



Столыпинский  
вестник

Научная статья

Original article

УДК 004.732.056

**РЕАЛИЗАЦИЯ СЕРВЕРА VPN С РОССИЙСКИМИ  
КРИПТОАЛГОРИТМАМИ В ОТЕЧЕСТВЕННОЙ ЗАЩИЩЕННОЙ  
ОПЕРАЦИОННОЙ СИСТЕМЕ**

**IMPLEMENTATION OF A VPN SERVER WITH RUSSIAN CRYPTO  
ALGORITHMS IN A DOMESTIC SECURE OPERATING SYSTEM**

**Кладов В. Е.**, кандидат технических наук, доцент, доцент кафедры «Вычислительной техники и защиты информации» Уфимский университет науки и технологий Россия, г. Уфа [lisinatanya02@yandex.ru](mailto:lisinatanya02@yandex.ru)

**Лисина Т. Е.**, студент 4 курс, Институт информатики, математики и робототехники Уфимский университет науки и технологий Россия, г. Уфа [lisinatanya02@yandex.ru](mailto:lisinatanya02@yandex.ru)

**Kladov V. E.**, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Information Security Ufa University of Science and Technology, Ufa, Russia [lisinatanya02@yandex.ru](mailto:lisinatanya02@yandex.ru)

**Lisina T. E.**, 4th year student, Institute of Computer Science, Mathematics and Robotics Ufa University of Science and Technology, Ufa, Russia, [kokievagalia@mail.ru](mailto:kokievagalia@mail.ru)

**Аннотация.** Статья посвящена задаче перехода на отечественные решения в области защиты информации. При этом предлагается за счет использования защищенных операционных систем обойтись без

специализированных дополнительных средств защиты. В статье решаются вопросы реализации виртуальных частных сетей для безопасной связи корпоративных сетей и их отдельных сегментов с использованием российских криптоалгоритмов.

**Abstract.** The article is devoted to the problem of transition to domestic solutions in the field of information security. At the same time, it is proposed to do without specialized additional security tools by using secure operating systems. The article addresses the issues of implementing virtual private networks for secure communication of corporate networks and their individual segments using Russian crypto-algorithms.

**Ключевые слова:** виртуальные частные сети, сервер OpenVPN, асимметричная криптография, инфраструктура открытых ключей, защищенные операционные системы.

**Keywords:** virtual private networks, OpenVPN, asymmetric cryptography, public key infrastructure, secure operating systems.

Наиболее распространенной и наиболее защищенной операционной системой в нашей стране является Astra Linux Special Edition, которая имеет сертификат по классу А1, соответствует первому уровню доверия и может использоваться при обработке любой информации ограниченного доступа, вплоть до государственной тайны с грифом особой важности.

Для обеспечения защищенной связи между отдельными подразделениями предприятия, отдельными сегментами корпоративной сети необходимо использование виртуальных частных сетей VPN.

Они могут быть реализованы с помощью семейства протоколов IPSec с использованием утилиты strongswan, входящей в состав расширенного репозитория, либо с помощью такого инструмента как OpenVPN, который входит в основной репозиторий ОС.

В данной статье остановимся именно на OpenVPN. Он позволяет реализовать защищенные соединения как хост-шлюз, так и хост-хост, в том

числе и на компьютерах, находящихся за межсетевыми экранами, использующими NAT, при чем без необходимости изменения их настроек.

Настроим VPN соединение (рисунок 1).

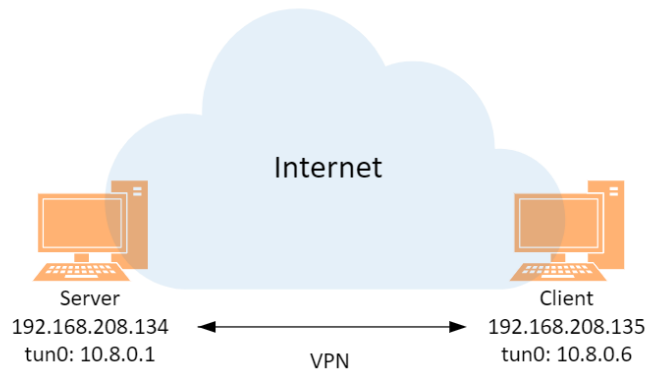


Рисунок 1 – Схема VPN-соединения

В данной статье остановимся на настройке сервера OpenVPN, а вопросы реализации клиента OpenVPN и реализации проверки защищенных каналов в операционной системе Astra Linux Special Edition рассмотрим в отдельной статье.

