



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ»**

РУКОВОДСТВО ПО КОНФИГУРАЦИИ X509

RU.33654484.0004-02 91 04

Листов 18

СОДЕРЖАНИЕ

1 Введение.....	3
1.1 Область применения.....	3
1.2 Краткое описание возможностей.....	3
1.3 Уровень подготовки администратора.....	4
2 Назначение и условия работы СКДПУ.....	5
2.1 Назначение СКДПУ.....	5
2.2 Требования к техническим и программным средствам.....	5
2.3 Требования к аппаратному обеспечению.....	6
2.4 Требования к программному обеспечению.....	6
3 Установка параметров X509.....	8
3.1 Настройка X509.....	8
3.2 Настройка X509 в режиме высокой доступности СКДПУ.....	8
4 Администраторские функции X509.....	9
4.1 Аутентификация пользователя.....	9
4.2 Управление списком отозванных сертификатов (CRL).....	9
5 Аутентификация X509.....	11
6 Выход из режима X509.....	12
7 Общие сведения.....	13
Перечень сокращений.....	14
Перечень рисунков.....	16
Перечень таблиц.....	17
История изменений.....	18

1 ВВЕДЕНИЕ

1.1 Область применения

Настоящий документ предназначен для администраторов СКДПУ и содержит описание действий для настройки параметров проверки подлинности X509 СКДПУ.

1.2 Краткое описание возможностей

Основные возможности СКДПУ приведены в [таблица 1](#).

Таблица 1 – Основные возможности СКДПУ

Основные возможности	Описание
Контроль доступа	СКДПУ позволяет создать политику управления доступом на основе прав пользователей: целевые учетные записи, протоколы, интервалы времени и типы сеансов.
Единая точка входа в систему (SSO)	Для доступа к учетным записям достаточно предоставить имя пользователя и пароль в СКДПУ.
Поддержка нескольких протоколов администрирования	СКДПУ поддерживает следующие протоколы администрирования устройств и серверов: RDP/TSE, SSH, TELNET, VNC, SFTP/SCP и т.д.
Отслеживание активности и запись сеансов	Регистрация и возможность записи всех действий, выполненных на управляемых устройствах в течение графического сеанса (RDP/TSE или VNC) или сеанса командной строки (SSH, TELNET).
Управление паролями	СКДПУ позволяет изменять пароли на управляемых устройствах по запросу или через заданные интервалы времени.
Работа без использования агентов	СКДПУ работает без использования специальных агентов на администрируемых устройствах или на рабочих станциях администраторов.
Статистика и отчеты о действиях	Возможность формировать рабочую статистику/отчеты и экспортировать эти данные в формате CSV через интерфейс администратора.

Основные возможности	Описание
Делегирование функций администрирования СКДПУ	Средства управления профилями позволяют определить, какие действия будут доступны каждому пользователю СКДПУ (например, создание пользователей, управление правами и т.д.)
Анализ потока и распознавание текста	СКДПУ позволяет в реальном времени обнаруживать определенные строки символов в сессиях SSH и анализировать содержимое сеансов подключения к удаленному рабочему столу (RDP/TSE).
Контроль в реальном времени	Администраторы СКДПУ могут просматривать активные сеансы подключения к удаленному рабочему столу и SSH в СКДПУ в реальном времени.
Поддержка Web Service	Вся информация о пользователях, учетных записях, устройствах, правах доступа в СКДПУ может вводиться или быть доступна с помощью Web Service API.

1.3 Уровень подготовки администратора

Администратор должен обладать следующими знаниями:

- Системное администрирование ОС Windows/Linux и активного сетевого оборудования;
- Базовые знания сетевых протоколов;
- Администрирование СКДПУ и умение с его помощью реализовывать корпоративную политику безопасности, в части относящейся к информационному обмену;
- Знание и соблюдение требований конфиденциальности (секретности) при проведении работ.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ РАБОТЫ СКДПУ

2.1 Назначение СКДПУ

СКДПУ предназначена для мониторинга и аудита действий поставщиков ИТ-услуг и других третьих лиц на администрируемых устройствах с целью контроля доступа внутренних и внешних поставщиков ИТ-услуг, владельцев учетных записей с расширенными правами и пользователей с повышенными рисками.

