ПРОФЕССИОНАЛИТЕТ, 2025, № 4 (008)

***УДК** 004.056.53*

Д. В. Демидова[1], Е. Д. Комнацкая[1]
[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ЗАЩИТЫ SSH-ПОДКЛЮЧЕНИЯ НА БАЗЕ ГОСТ-ШИФРОВАНИЯ В ОС АЛЬТ

Аннотация. В работе рассматриваются вопросы повышения безопасности удалённого администрирования за счёт применения отечественных криптографических алгоритмов при установлении SSH-соединений в операционной системе ALT Linux. Актуальность исследования обусловлена необходимостью соответствия требованиям российских регуляторов в области защиты информации и снижением зависимости от зарубежных криптографических решений. Проблема заключается в оценке устойчивости SSH-подключений при использовании ГОСТ-алгоритмов и анализе влияния выбранной криптополитики на возможность несанкционированного доступа и производительность соединения. В качестве объекта исследования выбран процесс установления и функционирования SSH-соединения, а предметом — поведение сервера при несовпадении криптографических наборов клиента и сервера. Для решения поставленной задачи была выполнена экспериментальная настройка SSH-сервера и клиента в ALT Linux с использованием пакетов gostcrypto, реализующих алгоритмы «Кузнечик», «Магма» и функции контроля целостности на основе Стрибога. Методика исследования включала моделирование легитимных и нелегитимных попыток подключения, анализ сетевого трафика с помощью Wireshark, а также измерение пропускной способности и ресурсной нагрузки. Результаты экспериментов показали, что сервер, настроенный на использование исключительно ГОСТ-алгоритмов, эффективно блокирует подключения с несовместимыми криптографическими параметрами. При корректной настройке клиента соединение устанавливается стабильно и соответствует заданной политике безопасности. Измерения производительности продемонстрировали, что применение ГОСТ-шифрования обеспечивает пропускную способность, сопоставимую со стандартными алгоритмами OpenSSH, при аналогичной нагрузке на вычислительные ресурсы. Сделан вывод о практической применимости ГОСТ-шифрования в SSH-соединениях для защищённого администрирования в отечественных операционных системах.

Ключевые слова: SSH-подключение; ГОСТ-криптография; ALT Linux; информационная безопасность; удалённое администрирование; сетевое шифрование.

Введение

SSH является стандартным средством удалённого администрирования, поэтому компрометация SSH-подключения ведёт к полному захвату системы. В российских условиях дополнительную актуальность имеет применение криптографических алгоритмов по ГОСТ 34.10-2012 [2] и ГОСТ 34.12-2015 [3], реализованных в составе дистрибутивов ALT Linux и предназначенных для соответствия требованиям регуляторов. Расширение OpenSSH за счёт пакетов с поддержкой ГОСТ позволяет строить защищённые каналы администрирования в отечественных ОС без использования зарубежных криптобиблиотек.

Объект исследования: процесс установления и функционирования SSH-подключения в ОС ALT Linux при удалённом администрировании хоста.

Предмет исследования: влияние использования ГОСТ-шифрования (алгоритмы «Кузнечик», «Магма», MAC на Стрибоге) на устойчивость SSH-подключения к несанкционированным попыткам подключения и на поведение сервера при несовпадении наборов алгоритмов у клиента и сервера.

Цель исследования: экспериментально проверить, как настроенный на ГОСТ-алгоритмы SSH-сервер ALT реагирует на подключения с «классическими» алгоритмами и с корректно настроенным ГОСТ-клиентом.

Литературный обзор:

– SSH (Secure Shell) — криптографический сетевой протокол удалённого доступа, обеспечивающий конфиденциальность, целостность и аутентификацию при работе в небезопасных сетях [8];

– ГОСТ Р 34.10-2012 описывает отечественный алгоритм электронной подписи, применяемый в российских криптографических средствах защиты для аутентификации и проверки подлинности данных [2]. Стандарт ГОСТ Р 34.12-2015 [3] определяет семейство блочных

шифров «Кузнечик» (блок 128 бит) и «Магма» (блок 64 бита), используемых для реализации симметричного шифрования в системах с повышенными требованиями к безопасности;

– ОС ALT Linux — отечественный дистрибутив Linux, в котором реализована поддержка ГОСТ-криптографии на уровне системных библиотек и программных пакетов, включая OpenSSL и OpenSSH [5];

– протокол OpenSSH реализует механизмы выбора алгоритмов шифрования (Ciphers), контроль целостности (MACs) и обмен ключами, что позволяет строить защищённые SSH-соединения между клиентом и сервером [6].

Методы исследования

Виртуальные машины были развернуты в среде аппаратной виртуализации на базе гипервизора KVM. Каждой виртуальной машине было выделено по 4 виртуальных процессорных ядра (vCPU) и 8 ГБ оперативной памяти. В качестве базовой аппаратной платформы использовался процессор архитектуры x86-64, без аппаратных ограничений по тактовой частоте. Конфигурации клиентской и серверной виртуальных машин были идентичны, что обеспечивало сопоставимость результатов измерений производительности. В рамках исследования также была выполнена настройка механизмов аутентификации и ключей хоста SSH с использованием отечественных алгоритмов электронной подписи. Для обеспечения полного соответствия криптографической политики требованиям регуляторов применялись ключи хоста и ключи пользователей, сформированные на основе алгоритма ГОСТ Р 34.10-2012. Основные этапы исследования включали:

Примечание к конфигурации. В эксперименте использовались пакеты ветки p10 для архитектуры x86_64 на обеих виртуальных машинах; иные ветки и i586 к воспроизводимой конфигурации не относятся.

