов целиком (значение в Unix: 3).</li> </ul> <p>Имя в Unix: CertsToInclude, тип: long.</p>                                                                      |
| Ответ: максимальное расхождение времени получения ответа и времени подписи | <p>Данная политика определяет максимально возможное расхождение времени получения ответа от службы OSCP и времени, когда служба его подписала. Эта политика используется в случае, если ни в запросе, ни в ответе не присутствует расширение 'nonce', для подтверждения соответствия выданного OSCP-ответа запросу на него. Значение задается в миллисекундах. Если расхождение больше, чем указано в политике, то ответ признается некорректным. Если политика не задана, то используется значение 3 минуты.</p> <p>Имя в Unix: ResponseAccuracy, тип: long.</p>            |
| Ответ: максимальная давность поля "ThisUpdate"                             | <p>Данная политика определяет максимально возможную давность поля "ThisUpdate" OSCP-ответа, содержащего время выпуска СОС, по которому был определен статус сертификата. Если расхождение больше, чем указано в политике, то ответ признается некорректным. Если политика не задана, то используется значение 1 день.</p> <p>Имя в Unix: ThisUpdateAccuracy, тип: long.</p>                                                                                                                                                                                                  |
| Ответ: не использовать стандартный Revocation Provider Windows             | <p>Запрещает использование стандартного Revocation Provider Windows (cryptnet.dll) при проверке сертификата службы OSCP на отзыв в случае, если его статус не удалось определить по протоколу OSCP.</p> <p>Не поддерживается в Unix.</p>                                                                                                                                                                                                                                                                                                                                     |
| Прокси-серверы: прокси-сервер по умолчанию                                 | <p>Определяет адрес прокси-сервера, используемый по умолчанию при подключении к службе OSCP. Формат адреса: "&lt;протокол&gt;://[&lt;пользователь&gt;:&lt;пароль&gt;@]&lt;сервер&gt;[:порт]/[путь]". Здесь в качестве протокола можно указать "http" или "https". При указании имени пользователя и пароля в адресе прокси-сервера также следует задать соответствующий тип аутентификации в политике «Аутентификация (прокси-сервер): тип по умолчанию» или «Аутентификация (прокси-сервер): тип по умолчанию (с использованием TLS)».</p> <p>Не поддерживается в Unix.</p> |
| Прокси-серверы: разрешённые прокси-серверы                                 | <p>Определяет адреса разрешённых прокси-серверов.</p> <p>Не поддерживается в Unix.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Название политики                                                                 | Описание политики                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Службы OCSP: адрес службы OCSP по умолчанию                                       | <p>Определяет адрес службы OCSP по умолчанию. Формат адреса: "&lt;протокол&gt;://[&lt;пользователь&gt;:&lt;пароль&gt;@]&lt;сервер&gt;[:порт]/[путь]". Здесь в качестве протокола можно указать "http" или "https". При указании имени пользователя и пароля в адресе службы OCSP также следует задать тип аутентификации в политике «Аутентификация: тип по умолчанию» или «Аутентификация: тип по умолчанию (с использованием TLS)».</p> <p>Имя в Unix: DefaultOCSPURL, тип: string.</p>                                                                                                                                                                                                                                                                                                                      |
| Службы OCSP: непроверяемые на отзыв сертификаты служб OCSP                        | <p>Этой политикой можно определить сертификаты служб OCSP, которые не следует проверять на отзыв.</p> <p>Имя в Unix: NocheckOCSPs, тип: multistring.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Службы OCSP: разрешённые службы OCSP                                              | <p>Определяет адреса служб OCSP, к которым клиент может обращаться. Если этот параметр задан, то обращение к не указанным в данной политике службам приведёт к ошибке. Если политика не задана, то разрешены любые службы OCSP.</p> <p>Имя в Unix: AllowedOCSPs, тип: multistring.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Службы OCSP: сертификаты уполномоченных служб OCSP                                | <p>Этой политикой можно определить сертификаты служб OCSP, наделенных полномочиями выдавать ответы со статусами любых сертификатов. Не заданные в данной политике службы проходят проверку на то, что они уполномочены Удостоверяющим Центром, издавшим проверяемый сертификат, выдавать информацию о статусе данного сертификата (см. RFC 2560, подраздел 4.2.2.2). Службы задаются посредством перечисления значений хэш-функций (по алгоритму SHA-1) их сертификатов в шестнадцатеричном виде. Получить это значение для сертификата можно в стандартном окне Windows для его отображения, выбрав на вкладке "Состав" в списке атрибутов "Печать" (зависит от операционной системы, обычно последний в списке). Значение может содержать пробелы.</p> <p>Имя в Unix: AuthorizedOCSPs, тип: multistring.</p> |
| Типы ответов: включать расширение 'AcceptableResponses' в запрос по умолчанию     | <p>Определяет, будет ли клиент по умолчанию включать расширение 'AcceptableResponses' в OCSP-запросы.</p> <p>Имя в Unix: UseAcceptRespByDefault, тип: bool.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Типы ответов: запретить использование расширения 'AcceptableResponses' в запросах | <p>Позволяет запретить клиенту включать расширение 'AcceptableResponses' в OCSP-запросы.</p> <p>Имя в Unix: DisableAcceptResp, тип: bool.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Типы ответов: требовать использование расширения 'AcceptableResponses' в запросах | <p>Позволяет запретить клиенту отправлять OCSP-запросы не имеющие расширение 'AcceptableResponses'.</p> <p>Имя в Unix: RequireAcceptResp, тип: bool.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