СКДПУ своевременно уведомляет Администратора о любых попытках подключения к устройствам, определенным как критичные, о неудачных попытках входа в СКДПУ или о невозможности автоматического входа с использованием заданной учетной записи.

СКДПУ предназначена для записи рабочих сеансов для последующего просмотра с целью аудита, управления инцидентами и проведения расследований.

СКДПУ анализирует все команды, вводимые в ходе сеансов SSH, в реальном времени и в случае обнаружения запрещенных строк отправляет соответствующее уведомление или разрывает сеанс подключения. Кроме того, СКДПУ использует технологию оптического распознавания символов (OCR) сеансов подключения к удаленному рабочему столу (RDP и VNC) в реальном времени, что упрощает процесс выявления причин сбоев или инцидентов безопасности.

СКДПУ поддерживает следующие протоколы передачи данных:

- HTTP (RFC 2616) и HTTPS (HTTP Over TLS – RFC 2818);
- SSH (RFC 4250 – 4256) и подсистемы указанного протокола;
- TELNET (RFC 854);
- RLOGIN (RFC 1282);
- произвольные TCP протоколы (RAWTCPIP) в рамках сессий SSH;
- RDP (v. 5 – 8.1) и VNC (на основе RFB 3.8, RFC 6143) в домене пользователя.

2.2 Требования к техническим и программным средствам

Минимальные характеристики программного и аппаратного обеспечения для развертывания сервера СКДПУ см. [таблица 2](#).

Таблица 2 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	интерфейс для подключения к LAN
ОС	ОС Astra Linux 1.6 Special Edition
Веб-сервер	HTTP Apache 2.4

Компонент	Описание
База данных	СУБД PostgreSQL версии 9.6
Брокер сообщений	RabbitMQ версии 3.6
Другое ПО	Интерпретаторы языка программирования Python 2.7, Python 3.5
	Библиотеки Python, обеспечивающие удовлетворение зависимостей для *.py части ПО

2.3 Требования к аппаратному обеспечению

АРМ пользователя СКДПУ должно быть оборудовано компьютером, обладающим следующим характеристиками:

Таблица 3 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ

Компонент	Описание
Процессор	архитектура x86-64 с тактовой частотой 2.6 ГГц
Оперативная память	6 ГБ
Жесткий диск	500 ГБ, SCSI или SATA
Интерфейсы	Интерфейс для подключения к LAN
Разрешение экрана	От 1280x1024

2.4 Требования к программному обеспечению

В состав программного обеспечения АРМ пользователя СКДПУ должна входить программа-клиент, предоставляющая возможность навигации и просмотра веб-ресурсов - веб-браузер.

Таблица 4 – Минимальные характеристики программного обеспечения АРМ пользователя СКДПУ

Компонент	Описание
Веб-обозреватель	Mozilla Firefox 80.0 и выше, Google Chrome 10.0 – 80.0, Microsoft Edge версии 44.18362.449.0. и выше . Обеспечивающий поддержку стандарта HTTP 1.1, TLS 1.2 и лучше
Брокер сообщений	Свободно распространяемый клиент для различных протоколов удаленного доступа, включая SSH, TELNET, RLOGIN. В качестве таких клиентов могут быть использованы «PuTTY», «WinSCP», «FileZilla»

Веб-браузер должен быть установлен перед началом работы с СКДПУ. Описание установки веб-браузера приведено в документации поставщика ПО.

