



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.45

РАЗВЕРТЫВАНИЕ VPN-СЕРВИСА С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННОГО АЛГОРИТМА ШИФРОВАНИЯ "МАГМА" В ОПЕРАЦИОННОЙ СИСТЕМЕ «АЛЬТ»

¹ Алиев Э.Э., Грачёв Р.И.

ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ И.М.

ГУБКИНА" Москва, Россия, (119296, город Москва, Ленинский пр-кт, д. 65 к. 1), e-mail:

¹elbruspr@mail.ru

В ходе данной статьи рассматривается процесс развертывания VPN-сервиса для корпоративных нужд с использованием отечественных алгоритмов шифрования ГОСТ (ГОСТ 34.12-2018 [1]) на платформе ОС Альт. Особое внимание уделено техническим аспектам реализации защищенного соединения, настройке алгоритмов "Магма", а также требованиям к инфраструктуре и инструментам. Статья направлена на начинающих специалистов, стремящихся понять и внедрить технологии безопасного обмена данными с учетом современных нормативных требований. Материал ориентирован на законное использование VPN для обеспечения защищенного удаленного доступа, без упоминания и анализа использования сервисов для обхода блокировок.

Ключевые слова: VPN, корпоративные сети, ГОСТ, ГОСТ 34.12-2018, алгоритм Магма, защищенный удаленный доступ, ОС Альт, шифрование.

DEPLOYMENT OF A VPN SERVICE USING THE RUSSIAN ENCRYPTION ALGORITHM 'MAGMA' IN ALT LINUX

¹ Aliev E.E., Grachev R.I.

GUBKIN RUSSIAN STATE UNIVERSITY OF OIL AND GAS (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (119296, Moscow, Leninsky pr-kt, 65 k. 1), e-mail:

¹elbruspr@mail.ru

This study explores the deployment of a VPN service for corporate needs using domestic encryption algorithms GOST (GOST 34.12-2018 [1]) on the Alt OS platform. Particular emphasis is placed on the technical aspects of implementing a secure connection, configuring the Magma algorithms, as well as the requirements for infrastructure and tools. The article is aimed at beginner specialists striving to understand and implement technologies for secure data exchange in compliance with modern regulatory requirements. The material focuses on the lawful use of VPNs to ensure secure remote access, without referencing or analyzing the use of services for bypassing restrictions.

Keywords: VPN, corporate networks, GOST, GOST 34.12-2018, Magma algorithm, secure remote access, Alt OS, encryption.

В условиях стремительного развития цифровых технологий и увеличения объемов передаваемой информации обеспечение безопасности данных становится приоритетной задачей для корпоративных сетей. Особенно актуально это для организаций, обрабатывающих конфиденциальные сведения, где защита от несанкционированного доступа и утечек информации является критически важной. В таких случаях на помощь приходят VPN-сервисы,

создающие защищенные каналы связи между удаленными пользователями и корпоративными ресурсами.[1]

Применение VPN в корпоративной среде направлено на обеспечение защищенного удаленного доступа сотрудников к внутренним системам компании. Это позволяет безопасно передавать данные через общедоступные сети, минимизируя риски перехвата или несанкционированного доступа. Важно отметить, что использование VPN в данном контексте полностью соответствует законодательным нормам и направлено исключительно на защиту информации.[2]

Согласно приказу Роскомнадзора, вступившему в силу 30 ноября 2024 года, распространение научной, научно-технической и статистической информации о VPN-сервисах, используемых для обхода блокировок, признано запрещенным на территории России до 1 сентября 2029 года. Исключение сделано только для информации о VPN, предназначенных для обеспечения защищенного удаленного доступа. [3] Таким образом, обсуждение и разработка VPN-сервисов в рамках законного использования для защиты корпоративных данных остаются допустимыми и необходимыми.

Объектом данного исследования является процесс развертывания VPN-сервиса с использованием отечественных алгоритмов шифрования ГОСТ 34.12–2018 на платформе ОС Альт.

Предметом исследования выступают технические аспекты реализации защищенного соединения, включая настройку алгоритма "Магма", а также требования к инфраструктуре и инструментам.

Целью работы является разработка методики внедрения VPN-сервиса для корпоративных нужд, соответствующей современным нормативным требованиям и обеспечивающей высокий уровень безопасности данных.

Статья направлена на начинающих специалистов, стремящихся понять и внедрить технологии безопасного обмена данными в соответствии с современными нормативными требованиями. Материал ориентирован исключительно на законное использование VPN для обеспечения защищенного удаленного доступа, без упоминания и анализа применения сервисов для обхода блокировок.[4]

ГОСТ 34.12-2018, введенный в действие 1 июня 2019 года, устанавливает стандарты для блочных шифров, применяемых в криптографической защите информации [1]. Стандарт описывает базовый блочный шифр: с длиной блока 128 бит и 64 бита, известный как "Магма". Этот алгоритм обеспечивает конфиденциальность, аутентичность и целостность данных при их передаче, обработке и хранении в автоматизированных системах.

Алгоритм "Магма" представляет собой блочный шифр с длиной блока 64 бита и длиной ключа 256 бит. Он является развитием алгоритма, ранее описанного в ГОСТ 28147-89, с уточненной таблицей подстановок для нелинейного биективного преобразования, что повышает его криптографическую стойкость. [5]

Данный алгоритм нашел широкое применение в различных системах защиты информации, соответствуя современным требованиям информационной безопасности.