Пакет OpenVPN входит в дистрибутивы Astra Linux и устанавливается по умолчанию.

OpenVPN использует в своей работе динамически подключаемую библиотеку OpenSSL, которая также устанавливается при установке операционной системы. Это позволяет использовать весь набор криптоалгоритмов библиотеки OpenSSL.

В первую очередь нас интересуют отечественные криптоалгоритмы. Только они могут использоваться в Российской Федерации. Для их использования необходима установка пакета алгоритмов защитного преобразования ГОСТ libgost-astra.

Для быстрой настройки сервера OpenVPN необходимо установить утилиту командной строки astra-openvpn-server или графическую оснастку fly-admin-openvpn-server

```
apt-get install fly-admin-openvpn-server
```

 или

```
apt-get install astra-openvpn-server
```

При установке графической оснастки автоматически будет установлена и соответствующая упомянутая утилита командной строки.

```

root@astra-server:~# apt-get install astra-openvpn-server
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  easy-rsa libccid openssl openssl-pkcs11 pccsd
Следующие НОВЫЕ пакеты будут установлены:
  astra-openvpn-server easy-rsa libccid openssl openssl-pkcs11 pccsd
Обновлено 0 пакетов, установлено 6 новых пакетов, для удаления отмечено 0 пакетов, и 0 пакетов не обновлено.
Необходимо скачать 0 B/1 791 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 5 375 kB.
Хотите продолжить? [Д/н] g
Пол:1 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 easy-rsa all 3.0.6-1 [37,9 kB]
Пол:2 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 astra-openvpn-server amd64 0.4.24 [91,0 kB]
Пол:3 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 libccid amd64 1.4.34-1 [337 kB]
Пол:4 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 openssl-pkcs11 amd64 0.21.0-1 [878 kB]
Пол:5 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 openssl amd64 0.21.0-1 [355 kB]
Пол:6 cdrom://OS Astra Linux 1.7.2 1.7_x86-64 DVD 1.7_x86-64/main amd64 pccsd amd64 1.0.24-1 [92,6 kB]
Выбор ранее не выбранного пакета easy-rsa.
(Чтение базы данных ... на данный момент установлено 190455 файлов и каталогов.)
Подготовка к распаковке .../0-easy-rsa_3.0.6-1_all.deb ...
    
```

Рисунок 2 – Установка инструмента командной строки astra-openvpn-server

При этом автоматически будет установлен и настроен пакет российских криптоалгоритмов libgost-astra.