#### 4.2.5. Запуск Службы

Запуск Службы может осуществить оператор, обладающий ключом и сертификатом подписи OCSP-ответов.

## Запуск Службы на ОС Windows

Запуск Службы выполняется с помощью программы командной строки **ocspsvc**. Программа устанавливается в каталог **Program Files\Crypto Pro\ocspsvc**.

Для запуска Службы, выполните следующую команду, указав путь к конфигурационному файлу:

```
> ocspsvc.exe --config="C:\Program Files\Crypto Pro\ocspsvc\ocsp_2012.json"
```

## Запуск Службы на ОС Linux

Для запуска Службы, выполните следующую команду, указав путь к конфигурационному файлу или его имя:

```
> ocspsvc --config=/usr/share/ocspsvc/ocsp_2012.json
```

или

```
> ocspsvc --name=ocsp_2012
```

При запуске Служба загружает ключ подписи OSCP-ответов в свой процесс и держит его открытым на протяжении всего сеанса работы.

Данная команда может использоваться для автоматического запуска Службы при загрузке операционной системы.

### 4.2.6. Остановка Службы

Для остановки Службы, нужно завершить работу процесса, в котором была запущена служба.

### 4.2.7. Проверка работоспособности Службы

После запуска Службы можно проверить её работоспособность с помощью программы командной строки **ocsputil**, которая поставляется в составе КриптоПро PKI SDK. Установка программы ocsputil совместно с модулем КриптоПро OSCP Client описана в разделе 2.2 настоящего руководства.

Для проверки Службы запросите у неё статус сертификата, выполнив следующие команды в этом каталоге:

```
> ocsputil makereq tobechecked.cer -o request.orq
```

Эта команда создаст запрос на статус сертификата из файла **tobechecked.cer**. Необходимо заранее подготовить файл с сертификатом. Созданный запрос будет записан в файл **request.orq** (значение параметра **request**). При возникновении ошибки, на экране будет выдано соответствующее сообщение.

Для того, чтобы отправить подготовленный запрос, воспользуйтесь командой:

```
> ocsputil sendreq --url=<url_службы>/ocspservice request.orq response.ors
```

Здесь **<url\_службы>** - URL виртуального каталога Службы. В конфигурационном файле данный параметр записан в поле "urls".

Эта команда отправит подготовленный запрос на статус сертификата из файла **request.orq** (предпоследний параметр командной строки). Если Служба выдаст ответ, он будет записан в файл **response.ors** (последний параметр командной строки).

Затем можно посмотреть и проверить содержимое OSCP-ответа с помощью следующей команды:

```
> ocsputil respinfo response.ors
```

Эта команда выведет на экран информацию об OSCP-ответе, в том числе статус сертификата.

Программа **ocsputil** использует для работы со Службой OSCP функции КриптоПро OSCP Client. Поэтому результат вызова этой программы зависит от групповых политик КриптоПро OSCP Client, настроенных на данном компьютере. Если Служба выдаёт ответ по СОС, то для

признания такого ответа правильным может потребоваться дополнительная настройка групповых политик (см. подраздел 4.2.4).