3 УСТАНОВКА ПАРАМЕТРОВ X509

3.1 Настройка X509

Шаг 1. Необходимо войти в административную консоль и назначить права системного пользователя `root`:

```
$ sudo -i
```

Шаг 2. С правами «`root`» выполните следующую команду:

```
# WABX509Setup
```



Для выполнения данной команды СКДПУ должна иметь действительную лицензию с опцией X509.

Шаг 3. Подключитесь к порту 8082 в веб-интерфейсе СКДПУ (обратите внимание, он доступен через HTTP): `http://ip_address:8082/`

Шаг 4. Отобразится интерфейс настройки X509.

Шаг 5. Необходимо нажать кнопку **Start**.

Шаг 6. Система выполнит следующие шаги:

Шаг a. Остановка пользовательского веб-интерфейса СКДПУ;

Шаг b. Загрузка открытого ключа CA (сертификата);

Шаг c. Загрузка закрытого ключа веб-сервера;

Шаг d. Загрузка открытого ключа веб-сервера (сертификата);

Шаг e. Перезагрузка пользовательского веб-интерфейса;

Шаг f. Завершение настройки и отображение журнала событий Apache. Он не должен содержать событий типа «ошибка» (error).



Когда проводятся эти операции, пользовательский веб-интерфейс СКДПУ недоступен; однако это не влияет на прокси-серверы.

3.2 Настройка X509 в режиме высокой доступности СКДПУ

Сначала необходимо провести настройку как описано в разделе [Настройка X509](#)

Затем провести аналогичную настройку на кластере.



Необходимо настроить `x509` на обоих узлах и убедиться, что ключи и сертификаты идентичные.

4 АДМИНИСТРАТОРСКИЕ ФУНКЦИИ X509

Когда перезапускается пользовательский веб-интерфейс СКДПУ, страница аутентификации СКДПУ отобразит новую ссылку на завершение аутентификации с использованием сертификата SSL (см. [рисунок 1](#)).

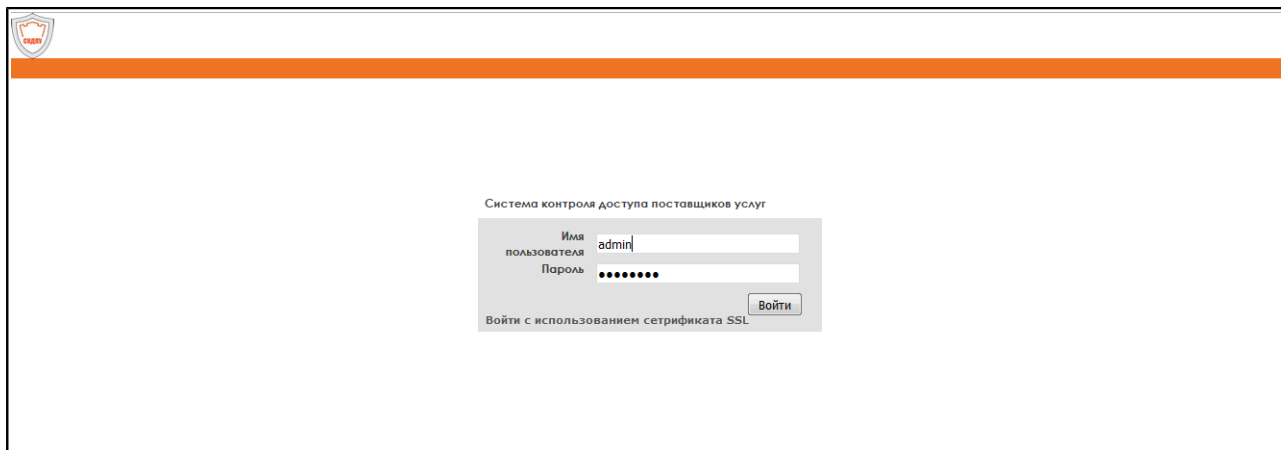


Рисунок 1 – Ссылка на сертификат SSL

Пользователи и администраторы могут войти, используя сохраненный сертификат, хранящийся или непосредственно в веб-браузере, или на токене.