Посмотреть полную информацию по работе утилиты можно по команде:  
astra-openvpn-server -h

```

root@astra-server:~# astra-openvpn-server -h
Варианты команд:
astra-openvpn-server -h|--help
astra-openvpn-server -v|--version
astra-openvpn-server --show-ciphers
astra-openvpn-server start [server "IP MASK"] [port PORT] [cipher CIPHER] [nic имя_сетевого_интерфейса] [cert путь_к_файлу] [ca путь_к_файлу] [key путь_к_файлу] [dh путь_к_файлу] [tls-auth путь_к_файлу]
astra-openvpn-server start [server "IP MASK"] [port PORT] [cipher CIPHER] [nic имя_сетевого_интерфейса] [KEY_COUNTRY RU] [KEY_PROVINCE MO] [KEY_CITY Moscow] [KEY_ORG Astra] [KEY_EMAIL none] [KEY_OU OS] [KEY_NAME User]
astra-openvpn-server start [server "IP MASK"] [port PORT] [cipher CIPHER] [nic имя_сетевого_интерфейса] [EASYSRSA_DN cn_onlyjorg] [EASYSRSA_REQ_COUNTRY RU] [EASYSRSA_REQ_PROVINCE MO] [EASYSRSA_REQ_CITY Moscow] [EASYSRSA_REQ_ORG none] [EASYSRSA_REQ_EMAIL none] [EASYSRSA_REQ_OU none] [EASYSRSA_REQ_CN имя_клиента]
astra-openvpn-server stop
astra-openvpn-server status
astra-openvpn-server rebuild-server-certs
astra-openvpn-server client имя_пользователя [nic имя_сетевого_интерфейса] [KEY_COUNTRY RU] [KEY_PROVINCE MO] [KEY_CITY Moscow] [KEY_ORG Astra] [KEY_EMAIL none] [KEY_OU OS] [KEY_NAME USER]
astra-openvpn-server client имя_пользователя [nic имя_сетевого_интерфейса] [EASYSRSA_DN cn_onlyjorg] [EASYSRSA_REQ_COUNTRY RU] [EASYSRSA_REQ_PROVINCE MO] [EASYSRSA_REQ_CITY Moscow] [EASYSRSA_REQ_ORG none] [EASYSRSA_REQ_EMAIL none] [EASYSRSA_REQ_OU none] [EASYSRSA_REQ_CN имя_клиента]
astra-openvpn-server revoke имя_пользователя
astra-openvpn-server get имя_параметра
astra-openvpn-server del имя_параметра
astra-openvpn-server set имя_параметра значение_параметра

Информационные команды.
    
```

Рисунок 3 – справка astra-openvpn-server

Просмотреть версию сервера OpenVPN и поддерживаемые криптоалгоритмы можно с помощью команд:

astra-openvpn-server -v

astra-openvpn-server --show-ciphers

```

root@astra-server:~# astra-openvpn-server -v
astra-openvpn-server: Версия 0.4.22
root@astra-server:~# astra-openvpn-server --show-ciphers
grasshopper-cbc
AES-256-GCM
AES-256-CBC
AES-128-CBC
root@astra-server:~# █
    
```

Рисунок 4 – версия и поддерживаемые криптоалгоритмы

Так как пакет libgost-astra установлен, то сервер OpenVPN будет автоматически настроен на работу с отечественным алгоритмом симметричного шифрования "Кузнечик" (grasshopper-cbc), по ГОСТ Р34.12-2015.

Для запуска сервера OpenVPN используем команду  
astra-openvpn-server start.

```

root@astra-server:~# astra-openvpn-server start
Предупреждение:Файл "/etc/openvpn/keys/server.crt" не найден
Предупреждение:Файл "/etc/openvpn/keys/ca.crt" не найден
Предупреждение:Файл "/etc/openvpn/keys/server.key" не найден
Предупреждение:Файл "/etc/openvpn/keys/dh2048.pem" не найден
Предупреждение:Файл "/etc/openvpn/keys/ta.key" не найден
Сетевой интерфейс по умолчанию определён как "eth0"
Сервис привязывается к адресу "192.168.208.134" сетевой карты "eth0"
Файл конфигурации /etc/openvpn/server.conf не обнаружен, создаём новый.
Файл со стандартными настройками сервера openvpn успешно распакован в /etc/openvpn/server.conf. Вносим исправления в стандартные н
астройки
Предупреждение:Вставка "mode server\n\n" неpeg "# Which local IP" в файле "/etc/openvpn/server.conf"
Предупреждение:Замена ";user nobody" на "user nobody" в файле "/etc/openvpn/server.conf"
Предупреждение:Замена ";group nogroup" на "group nogroup" в файле "/etc/openvpn/server.conf"
Предупреждение:Замена "#net.ipv4.ip_forward=1" на "net.ipv4.ip_forward=1" в файле "/etc/sysctl.conf"
Вносим исправления в настройки межсетевого экрана
Настраиваем правила для сетевого интерфейса eth0
Предупреждение:Вставка "# START OPENVPN RULES\n" неpeg "# Don't delete these" в файле "/etc/ufw/before.rules"
Предупреждение:Вставка "# NAT table rules\n" неpeg "# Don't delete these" в файле "/etc/ufw/before.rules"
Предупреждение:Вставка "*nat\n" неpeg "# Don't delete these" в файле "/etc/ufw/before.rules"
Предупреждение:Вставка ":POSTROUTING ACCEPT [0:0]\n" неpeg "# Don't delete these" в файле "/etc/ufw/before.rules"
Предупреждение:Вставка "# Allow traffic from OpenVPN client to eth0\n" неpeg "# Don't delete these" в файле "/etc/ufw/bef
ore.rules"
Предупреждение:Вставка "--A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE\n" неpeg "# Don't delete these" в файле "/etc/ufw/bef
ore.rules"
    
```