#### 4.2.8. Смена режима работы Службы

Для смены режима работы Службы следует внести необходимые изменения в конфигурационный файл, как описано в разделе 3 настоящего руководства. Для того, чтобы изменения вступили в силу, требуется перезапустить процесс, в котором работает Служба.

#### 4.2.9. Адрес Службы

Для получения OSCP-ответов клиентам нужно сообщить адрес настроенного и работающего экземпляра Службы.

Адрес Службы будет таким:

**http://<имя компьютера>:<порт>/ocspservice,**

где <имя компьютера> – сетевое имя компьютера, на котором работает Служба, <порт> – идентификатор порта Службы, заданный в конфигурационном файле.

### 4.3. Автоматический запуск Службы

Запуск Службы может выполняться путем запуска её исполняемых файлов. Однако, чтобы обеспечить автоматический старт Службы после перезагрузки сервера, можно настроить её автоматическую загрузку с помощью systemd как описано в этом разделе.

Для настройки автоматического запуска Службы необходимо выполнить следующие действия.

- создать файл в следующей директории:

```
/etc/systemd/system/ocspsvc.service
```

Пример файла:

```
[Unit]
Description=ocspsvc
[Service]
WorkingDirectory=/opt/svc/ocsp
ExecStart=/opt/svc/ocsp/ocspsvc --config=/opt/svc/ocsp/ocsp_2012.json
Restart=always
# Restart service after 10 seconds if the dotnet service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=ocspsvc
User=username
[Install]
WantedBy=multi-user.target
```

- Применить изменения:

```
sudo systemctl daemon-reload
```

- Разрешить автозагрузку:

```
sudo systemctl enable ocspsvc
```

- Запустить сервис:

```
sudo systemctl start ocspsvc
```

- Посмотреть информацию о работе сервиса можно с помощью следующих команд:

```
sudo systemctl status ocspsvc
sudo journalctl -u ocspsvc
```

## 4.4. Развертывание веб-сервера

Необходимо выполнить настройку веб-сервера nginx, Apache или IIS согласно эксплуатационной документации на КриптоПро CSP 5.0 R2.

### 4.4.1. Развертывание веб-сервера nginx в замкнутой программной среде (ЗПС) ОС Astra Linux SE

В составе дистрибутива УЦ поставляется установочный пакет веб-сервера nginx 1.18.0 (nginx\_1.18.0~astra-gost\_amd64\_signed.deb), подготовленный для использования в замкнутой программной среде (ЗПС) ОС Astra Linux SE.

Пример команды установки:

```
sudo dpkg -i nginx_1.18.0~astra-gost_amd64_signed.deb
```

### 4.4.2. Конфигурация nginx для Службы

Настройка выполняется путем редактирования файла конфигурации nginx (/etc/nginx/nginx.conf).

Пример конфигурации nginx:

```
user  nginx;
worker_processes  auto;

error_log  /var/log/nginx/error.log notice;
pid        /var/run/nginx.pid;

events {
    worker_connections  1024;
}

http {
    include mime.types;
    default_type text/html;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile      on;

    keepalive_timeout  65;

    location /ocspservice {
        proxy_pass http://localhost:2012;
    }

    location /ocsp/ocsp.srf {
        proxy_pass http://localhost:2012/ocspservice;
    }
}
```

### 4.4.3. Развертывание веб-сервера IIS в ОС Microsoft Windows.

Развертывание IIS производится средствами операционной системы, в **Диспетчере сервера** через мастер добавления ролей и компонентов.

#### 4.4.4. Конфигурация IIS для Службы

Конфигурация IIS осуществляется с использованием оснастки MMC Диспетчер служб IIS из состава ОС Windows. Оснастка устанавливается в процессе добавления роли IIS.

Для обеспечения работоспособности Службы на IIS необходимо настроить веб-приложение ocspsvc. Перед настройкой веб-приложения нужно создать пул приложений (например OCSPool), работающий под учетной записью, у которой есть права доступа к ключу и сертификату, используемым для подключения к УЦ, а также к ключу и сертификату, используемым для создания ответа Службой.