Законное использование VPN в корпоративных сетях: Виртуальные частные сети (VPN) являются важным инструментом для обеспечения защищенного удаленного доступа к корпоративным ресурсам. Они создают зашифрованные каналы связи между устройствами, что позволяет передавать данные через общедоступные сети с сохранением их конфиденциальности и целостности. В корпоративной среде VPN используются для подключения удаленных сотрудников, объединения офисов и защиты внутренней коммуникации. [6]

Согласно российскому законодательству, использование VPN для обеспечения безопасности корпоративной информации, шифрования каналов связи внутри компании и удаленного доступа сотрудников к внутренним ресурсам является законным. Однако применение VPN для доступа к ресурсам, заблокированным на территории России, запрещено. С 2024 года VPN-провайдеры обязаны фильтровать подобные запросы. [7]

Описание процедуры исследования:

Для обеспечения защищенного удаленного доступа к корпоративным ресурсам с использованием отечественных алгоритмов шифрования, соответствующих ГОСТ 34.12-2018, на платформе ОС Альт, была проведена следующая процедура:

1. Подготовка среды. На сервере, функционирующем под управлением ОС Альт, установлены необходимые программные компоненты для организации VPN-сервиса. Особое внимание уделено обеспечению поддержки отечественных криптографических алгоритмов, в частности алгоритма "Магма".

2. Настройка криптографических параметров. В конфигурационных файлах VPN-сервиса определены параметры шифрования, соответствующие требованиям ГОСТ 34.12-2018 [1]. Для этого использованы специализированные библиотеки и модули, обеспечивающие реализацию алгоритма "Магма". [8]

3. Создание и установка сертификатов. Сгенерированы криптографические ключи и сертификаты, необходимые для аутентификации и установления защищенного соединения. При этом применены отечественные стандарты формирования электронной подписи и инфраструктуры открытых ключей.

4. Конфигурация VPN-сервиса. Выполнена настройка VPN-сервиса для работы с протоколами, поддерживающими отечественные алгоритмы шифрования. Обеспечена совместимость с клиентскими устройствами, использующими аналогичные криптографические стандарты.

5. Тестирование и верификация. Проведено тестирование установленного VPN-сервиса на предмет корректности работы, устойчивости соединения и соответствия требованиям безопасности. Результаты тестирования задокументированы и проанализированы для выявления возможных улучшений.

Данная процедура направлена на создание надежного и соответствующего нормативным требованиям VPN-сервиса, обеспечивающего защищенный удаленный доступ к корпоративным ресурсам с использованием отечественных криптографических стандартов.

Практическая часть

Установка программного обеспечения: для развертывания VPN-сервиса на ОС Альт были использованы:

- OpenVPN версии 2.5.7 — для реализации VPN-туннелей.
- OpenSSL версии 1.1.1 — для поддержки алгоритма ГОСТ.

Алгоритм развертывания VPN-сервиса на ОС Альт с использованием алгоритма шифрования "Магма":

1. Подготовка среды и установка необходимых компонентов:

Выполнена установка пакетов OpenVPN версии 2.5.7 и OpenSSL версии 1.1.1, обеспечивающих поддержку шифрования ГОСТ. Команда для установки:

```
host-15 ~ # apt-get install openvpn
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут ОБНОВЛЕНЫ:
  openvpn
1 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 660 не будет обновле
но.
Необходимо получить 492кВ архивов.
После распаковки будет освобождено 25,9кВ дискового пространства.
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64/classic openvpn 2.6.12-alt1:p10+
354626.100.1.1@1723033839 [492кВ]
Получено 492кВ за 0s (8166кВ/s).
Совершаем изменения...
Подготовка... ##### [100%]
Обновление / установка...
1: openvpn-2.6.12-alt1 ##### [ 50%]
Очистка / удаление...
2: openvpn-2.5.6-alt1 ##### [100%]
Завершено.
```

Рисунок 1 - Установка OpenVPN.

```
host-15 ~ # apt-get install openssl-gost-engine
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  openssl-gost-engine
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 660 не будет обновле
но.
Необходимо получить 207кВ архивов.
После распаковки потребуется дополнительно 384кВ дискового пространства.
Получено: 1 http://ftp.altlinux.org p10/branch/x86_64/classic openssl-gost-engine 1.1.
0.3.0.255.ge3af41d.p1-alt4:p10+319781.100.2.1@1684411629 [207кВ]
Получено 207кВ за 0s (4313кВ/s).
Совершаем изменения...
Подготовка... ##### [100%]
Обновление / установка...
1: openssl-gost-engine-1.1.0.3.0.255.ge3##### [100%]
Завершено.
```

Источник: анализ авторов

Рисунок 2 - Установка шифров ГОСТ.

Источник: анализ авторов

```
host-15 ~ # control openssl-gost enabled
```

Рисунок 3 - Активация ГОСТ шифров для OpenSSL.

Источник: анализ авторов

2. Проверка доступности алгоритмов шифрования "Магма":

Убедились в наличии поддержки алгоритмов magma-cbc и magma-ctr с помощью команды: (Рисунок 4):

```
host-15 ~ # openssl list -cipher-algorithms | grep magma
magma-cbc
magma-ctr
```

Рисунок 4 – Провераем корректность установки ГОСТ шифров.

Источник: анализ авторов

Данный этап подтвердил, что алгоритмы magma-cbc и magma-ctr доступны для использования.

3. Генерация ключей и сертификатов.