Рисунок 5 – запуск службы astra-openvpn-server

Просмотрев статус службы, можно убедиться, что она работает.

```

root@astra-server:~# astra-openvpn-server status
• openvpn.service - OpenVPN service Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled) Active:
active (exited) since Tue 2024-03-12 01:35:17 +05; 35s ago Process: 3711 ExecStart=/bin/true (code=exited, status=0/SUCCESS) Main
PID: 3711 (code=exited, status=0/SUCCESS) map 12 01:35:17 astra-server systemd[1]: Starting OpenVPN service... map 12 01:35:17 ast
ra-server systemd[1]: Started OpenVPN service.
root@astra-server:~#
    
```

Рисунок 6 – статус службы astra-openvpn-server

При запуске сервера OpenVPN в рабочей папке пакета /etc/openvpn будут созданы:

- файл server.conf конфигурации openvpn;
- подпапка openvpn-certificates с настройками локального удостоверяющего центра (УЦ);
- подпапка keys с ключами;
- сертификат открытого ключа (ОК) УЦ ca.crt;
- сертификат ОК сервера server.crt;
- личный ключ сервера: server.key;

- файл параметров Диффи-Хеллмана для авторизации пользователей dh2048.pem
- файл дополнительной аутентификации TLS ta.key;
- файл списка отзыва сертификатов crl.pem (при выполнении отзыва сертификатов).

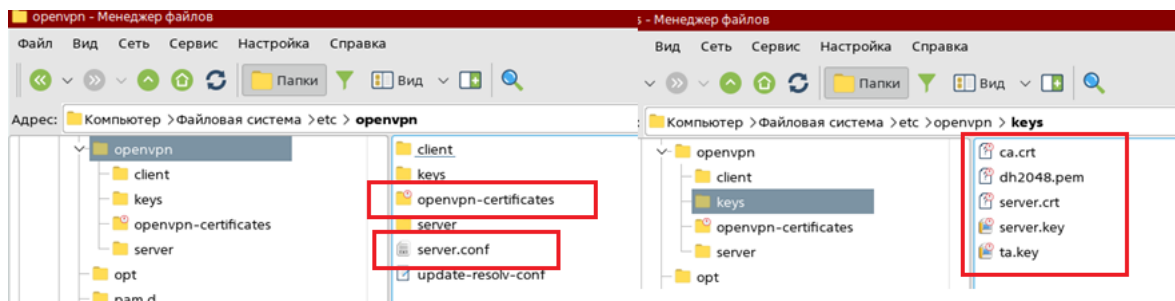


Рисунок 7 – созданные файлы и каталоги

Также при первом запуске службы будут выполнены настройки межсетевого экрана и операционной системы для работы OpenVPN как стандартной системной службы с автоматическим запуском при включении компьютера.

Рассмотрим настройки конфигурационного файла сервера:

