Калинин Фёдор Сергеевич
студент, кафедра комплексной безопасности критически важных объектов,
Российский государственный университет нефти и газа (НИУ) им. И. М. Губкина,
РФ, г. Москва

Стержаков Алексей Владимирович
студент, кафедра комплексной безопасности критически важных объектов,
Российский государственный университет нефти и газа (НИУ) им. И. М. Губкина,
РФ, г. Москва

НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И РАЗДЕЛЕНИЯ ТРАФИКА В СЛОЖНОЙ VPN-ТОПОЛОГИИ ТИПА «СЕТЬ-СЕТЬ» НА БАЗЕ ОТЕЧЕСТВЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

В работе представлена реализация защищённой VPN-инфраструктуры типа site-to-site на базе операционной системы Alt Workstation 11.1 с применением отечественных криптографических алгоритмов стандарта ГОСТ (Кузнечик ГОСТ Р 34.12-2015 и Магма ГОСТ 28147-89). Продемонстрирована полная цепь развёртывания: создание инфраструктуры открытых ключей (PKI) с поддержкой ГОСТ-алгоритмов, настройка OpenVPN для топологии сеть-сеть, реализация механизма разделения трафика посредством iptables, анализ зашифрованного трафика в Wireshark и оценка влияния различных алгоритмов шифрования на производительность системы.

Полученные результаты показывают, что отечественные алгоритмы обеспечивают надёжную криптографическую защиту и могут применяться в корпоративной инфраструктуре, хотя требуют больших вычислительных ресурсов в сравнении с AES.

ABSTRACT

This paper presents the implementation of a secure site-to-site VPN infrastructure based on Alt Workstation 11.1 operating system using domestic GOST cryptographic standards (Kuznyechik GOST R 34.12-2015 and Magma GOST 28147-89). A complete deployment chain is demonstrated: creation of public key infrastructure (PKI) with GOST algorithm support, OpenVPN configuration for site-to-site topology, traffic segregation mechanism implementation using iptables, encrypted traffic analysis in Wireshark, and performance evaluation of various encryption algorithms.

The obtained results show that domestic algorithms provide reliable cryptographic protection and can be applied in corporate infrastructure, although they require significantly higher computational resources compared to AES.

Ключевые слова: VPN, ГОСТ, OpenVPN, iptables, криптография, site-to-site, Alt Workstation.

Keywords: VPN, GOST, OpenVPN, iptables, cryptography, site-to-site, Alt Workstation.

Введение

Защита передачи данных между удалёнными локациями организации является критической задачей в области информационной безопасности. VPN-технологии обеспечивают конфиденциальность и целостность информации, но в контексте политики импортозамещения особое внимание уделяется использованию отечественных криптографических стандартов.

Целью работы является разработка и реализация конфигурации VPN-инфраструктуры типа site-to-site на базе Alt Workstation 11.1 с полной поддержкой ГОСТ-алгоритмов, интеграцией с межсетевым экраном iptables и полной проверкой функциональности системы.

Межсетевое экранирование и iptables

Межсетевой экран представляет собой систему контроля сетевого трафика на основе правил фильтрации пакетов. В Alt Workstation 11.1 основным инструментом является пакет netfilter/iptables, который работает с тремя встроенными цепочками: INPUT (входящий трафик), FORWARD (транзитный трафик) и OUTPUT (исходящий трафик). Каждая цепочка содержит набор правил, применяемых последовательно до первого совпадения с действием (ACCEPT, DROP, REJECT).

VPN-топология site-to-site

В отличие от point-to-point топологии, где соединяются отдельные клиенты с сервером, site-to-site позволяет связать две локальные сети через защищённый туннель. Это достигается благодаря механизму iroute, который объявляет локальные подсети на уровне OpenVPN и обеспечивает прозрачную маршрутизацию между сегментами сети.

Криптографические стандарты ГОСТ

Работа использует следующие отечественные стандарты:

- ГОСТ Р 34.12-2015 (Кузнечик) – симметричный блочный шифр с ключом 256 бит, аналог AES.
- ГОСТ 28147-89 (Магма) – симметричный шифр с ключом 256 бит, используется для совместимости.
- ГОСТ Р 34.11-2012 – криптографическая хеш-функция для контроля целостности.
- ГОСТ Р 34.10-2012 – алгоритм электронной цифровой подписи.