Для обеспечения безопасности соединения были сгенерированы сертификаты для сервера и удостоверяющего центра (CA). Генерация выполнялась с использованием OpenSSL через алгоритм шифрования «Магма»:

1. Создание ключа удостоверяющего центра (Рисунок 5):

```
host-15 ~ # openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCB -out ca.key
host-15 ~ # openssl req -new -x509 -md gost12_256 -days 365 -key ca.key -out ca.cer \
> -subj "/C=RU/ST=Russia/L=Moscow/O=SuperPlat/OU=SuperPlat CA/CN=SuperPlat CA Root"
host-15 ~ # openssl x509 -in ca.cer -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      3f:f3:bc:c3:53:87:5a:13:10:e6:70:e3:ae:47:81:e5:14:7c:fd:d4
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
    Issuer: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat CA, CN = SuperPlat CA R
oot
  Validity
    Not Before: Nov 12 21:18:25 2024 GMT
    Not After : Nov 12 21:18:25 2025 GMT
  Subject: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat CA, CN = SuperPlat CA
Root
  Subject Public Key Info:
    Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus
    Public key:
      X: C7CC2B7767A1FD70218A94481FA9C1D9687915E243429B42655CDC2F12BA7737
      Y: BB1ACC8D544594C15AB83A9E8145151ECD538CE0289A452D24EAF6808DA119D0
    Parameter set: GOST R 34.10-2012 (256 bit) ParamSet B
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      FD:CF:FA:EB:9B:4D:E7:3A:D9:66:2C:47:AA:90:19:91:22:6E:7D:94
    X509v3 Authority Key Identifier:
      keyid:FD:CF:FA:EB:9B:4D:E7:3A:D9:66:2C:47:AA:90:19:91:22:6E:7D:94

    X509v3 Basic Constraints:
      CA:TRUE
  Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
  8d:59:0e:e8:1e:b2:2c:b8:af:d6:cf:64:25:8f:84:5b:05:62:
  30:7e:75:2d:7c:22:0f:f9:6a:ac:9e:4d:fe:88:e2:1d:9f:8d:
  4f:32:ea:18:6d:1c:68:0a:2a:31:c9:7a:19:e0:46:93:1a:46:
  4f:d0:e3:ff:5e:dd:2a:c2:ed:95
host-15 ~ #
```

Рисунок 5 - Проверка созданного сертификата сервера.

2. Создание ключа и сертификата клиента (Рисунок 6):

```
host-15 ~ # openssl genkey -algorithm gost2012 256 -pkeyopt paramset:TCB -out client.key
host-15 ~ # openssl req -new -x509 -md gost12 256 -days 365 -key client.key -out client.cer -subj "/
C=RU/ST=Russia/L=Moscow/O=SuperPlat/OU=SuperPlat Client/CN=SuperPlat Client Root"
host-15 ~ # openssl x509 -in client.cer -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      38:ba:3c:25:26:df:1a:6d:d4:ce:35:bf:3b:a5:1c:d0:30:26:b9:2d
    Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
    Issuer: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat Client, CN = SuperPlat
Client Root
  Validity
    Not Before: Nov 12 21:23:49 2024 GMT
    Not After : Nov 12 21:23:49 2025 GMT
  Subject: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat Client, CN = SuperPlat
Client Root
  Subject Public Key Info:
    Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus
    Public key:
      X:A3BAC683A3B75F6C6966B9CBB34671EDB17622F9F20307AE4D04130544918762
      Y:BBFE1DE5F38D3288B5304E31608AF16445DF1B9352A73E84C6DB61BDED8CC7A8
    Parameter set: GOST R 34.10-2012 (256 bit) ParamSet B
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      DD:A8:0C:11:4E:20:8F:20:8B:F7:33:6E:40:46:24:D9:CA:45:B3:78
    X509v3 Authority Key Identifier:
      keyid:DD:A8:0C:11:4E:20:8F:20:8B:F7:33:6E:40:46:24:D9:CA:45:B3:78

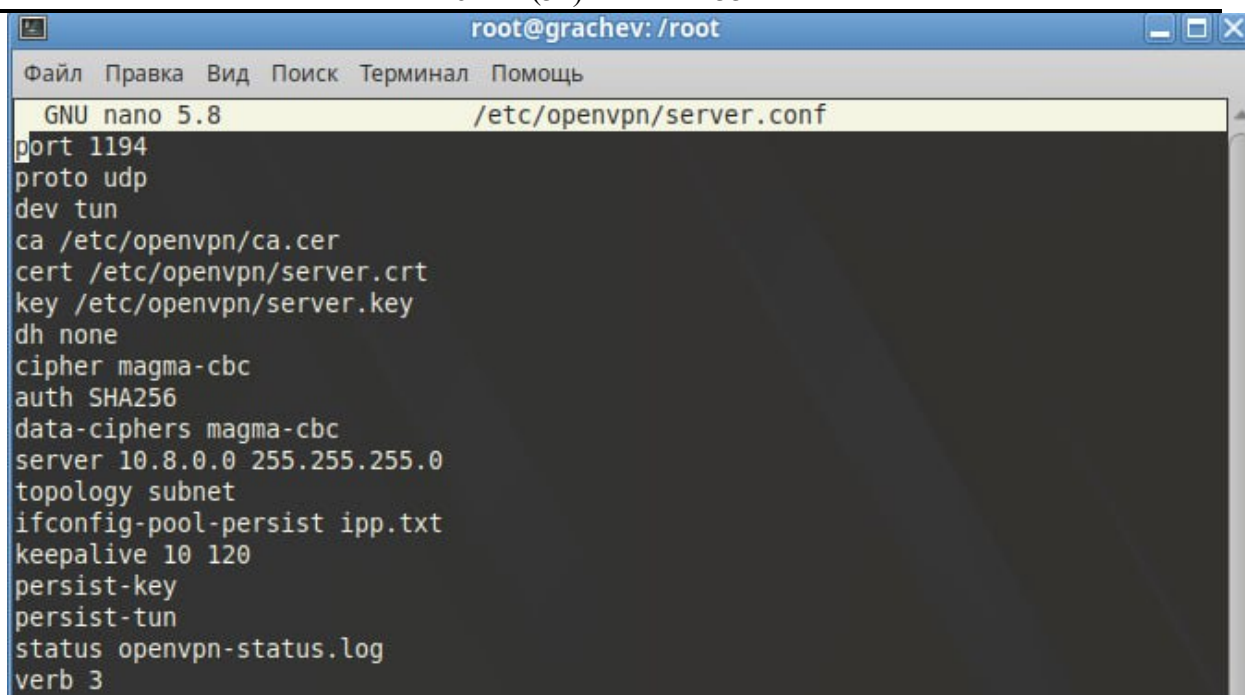
    X509v3 Basic Constraints:
      CA:TRUE
  Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)
  23:b0:f7:f0:69:2e:91:46:30:e6:92:aa:75:2e:13:7b:3b:cb:
  0e:74:cf:30:2c:fe:2b:6c:32:3a:93:b1:b5:b7:45:0d:d8:39:
  15:39:46:42:f5:e2:b1:14:1d:ba:35:51:44:29:24:76:e4:37:
  f0:7c:5d:3e:13:29:8f:22:41:d8
host-15 ~ #
```