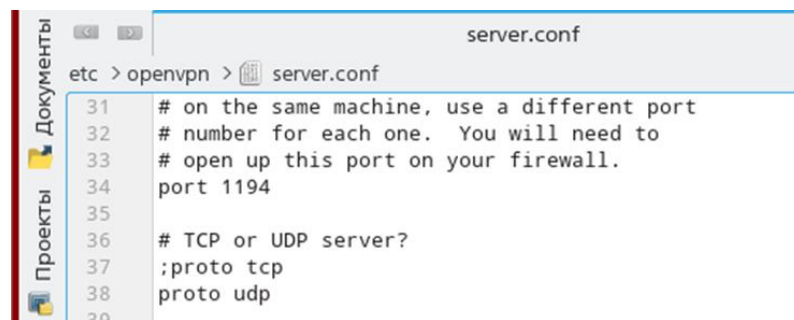


Рисунок 8 – Используемые OpenVPN протокол и порт

Используемый протокол транспортного уровня и используемый порт задаются в строчках 34, 37, 38. UDP рекомендуется использовать при необходимости более быстрой передачи данных, а TCP – когда, требуется более надежное соединение и меньшая вероятность блокировки трафика. Портами по умолчанию будут соответственно 1194 и 443

```

server.conf
etc > openvpn > server.conf
52 # unless you partially or fully disable
53 # the firewall for the TUN/TAP interface.
54 ;dev tap
55 dev tun
    
```

Рисунок 9 – используемые сетевые устройства

В строке 55 указано используемое сетевое устройство tun. TUN и TAP — разные режимы работы сетевых интерфейсов, используемых в VPN приложениях, таких как OpenVPN. TUN работает на сетевом уровне IP, позволяет создавать маршрутизированные VPN и передавать IP-трафик, а TAP работает на канальном уровне, поддерживает передачу всех типов данных, подобно физическому Ethernet-адаптеру, и может создавать мост между удаленными сетями.

```

server.conf
etc > openvpn > server.conf
79 # (see "pkcs12" directive in man page).
80 ca /etc/openvpn/keys/ca.crt
81 cert /etc/openvpn/keys/server.crt
82 key /etc/openvpn/keys/server.key
83
84 # Diffie hellman parameters.
85 # Generate your own with:
86 # openssl dhparam -out dh2048.pem 2048
87 dh /etc/openvpn/keys/dh2048.pem
    
```

Рисунок 10 – месторасположение ключей

В строках 80–82 прописываем путь до сертификата открытого ключа УЦ и сервера OpenVPN, и также до личного ключа сервера.

```

server.conf
etc > openvpn > server.conf
100 # Each client will be able to reach the server
101 # on 10.8.0.1. Comment this line out if you are
102 # ethernet bridging. See the man page for more info.
103 server 10.8.0.0 255.255.255.0
    
```

Рисунок 11 – IP-адрес сервера OpenVPN

В строке 103 указываем серверный режим работы и VPN подсеть, из которой OpenVPN будет выделять адреса клиентам, при этом в данном случае серверу OpenVPN будет отведен адрес 10.8.0.1.

```

server.conf
etc > openvpn > server.conf
109 # previously assigned.
110 ifconfig-pool-persist /var/log/openvpn/ipp.txt
    
```

Рисунок 12 – месторасположение файла IP адресов клиентов

В строке 110 прописан путь к файлу с долговременными ассоциации IP-адресов клиентов OpenVPN, что обеспечивает постоянство IP-адресов, назначенных клиентам при каждом их подключении к серверу OpenVPN.

```

server.conf
etc > openvpn > server.conf
244 # The second parameter should be '0'
245 # on the server and '1' on the clients.
246 tls-auth /etc/openvpn/keys/ta.key 0
    
```

Рисунок 13 – месторасположение файла ta.key

В строке 246 прописан путь к файлу дополнительной аутентификации TLS, который используется для усиления безопасности соединения путем применения дополнительного уровня аутентификации на транспортном уровне модели OSI (TLS).

```

server.conf
etc > openvpn > server.conf
253 # See also the ncp-cipher option in the manpage
254 cipher grasshopper-cbc
255 ncp-disable
    
```

Рисунок 14 -алгоритм шифрования трафика VPN соединения

В строке 254 указываем алгоритм шифрования трафика VPN соединения. В соответствии с законодательством используем современный российский алгоритм симметричного шифрования «Кузнечик» по ГОСТ Р 34.12-2015, обозначаемый как grasshopper-cbc.

ncp-disable в 255 строке указывает на отключение использования Next-Generation Encryption (NGE) или Next-Gen Crypto Proposal (NCP).



```

server.conf
etc > openvpn > server.conf
277 user nobody
278 group nogroup
279
280 # The persist options will try to avoid
281 # accessing certain resources on restart
282 # that may no longer be accessible because
283 # of the privilege downgrade.
284 persist-key
285 persist-tun
    
```

Рисунок 15 – имена, используемые для процесса OpenVPN

Строки 277 и 278 устанавливают пользователя и группу, от имени которых будет выполняться процесс OpenVPN. Рекомендуется использовать пользователя nobody с минимальными привилегиями для запуска сервисов или процессов с минимальными привилегиями доступа к ресурсам системы. и соответствующую ему группу nogroup.