Использование этих алгоритмов в OpenVPN требует установки пакета openssl-gost-engine и корректной конфигурации движка ГОСТ в OpenSSL.

Сетевая топология и подготовка инфраструктуры

Эксперимент проводился в виртуальной среде на двух машинах Alt Workstation 11.1:

Машина ALT-left (сервер):

- enp0s3: 10.0.1.4/24 (локальная сеть A)
- enp0s8: 192.168.1.10/24 (сеть управления)
- tun0: 10.8.0.1/24 (VPN-туннель)

Машина ALT-right (клиент):

- enp0s3: 10.0.2.15/24 (локальная сеть B)
- enp0s8: 192.168.1.20/24 (сеть управления)
- tun0: 10.8.0.2/24 (VPN-туннель)

VPN-туннель использует UDP 1194 для связи между управляющими интерфейсами.

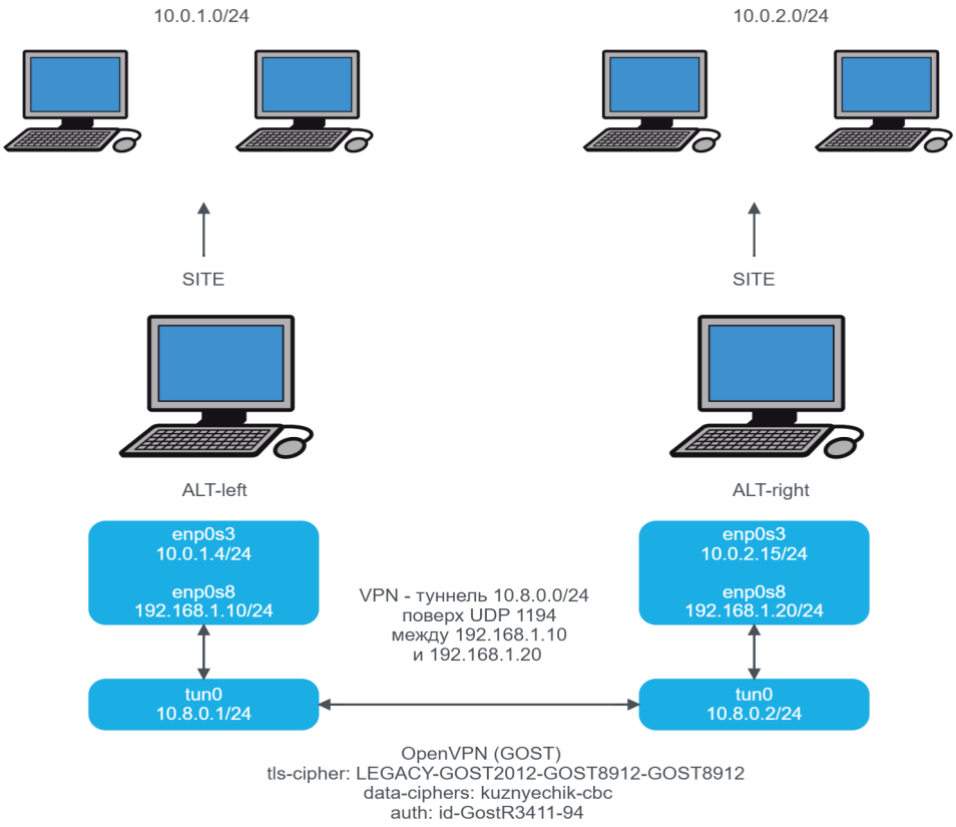

Рисунок 1 – Схема сети

Создание инфраструктуры открытых ключей с поддержкой ГОСТ

На машине ALT-left была создана структура центра сертификации (CA) с использованием ГОСТ Р 34.12-2015.