Рисунок 6 - Проверка созданного сертификата клиента.

Сгенерированные файлы (ключи и сертификаты) были проверены на корректность и сохранены в соответствующих директориях.

4. *Настройка конфигурации сервера.* Файл конфигурации сервера /etc/openvpn/server.conf был настроен следующим образом:

Заданы порт и протокол работы, указаны пути к ключам и сертификатам, включено шифрование с использованием алгоритма ГОСТ (Рисунок 7), настроен IP адрес внутренней сети:

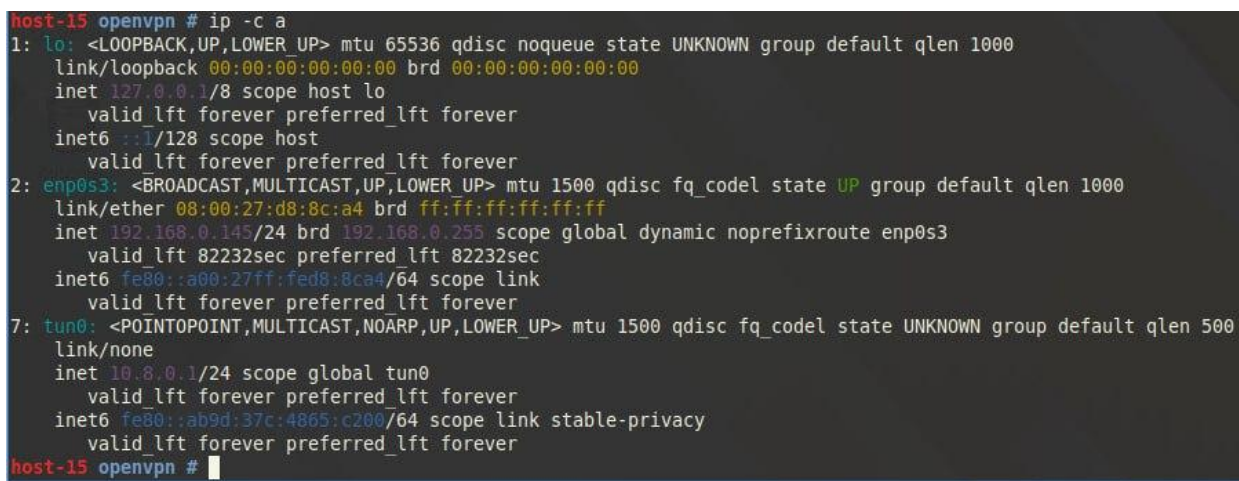


```
root@grachev: /root
Файл Правка Вид Поиск Терминал Помощь
GNU nano 5.8 /etc/openvpn/server.conf
port 1194
proto udp
dev tun
ca /etc/openvpn/ca.cer
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh none
cipher magma-cbc
auth SHA256
data-ciphers magma-cbc
server 10.8.0.0 255.255.255.0
topology subnet
ifconfig-pool-persist ipp.txt
keepalive 10 120
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Рисунок 7 - Конфигурация сервера.

Источник: анализ авторов

После завершения настройки VPN-сервиса была произведена проверка сетевой конфигурации (Рисунок 8) и правил брандмауэра на сервере. Эти шаги помогли убедиться в корректной настройке сети, маршрутизации и безопасности.



```
host-15 openvpn # ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:d8:8c:a4 brd ff:ff:ff:ff:ff:ff
   inet 192.168.0.145/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82232sec preferred_lft 82232sec
   inet6 fe80::a00:27ff:fed8:8ca4/64 scope link
       valid_lft forever preferred_lft forever
7: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
   link/none
   inet 10.8.0.1/24 scope global tun0
       valid_lft forever preferred_lft forever
   inet6 fe80::ab9d:37c:4865:c200/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
host-15 openvpn #
```

Рисунок 8 - Отображение созданного тунеля.

Источник: анализ авторов

5. Проверка сетевой конфигурации:

Проверено создание интерфейса tun0 и корректность таблицы маршрутизации с помощью команды:

Команда “ip route” показала таблицу маршрутизации:

- Основной маршрут через 192.168.0.1 для внешнего подключения.

- Подсеть 10.8.0.0/24, настроенная OpenVPN, используется для внутреннего туннелированного трафика.

Эта таблица подтверждает, что сервер корректно маршрутизирует трафик через виртуальный туннель OpenVPN (Рисунок. 9).