Опции persist key и persist tun в строке 284–285 сохраняет долгосрочные ключи и параметры устройства TUN/TAP даже при перезапуске сервера или клиента.

```

308 # 9 is extremely verbose
309 verb 3
310
311 # Silence repeating messages. At most 20
312 # sequential messages of the same message
313 # category will be output to the log.
314 ;mute 20
315
316 # Notify the client that when the server restarts so it
317 # can automatically reconnect.
318 explicit-exit-notify 1
319 local 192.168.208.134
320
321 crl-verify /etc/openvpn/keys/crl.pem
    
```

Рисунок 16 – детализация аудита

В строке 309 указан 3 уровень подробности вывода информации в журнале OpenVPN во время работы сервера или клиента. Чем выше число, тем более подробный вывод. Значение 3 обычно предоставляет довольно подробный вывод, что делает его удобным для отладки и просмотра основной информации о соединении в журналах OpenVPN.

Значение «1» для параметра explicit-exit-notify в строке 318 устанавливает режим отправки явных уведомлений об отключении клиента VPN серверу.

Строка 319 указывает на каком локальном IP-адресе ожидать входящие подключения.

Строка 321 указывает путь к файлу отзыва сертификатов.

Для корректной работы OpenVPN необходимо на сервере включить маршрутизацию транзитных IP-пакетов или IP-форвардинг, установив в 1 параметр `net.ipv4.ip_forward`, в файле `/etc/sysctl.conf` и сохранив изменения.

```

sysctl.conf
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
    
```

Рисунок 17 – включение маршрутизации транзитных IP-пакетов

Для реализации виртуальной частной сети и обеспечения возможности подключения клиентов к серверу OpenVPN необходимо создать для них ключи.

Создание клиентского набора ключей осуществляется на сервере OpenVPN с помощью опции `client` утилиты командной строки `astra-openvpn-server`:

`astra-openvpn-server client <имя_клиента>`

```

root@astra-server:~# astra-openvpn-server client lisina
Сетевой интерфейс по умолчанию определён как "eth0"
Сервис привязывается к адресу "192.168.200.134" сетевой карты "eth0"
Обнаружен ранее созданный файл конфигурации /etc/openvpn/server.conf.
Генерация ключа и сертификата для клиента lisina
В конфигурации клиента заданы: сервер 192.168.200.134, порт 1194, алгоритм защитного преобразования grasshopper-cbc
/etc/openvpn/clients_keys/lisina
root@astra-server:~#
    
```

Рисунок 18 – создание клиентского комплекта файлов

При ее выполнении в подпапке клиентских ключей для OpenVPN `/etc/openvpn/clients-keys` будет создана подпапка с именем указанного клиента, куда будут помещены созданные для клиента файлы личного ключа `<имя_клиента>.key` и сертификата его ОК `<имя_клиента>.cert`, подписанного УЦ.

Дополнительно в эту же папку будут скопированы необходимые для клиента файл сертификата УЦ (по умолчанию `ca.crt`) и дополнительной аутентификации TLS (`ta.key`).