Процесс включал следующие этапы:

1. Активация ГОСТ-движка:

control openssl-gost enabled

2. Генерация корневого ключа CA:

openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCA -out ca-root.key

3. Создание самоподписанного сертификата CA:

openssl req -new -x509 -md_gost12_256 -days 3650 -key ca-root.key -out ca-root.crt -subj "/C=RU/ST=Russia/L=Moscow/O=VPN/OU=CA/CN=VPN-ROOT-CA"

4. Генерация ключей и сертификатов сервера и клиента аналогичным способом с подписанием CA.

Все криптографические операции использовали алгоритм ГОСТ Р 34.11-2012 для подписания сертификатов.

Конфигурация OpenVPN с ГОСТ

Конфигурация сервера (/etc/openvpn/server.conf):

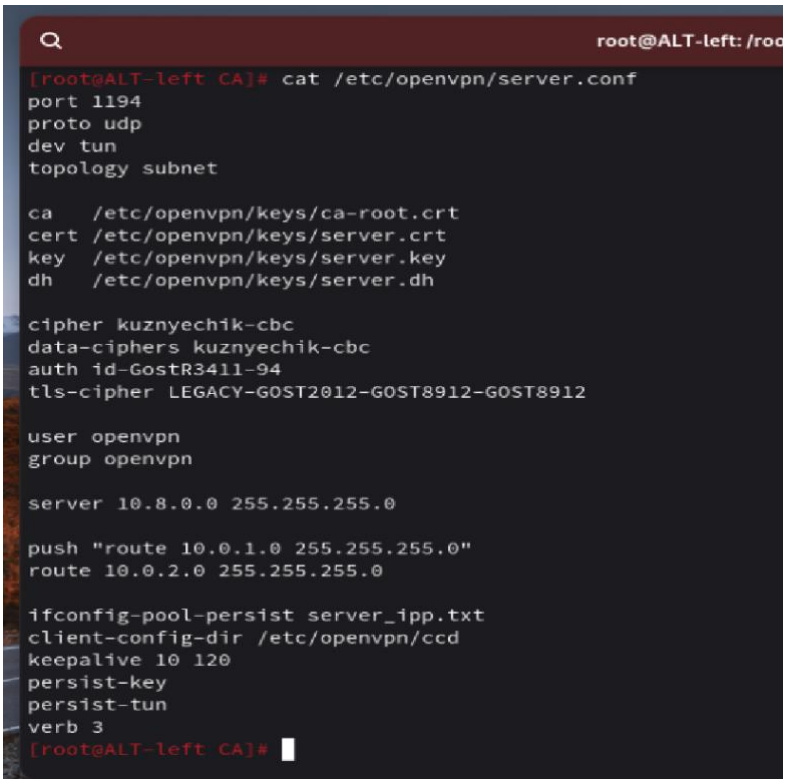

Рисунок 2 – Настройка конфига OpenVPN с ГОСТ на сервере

Конфигурация клиента (/etc/openvpn/client.conf):

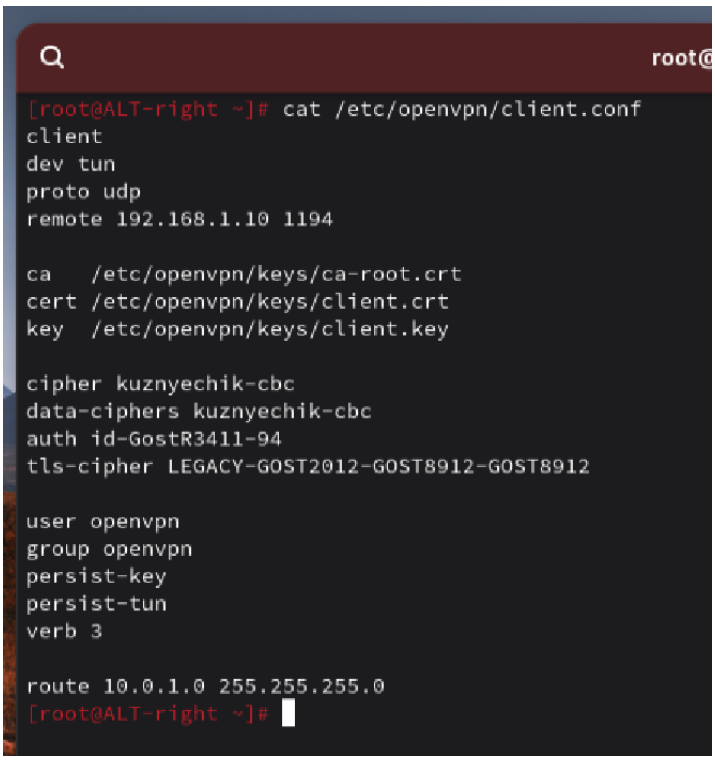

Рисунок 3 – Настройка конфига OpenVPN с ГОСТ на клиенте

Файл CCD для объявления локальной сети клиента:

```
# iroute 10.0.2.0 255.255.255.0
```