При создании непосредственно веб-приложения ocspsvc в качестве физического пути необходимо выбрать локальную папку, содержащую бинарные модули Службы, а в качестве пула приложений – пул, созданный выше.

Для работы Службы необходимо указать путь до конфигурационного файла Службы в файле настроек IIS web.config.

Пример файла web.config:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <location path="." inheritInChildApplications="false">
    <system.webServer>
      <handlers>
        <add name="aspNetCore" path="*" verb="*" modules="AspNetCoreModuleV2"
resourceType="Unspecified" />
      </handlers>
      <aspNetCore processPath=".\\ocspsvc.exe" arguments="--config=.\\ocsp_2012.json"
stdoutLogEnabled="false" stdoutLogFile=".\logs\\stdout" hostingModel="inprocess" />
    </system.webServer>
  </location>
</configuration>
```

## 5. Перечень сокращений

|      |                                                                                                |
|------|------------------------------------------------------------------------------------------------|
| COM  | Модель компонентных объектов (Component Object Model)                                          |
| CSP  | Криптопровайдер (Cryptographic Service Provider)                                               |
| DCOM | Распределённый COM (Distributed COM)                                                           |
| DNS  | Доменная система имён (Domain Name System)                                                     |
| MMC  | Консоль управления Microsoft (Microsoft Management Console)                                    |
| OCSP | Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol) |
| OID  | Идентификатор объекта (Object Identifier)                                                      |
| RPC  | Удалённый вызов процедур (Remote Procedure Call)                                               |
| UNC  | Универсальное соглашение об именовании (Universal naming convention)                           |
| БД   | База данных                                                                                    |
| НСД  | Несанкционированный доступ                                                                     |
| ОС   | Операционная система                                                                           |
| ПК   | Программный комплекс                                                                           |
| ПО   | Программное обеспечение                                                                        |
| СКЗИ | Средство криптографической защиты информации                                                   |
| СОО  | Список отзыва сертификатов (Certificate Revocation List)                                       |
| УЦ   | Удостоверяющий Центр                                                                           |
| ЦР   | Центр Регистрации                                                                              |
| ЦС   | Центр Сертификации                                                                             |
| ЭП   | Электронная подпись                                                                            |

## 6. Перечень ссылочных документов

1. Santesson, S., et al., "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP", IETF, RFC 6960, June 2013.
2. Cooper, D., et al., "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile", IETF, RFC 5280, May 2008.
3. МР 26. 2.001-2020 «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509»

## Приложение А. Заполнение полей thisUpdate и nextUpdate службой актуальных статусов при различных режимах работы

| Режим работы                                            | Основной источник | Источник информации о статусе сертификата | Поле thisUpdate <sup>1</sup>    | Поле nextUpdate                 |
|---------------------------------------------------------|-------------------|-------------------------------------------|---------------------------------|---------------------------------|
| Работа по базе данных Реестра сертификатов КриптоПро УЦ | Доступен          | БД Реестра сертификатов КриптоПро УЦ      | Текущее время                   | Не включается                   |
|                                                         | Недоступен        | Статус сертификата «Неизвестен»           |                                 |                                 |
| Работа по СОС                                           | Доступен          | СОС                                       | Время последнего обновления СОС | Время следующего обновления СОС |
|                                                         | Недоступен        | Статус сертификата «Неизвестен»           |                                 |                                 |

<sup>1</sup> Если включена опция **Заменять время последнего обновления CRL текущим временем**, то в поле **thisUpdate** в любом случае проставляется текущее время.

## Приложение В. Пример командного файла, обновляющего файлы СОС

Использование:

```
copyCRL.bat [source-folder] [destination-folder]
```

**[source-folder]** – определяет папку, из которой будут скопированы файлы СОС.

**[destination-folder]** – определяет папку, в которую будут помещены файлы СОС.

```
@echo off
if /I %1 EQU "" (
echo Error: set source folder
goto err)

if /I %2 EQU "" (
echo Error: set destination folder
goto err)

cd /d "%1"
for %%c in (*.crl) DO (
if exist "%2\%%c" (
copy %%c %2\new_%%c
move /y %2\new_%%c %2\%%c) else (
copy /y %%c %2\))
exit 0

:err
echo usage: copyCRL.bat [source-folder] [destination-folder]
exit 1
```