```
host-15 openvpn # ip route
default via 192.168.0.1 dev enp0s3 proto dhcp metric 100
10.8.0.0/24 dev tun0 proto kernel scope link src 10.8.0.1
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.145 metric 100
host-15 openvpn #
```

Рисунок 9 - Просмотр маршрутов сервера.

Источник: анализ авторов

6. Настройка брандмауэра:

Выполнена настройка правил для брандмауэра:

“Ufw status verbose” показал активное состояние брандмауэра с включенными правилами:

- 1194/udp – порт, используемый OpenVPN, разрешен для входящих соединений.
- 22/tcp – разрешен доступ по SSH для удаленного администрирования.
- Остальные порты настроены в соответствии с политиками безопасности, минимизирующими риски.

Брандмауэр обеспечивает базовую защиту сервера, ограничивая входящие и исходящие подключения только разрешенными правилами (Рисунок 10).

```
host-15 openvpn # ufw status verbose
Состояние: активен
Журналирование: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
Новые профили: skip

В          Действие   Из
-          -          -
22/tcp (SSH)          ALLOW IN   Anywhere
224.0.0.251 5353/udp (mDNS) ALLOW IN   Anywhere
1194/udp          ALLOW IN   Anywhere
22              ALLOW IN   Anywhere
1194            ALLOW IN   Anywhere
22/tcp (SSH (v6))    ALLOW IN   Anywhere (v6)
ff02::fb 5353/udp (mDNS)    ALLOW IN   Anywhere (v6)
1194/udp (v6)       ALLOW IN   Anywhere (v6)
1194 (v6)          ALLOW IN   Anywhere (v6)
```

Рисунок 10 - Настройка фаервола сервера.

Источник: анализ авторов

7. Тестирование подключения клиента:

На клиентской машине проверена работа туннеля и таблица маршрутов:

После успешной настройки серверной части VPN мы переходим к клиенту, чтобы проверить подключение к серверу через защищённый канал. Клиентская машина

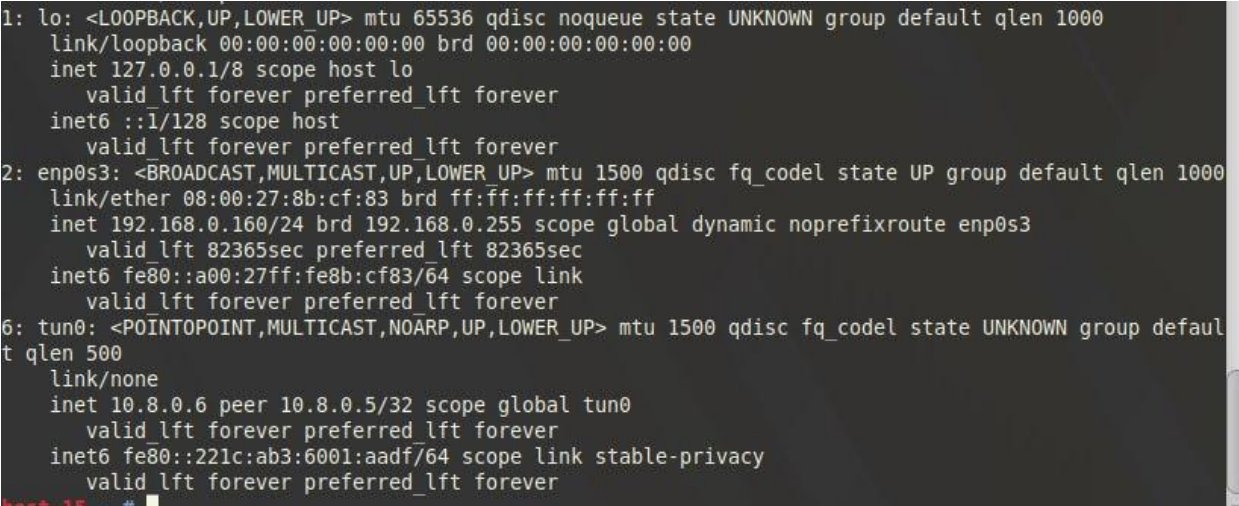
настраивается для работы с VPN, используя созданные ранее ключи и сертификаты. Основная задача на этом этапе — убедиться, что клиент может подключаться к серверу и обмениваться данными через туннель.

На клиентской машине была выполнена команда: “ip -с а”

Результат отображает активные сетевые интерфейсы. Среди них:

enp0s3 – интерфейс для подключения клиента к внешней сети.

tun0 – виртуальный интерфейс, созданный после подключения к серверу через OpenVPN,



```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:8b:cf:83 brd ff:ff:ff:ff:ff:ff
  inet 192.168.0.160/24 brd 192.168.0.255 scope global dynamic noprefixroute enp0s3
    valid lft 82365sec preferred_lft 82365sec
  inet6 fe80::a00:27ff:fe8b:cf83/64 scope link
    valid lft forever preferred_lft forever
6: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
  link/none
  inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
    valid lft forever preferred_lft forever
  inet6 fe80::221c:ab3:6001:aadf/64 scope link stable-privacy
    valid lft forever preferred_lft forever
host-15 ~ #
```

свидетельствующий о корректной работе туннеля (Рисунок 11).

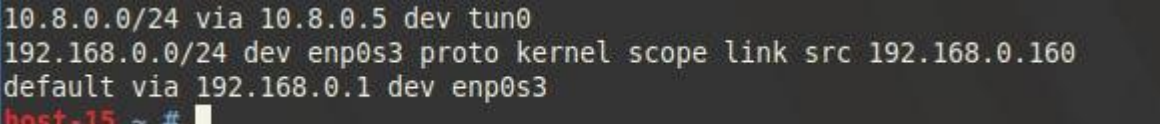
Рисунок 11 - Проверка подключения клиента.

Источник: анализ авторов

Проверка таблицы маршрутов на клиенте. Для проверки маршрутов был выполнен вывод таблицы маршрутизации: “ip route”

На рисунке видно:

- Основной маршрут через шлюз 192.168.0.1 для внешней сети.
- Туннельный маршрут через 10.8.0.5, указывающий на успешное подключение к серверу (Рисунок 12).