Ключевой особенностью является использование параметра iroute, который объявляет маршруты подсетей через VPN-туннель, обеспечивая двустороннюю маршрутизацию между локальными сетями.

Реализация разделения трафика посредством iptables

На обеих машинах были установлены правила межсетевого экрана с жёсткой политикой DROP и выборочным разрешением необходимого трафика.

1. Установка политик

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
```

```
# iptables -P OUTPUT ACCEPT
```

2. Базовые разрешения

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

3. Разделение трафика

```
# iptables -A FORWARD -i enp0s3 -o tun0  -s 10.0.1.0/24 -d 10.0.2.0/24 -p tcp -m multiport --dports 22,80,443 -m conntrack --ctstate NEW -j ACCEPT
# iptables -A FORWARD -i enp0s3 -o tun0 -s 10.0.1.0/24 -d 10.0.2.0/24 -p icmp -j ACCEPT
```

4. Блокирование прямого доступа к сети управления

```
# iptables -A FORWARD -i enp0s3 -o enp0s8 -s 10.0.1.0/24 -d 192.168.1.0/24 -j DROP
```

5. Разрешение трафика через туннель

```
# iptables -A INPUT -i tun0 -j ACCEPT
# iptables -A FORWARD -i tun0 -j ACCEPT
# iptables -A FORWARD -o tun0 -j ACCEPT
```

Аналогичная конфигурация была применена на ALT-right с инверсией направлений для гарантии двусторонней фильтрации.

Тестирование разделения трафика

1. Проверка связности между локальными сетями

На ALT-right выполнен ping к серверу в локальной сети A:

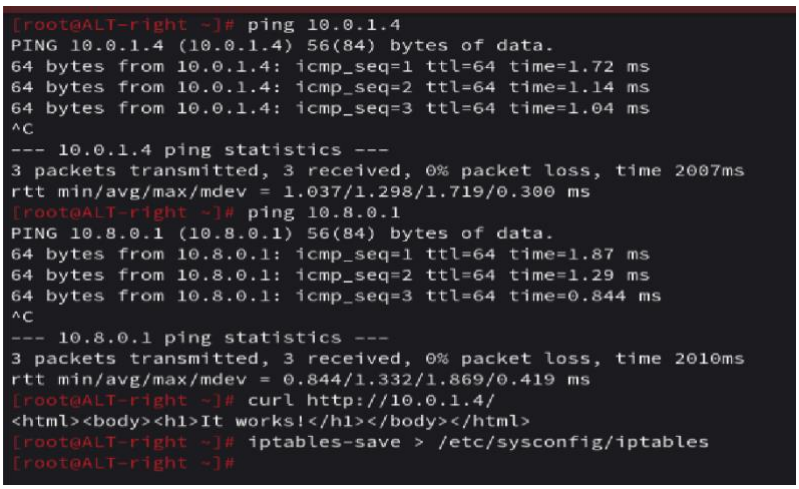

Рисунок 4 – Проверка ping на ALT-right

Успешные ответы подтверждают, что туннель работает и маршрутизация настроена корректно.

На ALT-left выполнен ping к клиенту в локальной сети B:

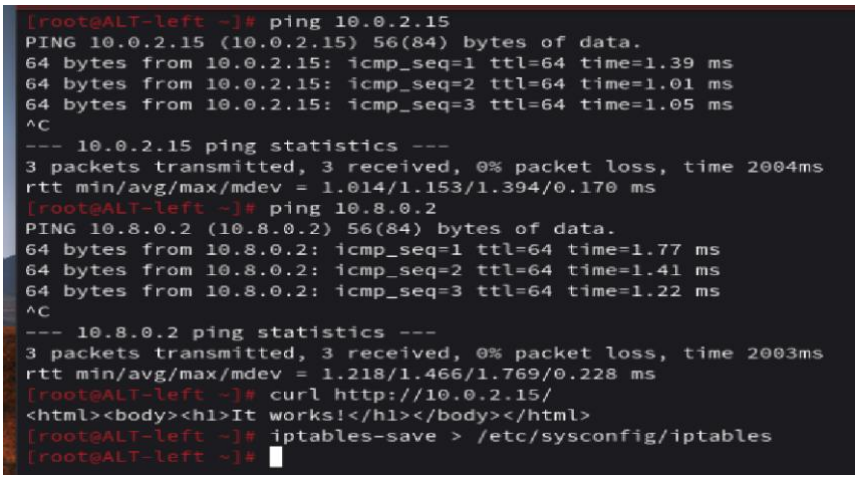

Рисунок 5 – Проверка ping на ALT-left

Аналогично, успешные ответы подтверждают двусторонние маршруты.

2. Проверка блокирования несанкционированного трафика

На ALT-right была выполнена попытка пинга сети управления с сервера:

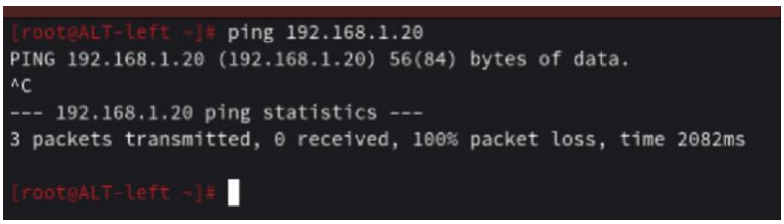

Рисунок 6 – Проверка из А нельзя попасть в транзитную сеть

Анализ трафика и верификация криптографии

Анализ в Wireshark