4.1 Аутентификация пользователя

Для аутентификации пользователя в форме добавления/редактирования данных пользователя (пункт **Пользователи/Аккаунты** бокового меню) в поле **Сертификат DN** должно быть введено имя сертификата.

Например, чтобы связать пользователя с сертификатом необходимо ввести в поле следующее:

```
C=FR, ST=IDF, L=PARIS, O=MyCorp, CN=Olivier Hervieu
```

Когда сертификат используется, связанный пользователь будет аутентифицирован в СКДПУ.



1. Сертификаты должны быть подписаны тем же центром сертификации, что и сертификат веб-сервера;
2. Некоторые сертификаты включают в себя поле **Адрес электронной почты** в сертификате с отпечатком пальца. Замените значение этого поля на `/emailAddress =...`;
3. В сертификатах с отпечатком пальца поддерживается кодировка Unicode, если сертификат закодирован в UTF-8 согласно RFC2253, если нет, то поддерживается только стандартный код ASCII.

4.2 Управление списком отозванных сертификатов (CRL)

В Меню **Конфигурация/X509 Параметры** СКДПУ можно ввести адрес для направления списка отозванных сертификатов (CRL) (см. [рисунок 2](#)).

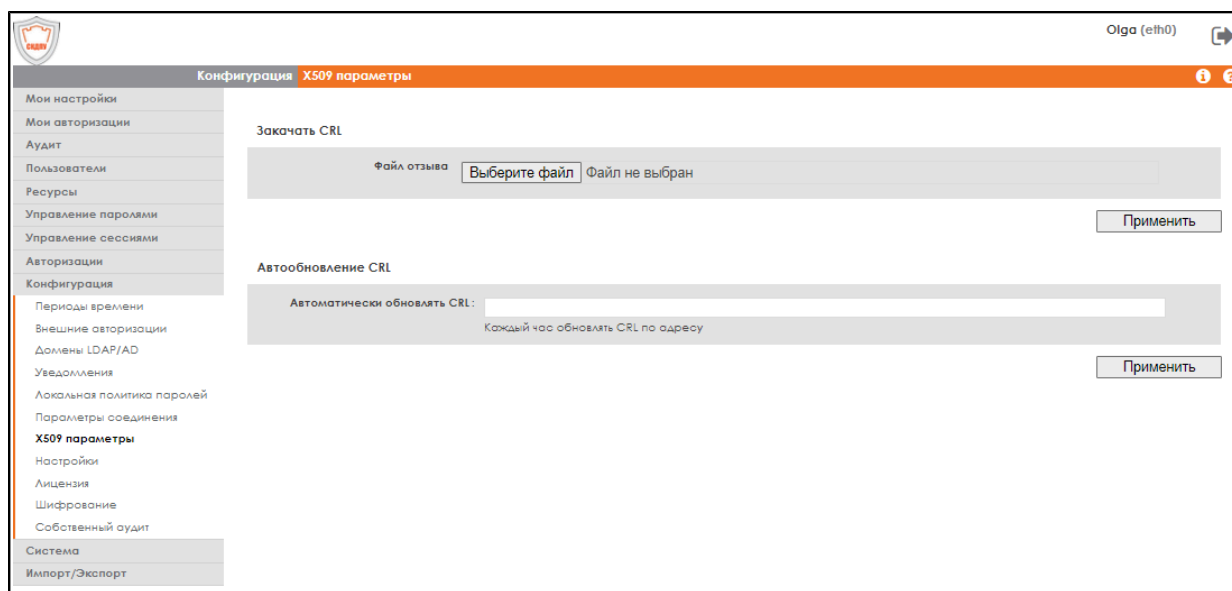


Рисунок 2 – Управление списком отозванных сертификатов



После загрузки CRL необходимо перезапустить пользовательский веб-интерфейс СКДПУ с помощью следующей команды:

```
# /etc/init.d/wabgui restart
```