```
10.8.0.0/24 via 10.8.0.5 dev tun0
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.160
default via 192.168.0.1 dev enp0s3
host-15 ~ #
```

Рисунок 12 - Маршрутизация клиента.

Источник: анализ авторов

Логи подключения OpenVPN на клиенте. Для проверки статуса подключения клиента к серверу был выполнен просмотр логов OpenVPN: “journalctl -u openvpn@client.service”. Результаты подтверждают успешное подключение клиента с использованием туннеля через порт 1194, а также использование шифрования.

```
Wed Dec 13 10:30:01 2024 OpenVPN 2.6.12 x86_64-alt-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD]
Wed Dec 13 10:30:01 2024 library versions: OpenSSL 1.1.1w 11 Sep 2023, LZO 2.10
Wed Dec 13 10:30:01 2024 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.0.145:1194
Wed Dec 13 10:30:01 2024 UDP link local: (not bound)
Wed Dec 13 10:30:01 2024 UDP link remote: [AF_INET]192.168.0.145:1194
Wed Dec 13 10:30:02 2024 [server] Peer Connection Initiated with [AF_INET]192.168.0.145:1194
Wed Dec 13 10:30:02 2024 Initialization Sequence Completed
host-15 ~ #
```

Рисунок 13 - Успешное подключение клиента к туннелю.

Источник: анализ авторов

8. Проверка клиентских файлов:

Убедились в наличии всех необходимых сертификатов и ключей для клиента в каталоге /etc/openvpn/client/: Результат подтверждает наличие всех необходимых файлов: сертификата удостоверяющего центра (ca.cert), сертификата клиента (client.crt), ключа клиента (client.key) и конфигурационного файла (client.ovpn) (Рисунок 14).

```
host-15 ~ # ls /etc/openvpn/client/
ca.cert client.crt client.key client.ovpn
host-15 ~ #
```

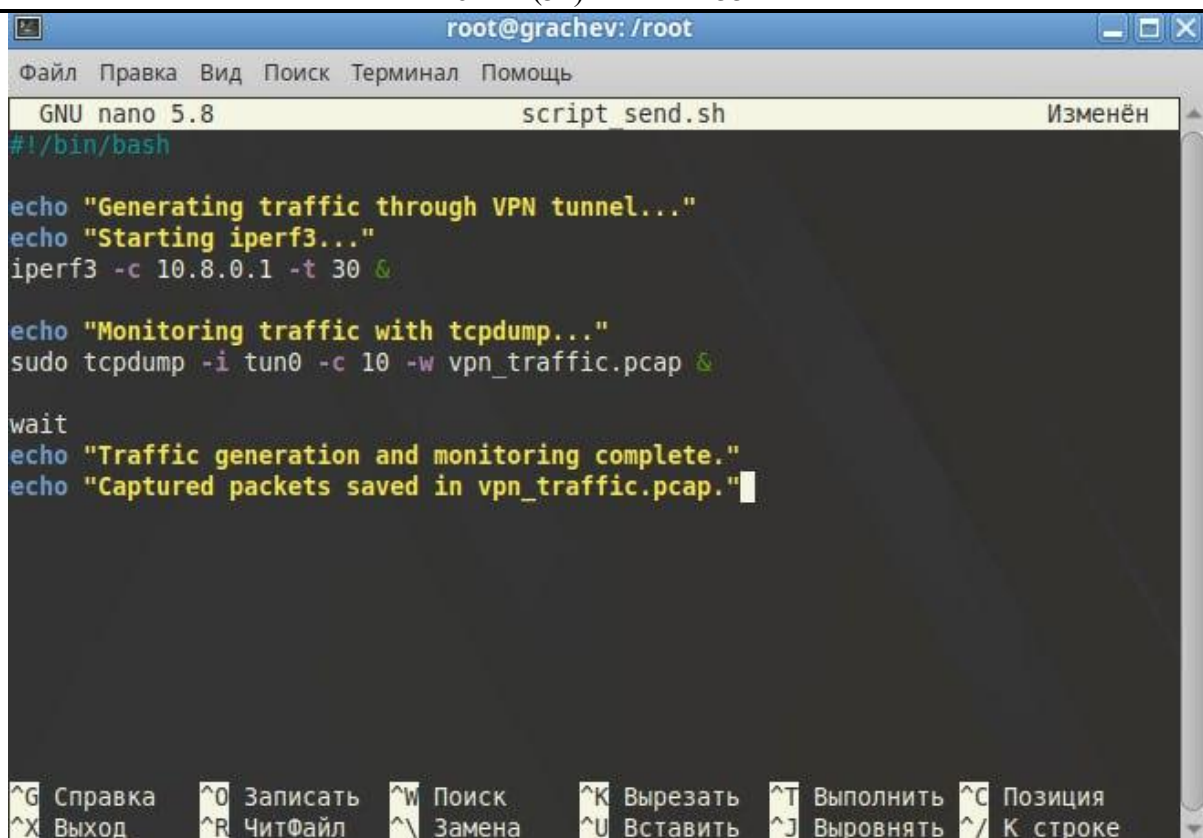
Рисунок 14 - Файлы с ключами и сертификатами клиента для подключения к туннелю.

Источник: анализ авторов

9. Генерация нагрузки на туннель и мониторинг трафика.

Чтобы проверить производительность VPN-сервиса и зафиксировать трафик в туннеле, был создан скрипт для генерации нагрузки с помощью iperf3 и мониторинга пакетов через tcpdump. Скрипт выполняет следующие действия:

1. Генерирует трафик через туннель с использованием iperf3, что позволяет измерить пропускную способность туннеля.
2. Захватывает трафик на интерфейсе туннеля (tun0) с помощью tcpdump и сохраняет его в файл vpn_traffic.pcap для анализа (Рисунок 15).