На физическом интерфейсе enp0s8 при захвате трафика было зафиксировано:

- Видны только пакеты UDP 1194 (OpenVPN)
- Отсутствует информация об ICMP, TCP портах, IP-адресах локальных сетей
- Полезная нагрузка полностью зашифрована (случайные байты)

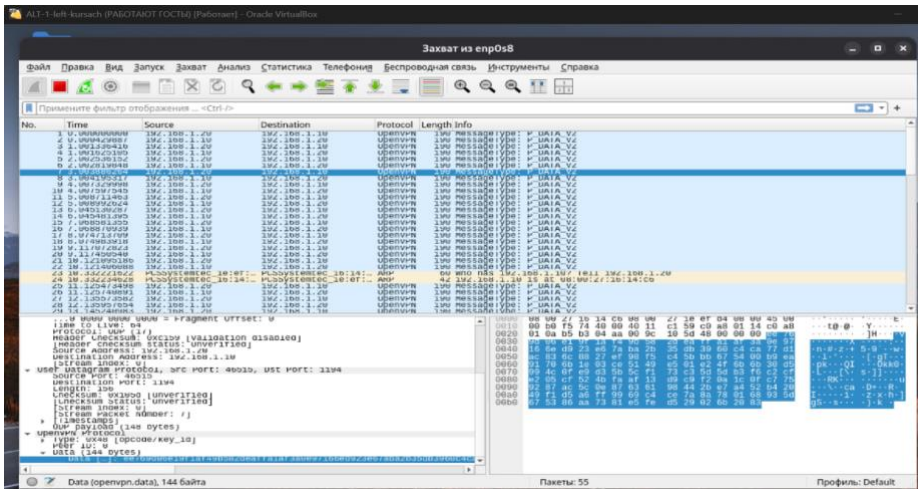

Рисунок 7 – Проверка через Wireshark до расшифровки

На туннельном интерфейсе tun0:

- Видны реальные ICMP Echo Request/Reply пакеты
- Отображаются IP-адреса источника (10.0.2.15) и назначения (10.0.1.4)
- Полезная нагрузка полностью видна в открытом виде

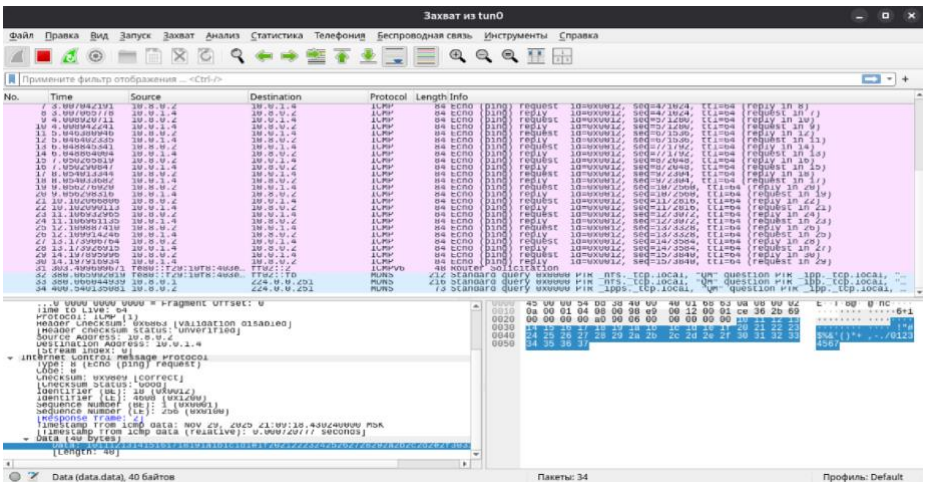

Рисунок 8 – Проверка через Wireshark после расшифровки

Это подтверждает, что криптография ГОСТ работает корректно: данные шифруются при выходе через внешний интерфейс и расшифровываются при входе во внутренний интерфейс туннеля.

Таблица 1. Сравнение видимости трафика

Параметр	Интерфейс enp0s8 (внешний)	Интерфейс tun0 (туннель)
Видимые протоколы	Только UDP/1194 OpenVPN	ICMP, TCP, UDP (реальные)
IP-адреса источника/назначения	192.168.1.10 ↔ 192.168.1.20	10.0.2.15 → 10.0.1.4
Порты и сервисы	Скрыты, только 1194 видна	Все видны полностью
Полезная нагрузка	Полностью зашифрована	Видна в открытом виде
Информация о приложениях	Недоступна	Полностью видна
Уровень конфиденциальности	Высокий	Отсутствует

Таблица 2. Атаки на стандартные способы шифрования

Интерфейс	Видимый трафик	Доступность данных
enp0s8 (внешний)	Только UDP/1194 OpenVPN	Полная криптографическая защита. Полезная нагрузка скрыта шифрованием ГОСТ
tun0 (внутренний VPN)	Реальные ICMP, IP-адреса, полезная нагрузка	Полный доступ, так как трафик уже расшифрован OpenVPN.

Оценка производительности

Для оценки влияния криптографических алгоритмов была использована утилита iperf3. Каждый тест длился 30 секунд с одновременным мониторингом загрузки процессора и памяти.

Таблица 3. Нагрузка на систему при различных методах шифрования на alt-workstation 11.1

Метрика	До нагрузки	Kuznyechik-CBC	Magma-CBC	AES-256-GCM	Без шифрования
Процессор					
User CPU (%)	0	18,1	12	3,1	1,9
System CPU (%)	0,2	19,3	14,4	25,3	5,4
Idle (%)	99,7	62,6	73,6	71,5	92,6