5 АУТЕНТИФИКАЦИЯ X509

При аутентификации с помощью сертификата использование прокси-серверов меняется:

- Пользователь подключается к целевому устройству (через клиент RDP или SSH);
- Прокси-сервер запрашивает метод аутентификации через пользовательский веб-интерфейс;
- Если пользователь аутентифицирован по X509, система запрашивает подтверждение для входа в веб-интерфейс;
- Нажав кнопку **Войти**, пользователь автоматически аутентифицируется на целевом устройстве.



1. Для аутентификации с помощью учетной записи, пользователь вводит свой пароль на целевом устройстве.
2. Аутентификация X509 недоступна по протоколу SFTP.

6 ВЫХОД ИЗ РЕЖИМА X509

Для выхода из режима X509 введите команду:

```
# WABX509Unset
```

После этого генерируются новые автоматически подписанные сертификаты, и пользователи могут больше не использовать при входе свои сертификаты.

7 ОБЩИЕ СВЕДЕНИЯ

Сертификаты X509 поддерживаются расширением *Apache mod_ssl*. Используемые ключи конфигурации включают следующие:

- SSLEngine on;
- SSLOptions +StdEnvVars -ExportCertData;
- SSLProtocol all;
- SSLCipherSuite HIGH:MEDIUM;
- SSLCACertificateFile <CA public key in PEM format>;
- SSLCACertificatePath <CA path>;
- SSLCertificateFile <public part of the server certificate>;
- SSLCertificateFile <private part of the server certificate>;
- SSLCARevocationFile <revocation list>;
- SSLVerifyClient require;
- SSLVerifyClient require;

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

CRL	Certificate Revocation List — это список сертификатов, которые удостоверяющий центр пометил как отозванные.
CSV	Comma-Separated Values - текстовый формат, предназначенный для представления табличных данных.
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	HyperText Transfer Protocol Secure - расширение протокола HTTP, поддерживающее шифрование.
LAN	Local Area Network (локальная компьютерная сеть)
OCR	Optical character recognition - механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные - последовательность кодов, используемых для представления символов в компьютере (например, в текстовом редакторе).
RDP	Remote Desktop Protocol, протокол удаленного рабочего стола
RFB	Remote FrameBuffer — простой клиент-серверный сетевой протокол прикладного уровня для удалённого доступа к графическому рабочему столу компьютера, используемый в VNC.
RFC	Request for Comments, рабочее предложение – стандарты Интернета в части реализаций.
RLOGIN	Remote LOGIN (удалённый вход в систему)
SCP	Secure Copy Protocol — утилита и протокол копирования файлов между компьютерами, использующий, в отличие от утилиты RCP, в качестве транспорта не RSH, а зашифрованный SSH.
SFTP	SSH File Transfer Protocol — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.
SSH	Secure SHell (безопасная оболочка), протокол защищенной передачи данных
SSL	Secure Sockets Layer (уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей

	обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
SSO	Single Sign-On — технология, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации.
TCP	Transmission Control Protocol (TCP, протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета.
TELNET	TErminaL NETwork - сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP)
TLS	Transport Layer Security — протокол защиты транспортного уровня
VNC	Virtual Network Computing - система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).
APM	Автоматизированное рабочее место
ОС	Операционная система
ПО	Программное обеспечение

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Ссылка на сертификат SSL.....	9
Рисунок 2 – Управление списком отозванных сертификатов.....	10

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Основные возможности СКДПУ.....	3
Таблица 2 – Минимальные характеристики аппаратно-программного обеспечения сервера СКДПУ.....	5
Таблица 3 – Минимальные характеристики аппаратного обеспечения сервера СКДПУ.....	6
Таблица 4 – Минимальные характеристики программного обеспечения АРМ пользователя СКДПУ.....	6