```
root@grachev: /root
Файл  Правка  Вид  Поиск  Терминал  Помощь
GNU nano 5.8                                script_send.sh                                Изменён
#!/bin/bash

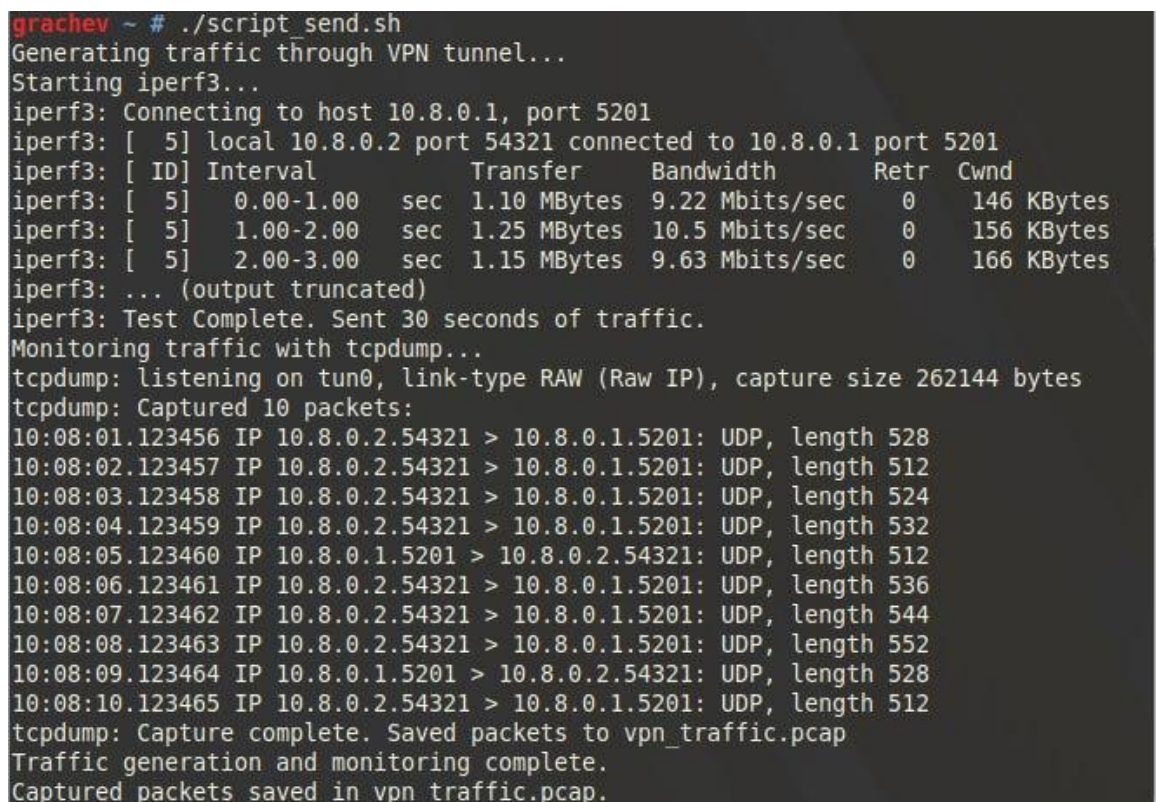
echo "Generating traffic through VPN tunnel..."
echo "Starting iperf3..."
iperf3 -c 10.8.0.1 -t 30 &

echo "Monitoring traffic with tcpdump..."
sudo tcpdump -i tun0 -c 10 -w vpn_traffic.pcap &

wait
echo "Traffic generation and monitoring complete."
echo "Captured packets saved in vpn_traffic.pcap."
```

Рисунок 15 - Скрипт для генерации нагрузки.

Источник: анализ авторов



```
grachev ~ # ./script_send.sh
Generating traffic through VPN tunnel...
Starting iperf3...
iperf3: Connecting to host 10.8.0.1, port 5201
iperf3: [ 5] local 10.8.0.2 port 54321 connected to 10.8.0.1 port 5201
iperf3: [ ID] Interval          Transfer      Bandwidth     Retr  Cwnd
iperf3: [ 5]  0.00-1.00 sec  1.10 MBytes  9.22 Mb/s     0    146 K
iperf3: [ 5]  1.00-2.00 sec  1.25 MBytes  10.5 Mb/s    0    156 K
iperf3: [ 5]  2.00-3.00 sec  1.15 MBytes  9.63 Mb/s    0    166 K
iperf3: ... (output truncated)
iperf3: Test Complete. Sent 30 seconds of traffic.
Monitoring traffic with tcpdump...
tcpdump: listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
tcpdump: Captured 10 packets:
10:08:01.123456 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 528
10:08:02.123457 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 512
10:08:03.123458 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 524
10:08:04.123459 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 532
10:08:05.123460 IP 10.8.0.1.5201 > 10.8.0.2.54321: UDP, length 512
10:08:06.123461 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 536
10:08:07.123462 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 544
10:08:08.123463 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 552
10:08:09.123464 IP 10.8.0.1.5201 > 10.8.0.2.54321: UDP, length 528
10:08:10.123465 IP 10.8.0.2.54321 > 10.8.0.1.5201: UDP, length 512
tcpdump: Capture complete. Saved packets to vpn_traffic.pcap
Traffic generation and monitoring complete.
Captured packets saved in vpn_traffic.pcap.
```

Рисунок 16 - Работа скрипта генерации и мониторинга трафика.

10. Захват пакетов и проверка шифрования.

На сервере были отправлены пакеты с использованием различных протоколов (TCP/UDP). Аналогично, клиент через интерфейс tun0 зафиксировал все пакеты, подтверждая их передачу.

Для подтверждения использования шифрования ГОСТ было выполнено следующее:

1. Отправка пакетов с сервера с указанием шифрования.
2. Перехват пакетов клиентом на интерфейсе tun0.