Суммарная нагрузка (%)	0,2	37,4	26,4	28,4	7,3
Процесс OpenVPN (%)	—	88,5	73,2	89,1	—
Память					
Использовано (МБ)	1786,7	1793,4	1448,2	1866,1	1758,7
Доступно (МБ)	3084,4	3087,6	3382,8	3094,9	3112,3

Анализ результатов

Наибольшая суммарная загрузка наблюдается при использовании Kuznyechik-CBC (37,4%), что отражает высокую вычислительную сложность алгоритма. Magma-CBC показывает умеренную нагрузку (26,4%), что

позволяет рассматривать его как компромиссный вариант для систем с ограниченными ресурсами.

AES-256-GCM демонстрирует более сбалансированную нагрузку (28,4%), благодаря использованию аппаратного ускорения инструкций AES-NI на уровне ядра процессора.

Колебания потребления памяти в пределах 100–150 МБ незначительны и не позволяют выявить существенные различия между алгоритмами.

Разработанная инфраструктура полностью обеспечивает защищённую передачу данных между удалёнными сетями с корректной маршрутизацией и разделением трафика. Анализ в Wireshark подтвердил полное шифрование трафика на внешнем интерфейсе с использованием ГОСТ Р 34.12-2015, гарантируя конфиденциальность данных при передаче через открытые каналы.

Отечественные алгоритмы требуют значительно больше вычислительных ресурсов по сравнению с AES, однако остаются приемлемыми для корпоративной инфраструктуры с типичными объёмами трафика, при этом Magma-CBC рекомендуется для систем с ограниченными ресурсами. Правила iptables эффективно блокируют несанкционированный доступ между сегментами сети, обеспечивая дополнительный уровень защиты на сетевом уровне.

Полученные результаты демонстрируют возможность полного перехода на отечественные криптографические решения в инфраструктуре, соответствующей требованиям политики импортозамещения и стандартам безопасности ГОСТ.

Список литературы

1. ГОСТ Р 34.12-2015. Блоковые шифры электронного документооборота. Кузнечик. – М.: Стандартинформ, 2015.
2. ГОСТ Р 34.11-2012. Хеш-функции. Функция хеширования. – М.: Стандартинформ, 2012.
3. ГОСТ Р 34.10-2012. Алгоритмы цифровой подписи на эллиптических кривых. – М.: Стандартинформ, 2012.