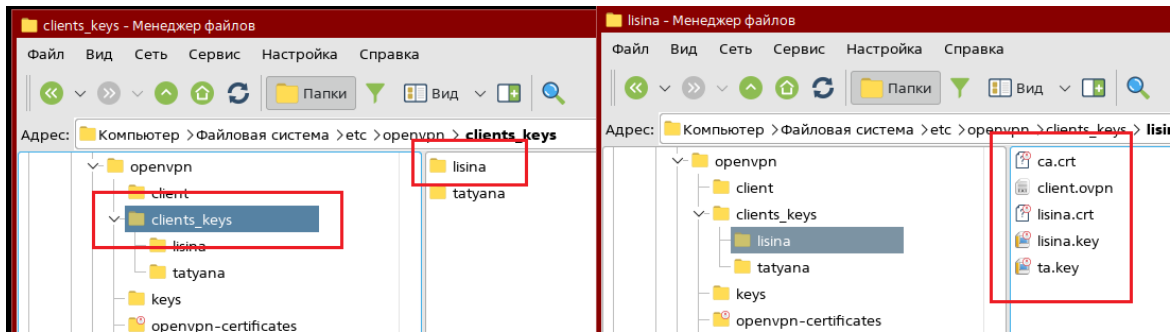


Рисунок 19 – клиентский комплект файлов

Для запрета подключения клиента можно отозвать сертификат его ОК.  
 astra-openvpn-server revoke <имя\_клиента>,

При этом:

- сертификат клиента в базе данных УЦ будет помечен как «отозванный»;
- в каталоге etc/openvpn/keys появится список отозванных сертификатов и произойдет перезагрузка сервера OpenVPN

```
root@astra-server:~# astra-openvpn-server revoke tatyana
Сетевой интерфейс по умолчанию определен как "eth0"
Сервис привязывается к адресу "192.168.208.134" сетевой карты "eth0"
Обнаружен ранее созданный файл конфигурации /etc/openvpn/server.conf.
root@astra-server:~#
```

Рисунок 20 – отзыв сертификата для клиента tatyana

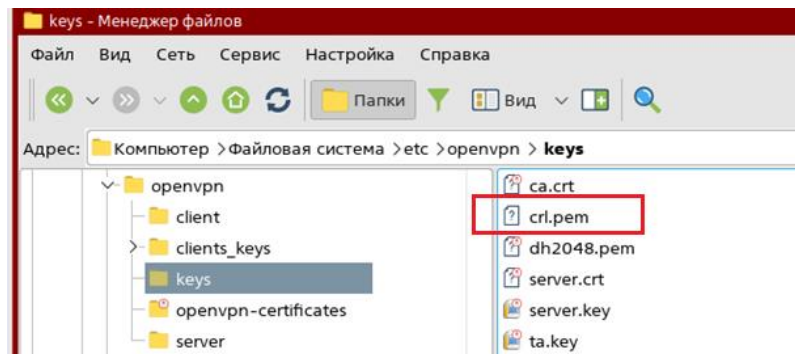


Рисунок 21 – файл списка отозванных сертификатов

Полную замену ключей и сертификатов сервера и УЦ можно произвести с помощью опции rebuild-server-certs команды astra-openvpn-server, которая останавливает службу, удаляет все сертификаты сервера и клиентов, повторно генерирует все сертификаты сервера и запускает его, при этом имена файлов сертификатов сервера берутся из конфигурационного файла сервера.

Таким образом в данной статье рассмотрены различные аспекты настройки сервера VPN, использующего российские криптоалгоритмы в отечественной защищенной операционной системе Astra Linux Special Edition

**Использованные источники:**

1. Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION» Руководство администратора. Часть 1.
2. OpenVPN // Справочный центр Astra Linux URL: <https://wiki.astralinux.ru/display/doc/OpenVPN> (дата обращения: 21.11.2023).

**The sources used:**

1. Special purpose operating system "ASTRA LINUX SPECIAL EDITION" Administrator's Guide. Part 1.
2. OpenVPN // Astra Linux Help Center URL: <https://wiki.astralinux.ru/display/doc/OpenVPN> (date of access: 11/21/2023).

© Кладов В. Е., Лисина Т. Е., 2024 Научный сетевой журнал «Столыпинский вестник» №5/2024.

**Для цитирования:** Кладов В. Е., Лисина Т. Е. РЕАЛИЗАЦИЯ СЕРВЕРА VPN С РОССИЙСКИМИ КРИПТОАЛГОРИТМАМИ В ОТЕЧЕСТВЕННОЙ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ Столыпинский вестник. №5/2024.