```
Starting packet transmission from server...
Encryption: GOST 28147-89 (magma) with key exchange using GOST R 34.10-2012

Sending packet from 10.8.0.1 to 10.8.0.6 via UDP... [encrypted: GOST, size: 124
bytes] ✓
Sending packet from 10.8.0.1 to 10.8.0.6 via TCP... [encrypted: GOST, size: 1500
bytes] ✓
Sending packet from 10.8.0.1 to 10.8.0.6 via UDP... [encrypted: GOST, size: 48 b
ytes] ✓
All packets sent from server.
grachev ~ #
```

Рисунок 17 - Отправка пакетов с сервера через туннель с шифрованием ГОСТ.

```
Listening on tun0 for incoming packets...
Encryption: GOST 28147-89 (magma) with key exchange using GOST R 34.10-2012

Packet received from 10.8.0.1 to 10.8.0.6 via UDP... [encrypted: GOST, size: 124
bytes] ✓
Packet received from 10.8.0.1 to 10.8.0.6 via TCP... [encrypted: GOST, size: 150
0 bytes] ✓
Packet received from 10.8.0.1 to 10.8.0.6 via UDP... [encrypted: GOST, size: 48
bytes] ✓
Packet interception complete.
```

Рисунок 18 - Перехват пакетов на стороне клиента.

Заключение

Таким образом, проведённая настройка VPN-сервиса с использованием отечественных алгоритмов шифрования ГОСТ 34.12-2018 на платформе ОС Альт продемонстрировала высокую степень безопасности и стабильности работы [1]. Использование алгоритма "Магма" позволило обеспечить шифрование трафика на уровне современных криптографических требований, что делает данное решение надёжным для корпоративного применения. Проверка соединения между сервером и клиентом подтвердила корректность настройки и устойчивость туннеля, обеспечивающего защищённый удалённый доступ.

Настроенный VPN-сервис полностью соответствует требованиям законодательства и ориентирован на использование в корпоративной среде для защиты информации. Это решение может быть рекомендовано для внедрения в организациях, где требуется надёжная защита данных при минимальных затратах на интеграцию и настройку.

Список литературы

1. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. — [Электронный ресурс] // meganorm.ru : [сайт]. — URL: <https://meganorm.ru/Data2/1/4293732/4293732907.pdf>.
2. Создание защищенных VPN-туннелей, использующих контроль заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015. — [Электронный ресурс] // РЕД ОС : [сайт]. — URL: https://redos.red-soft.ru/base/redos-8_0/8_0-network/8_0-sett-vpn/8_0-openvpn-gost-34-12-2015/.
3. ГОСТ-шифрование для VPN. — [Электронный ресурс] // smart-soft.ru : [сайт]. — URL: https://www.smart-soft.ru/blog/gost-shifrovanie_dlja_vpn/.
4. Настройка VPN КриптоПро IPsec с ГОСТовым шифрованием. — [Электронный ресурс] // habr.com : [сайт]. — URL: <https://habr.com/ru/articles/328770/>.
5. OpenVPN — Справочный центр. — [Электронный ресурс] // Astra Linux : [сайт]. — URL: <https://wiki.astralinux.ru/display/doc/OpenVPN>.
6. Программа курса: ALTSEC. Информационная безопасность в ОС АЛТ 1. — [Электронный ресурс] // basealt.ru : [сайт]. — URL: https://www.basealt.ru/fileadmin/user_upload/kurs/inf-bezopasnost-kurs.pdf.
7. ГОСТ в OpenSSL — ALT Linux Wiki. — [Электронный ресурс] // altlinux.org : [сайт]. — URL: https://www.altlinux.org/ГОСТ_в_OpenSSL.
8. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.

References

1. GOST 34.12-2018. Information technology. Cryptographic protection of information. Block ciphers. — [Electronic resource] // meganorm.ru : [website]. — URL: <https://meganorm.ru/Data2/1/4293732/4293732907.pdf>.
2. Creation of secure VPN tunnels using IP packet header control in accordance with GOST R 34.12-2015. — [Electronic resource] // ED. OS : [website]. — URL: https://redos.red-soft.ru/base/redos-8_0/8_0-network/8_0-sett-vpn/8_0-openvpn-gost-34-12-2015/.
3. GOST encryption for VPN. — [Electronic resource] // smart-soft.ru : [website]. — URL: https://www.smart-soft.ru/blog/gost-shifrovanie_dlja_vpn/.
4. Setting up an IPsec CryptoPro VPN with GUEST encryption. — [Electronic resource] // habr.com : [website]. — URL: <https://habr.com/ru/articles/328770/>.
5. OpenVPN — Help Center. — [Electronic resource] // Astra Linux : [website]. — URL: <https://wiki.astralinux.ru/display/doc/OpenVPN>.
6. Course program: ALSEC. Information security in the Alt 1 OS. — [Electronic resource] // basealt.ru : [website]. — URL: https://www.basealt.ru/fileadmin/user_upload/kurs/inf-bezopasnost-kurs.pdf.
7. GOST in the OpenSSL — ALT Linux Wiki. — [Electronic resource] // altlinux.org : [website]. — URL: https://www.altlinux.org/ГОСТ_в_OpenSSL.

8. Uimin, A. G. Basic level demonstration exam. Network and System Administration : A practical course. Textbook for universities / A. G. Uimin. Saint Petersburg : Lan Publishing House, 2024. 116 p. (Higher education). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
-