4. ALT Linux Alt Workstation 11.1. Глава 83. Создание защищенных VPN-туннелей с OpenVPN и GOST-криптографией [Электронный ресурс]. – URL: https://docs.altlinux.org/ru-RU/alt-kworkstation/11.1/html/alt-kworkstation/vpn.html (дата обращения: 02.11.2025).
5. OpenVPN 2.6 Reference Manual [Электронный ресурс]. – URL: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/ (дата обращения: 02.11.2025).
6. OpenSSL GOST Engine Documentation. Версия 3.0+ [Электронный ресурс]. – ALT Linux repositories (дата обращения: 02.11.2025).
7. Федеральный закон от 27.12.2002 № 184-ФЗ «О технических регламентах». – М.: Официальное издание, 2023.
8. Руководство по межсетевым экранам netfilter/iptables. Версия 1.8.8 [Электронный ресурс]. – URL: https://netfilter.org/documentation/HOWTO/NAT-HOWTO-6.html (дата обращения: 02.11.2025).
9. Межсетевые экраны. Топология VPN [Электронный ресурс]. – Режим доступа: https://intuit.ru/studies/courses/14250/1286/lecture/24248 (дата обращения: 02.11.2025).
10. Solar NGFW. Межсетевой экран: функции защиты [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_ngfw/blog/3408/ (дата обращения: 02.11.2025).

11. VPN (PPTP, PPPoE) [Электронный ресурс]. – Режим доступа: https://www.altlinux.org/VPN_(PPTP_PPPoE) (дата обращения: 13.11.2025).
12. OpenVPN [Электронный ресурс]. – Режим доступа: https://www.altlinux.org/OpenVPN (дата обращения: 15.11.2025).
13. NetworkManager [Электронный ресурс]. – Режим доступа: https://www.altlinux.org/NetworkManager (дата обращения: 18.11.2025).
14. ALT Linux Alt Workstation 11.1. Руководство пользователя [Электронный ресурс]. – Режим доступа: https://docs.altlinux.org/ru-RU/alt-workstation/11.1/html/alt-workstation/index.html (дата обращения: 18.11.2025).
15. OpenVPN // ALT Linux Wiki: [сайт]. – URL: https://www.altlinux.org/OpenVPN (дата обращения: 01.12.2025).
16. Введение в Iptables / Хабр // Habr.com : [сайт]. – URL: https://habr.com/ru/articles/747616/(дата обращения: 01.12.2025).
17. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. – 3-е издание, стереотипное. – Санкт-Петербург : Издательство "Лань", 2022. – 480 с. – ISBN 978-5-8114-9255-8.