– экспериментальная настройка программного обеспечения: установка пакетов openssl-gost-engine [7] и семейства openssh-*-gostcrypto, изменение репозитория apt и конфигурации sshd_config/ssh_config согласно официальной документации ALT Linux.;

– метод активного сетевого эксперимента: моделирование легитимного администратора и злоумышленника, фиксирование результатов попыток подключения по SSH с разными наборами шифров и MAC-алгоритмов и анализ выводимых сервером сообщений об ошибке согласования алгоритмов;

– анализ сетевого трафика с помощью Wireshark: для верификации криптографических параметров установленного SSH-соединения был выполнен захват сетевых пакетов на интерфейсе сервера [1];

– измерение производительности и ресурсной нагрузки: для оценки влияния ГОСТ-шифрования на производительность SSH-сессий применялись утилита iperf — для измерения пропускной способности сети внутри установленного SSH-туннеля; утилита htop — для мониторинга загрузки центрального процессора и использования оперативной памяти в реальном времени.

В рамках сравнительного анализа производительности в качестве базового зарубежного алгоритма был выбран шифр ChaCha20-Poly1305, широко используемый в реализации OpenSSH и являющийся алгоритмом по умолчанию при отсутствии или ограниченной эффективности аппаратного ускорения AES. Сравнение с алгоритмами семейства AES (AES-256-CTR, AES-256-GCM) в данной работе не проводилось, так как целью эксперимента являлась оценка накладных расходов ГОСТ-алгоритмов в типовом программном сценарии без учёта специализированных аппаратных расширений.

Ход исследования

1. Подготовка криптобиблиотеки и репозиториев.

В файл /etc/apt/sources.list был добавлен репозиторий RPMS.gostcrypto ALT Linux (см. рисунок 1) [5], после чего выполнено обновление списка пакетов apt-get update и установка openssl-gost-engine [7], что позволило включить поддержку ГОСТ в OpenSSL. Корректность установки проверялась командой openssl ciphers | grep GOST, по выводу которой фиксировалось появление режимов с «magma» и «grasshopper».

```
# Local package resource list for APT goes here.
# To inspect package defined part, see /etc/apt/sources.list.d/*.list
#
#https://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch/gostcrypto/ x86_64 RPMS
#https://ftp.altlinux.org/pub/distributions/ALTLinux/p10/branch/gostcrypto/ noarch RPMS
```

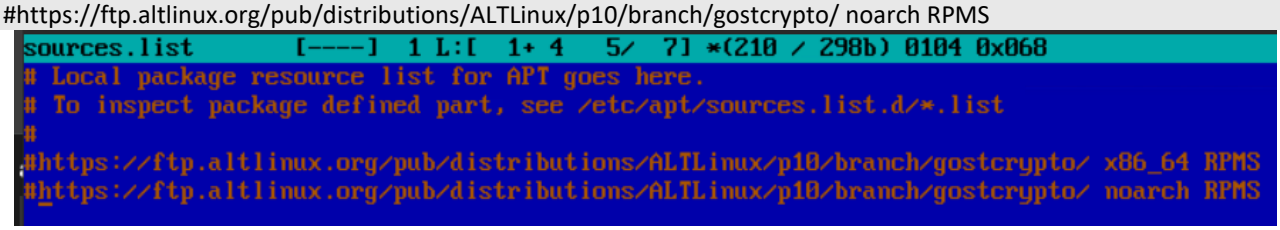

Рис. 1. Добавление репозитория gostcrypto

Ссылка на пакет openssl-gost-engine: *https://packages.altlinux.org/ru/p10/srpms/openssl-gost-engine/*

2. Установка SSH с ГОСТ.

На сервере и клиенте последовательно были установлены пакеты openssh-gostcrypto, openssh-clients-gostcrypto, openssh-server-gostcrypto [6] и сопутствующие компоненты, после чего демон sshd был перезапущен командой systemctl restart sshd. Таким образом, как сервер, так и клиент получили возможность использовать ГОСТ-алгоритмы на уровне SSH.

```
# apt-get install openssh-gostcrypto openssh-clients-gostcrypto openssh-server-gostcrypto openssh-server-control-gostcrypto openssh-common-gostcrypto openssh-askpass-common-gostcrypto
```

Ссылка на пакеты:

http://rsync.altlinux.ru/pub/distributions/ALTLinux/p10/branch/x86_64/RPMS.gostcrypto/

3. Настройка серверной стороны.

В файле /etc/openssh/sshd_config на сервере значения директив Ciphers и MACs были ограничены ГОСТ-алгоритмами, например, grasshopper-ctr@altlinux.org и hmac-streebog-512@altlinux.org (см. рисунок 2), а затем применены перезапуском sshd. Дополнительно был создан отдельный пользователь, к которому разрешалось подключение только с использованием этих алгоритмов.

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

#AllowGroups wheel users
```

```
# Accept locale environment variables
AcceptEnv LANG LANGUAGE LC_ADDRESS LC_ALL LC_COLLATE LC_CTYPE
AcceptEnv LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY
AcceptEnv LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE LC_TIME

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding yes
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
#Match Group secured
#       AuthorizedKeysFile /etc/openssh/authorized_keys/%u
#Match Group !secured,*
#       AuthorizedKeysFile /etc/openssh/authorized_keys/%u .ssh/authorized_keys

Ciphers grasshopper-ctr@altlinux.org
MACs grasshopper-mac@altlinux.org,hmac-stribog-512@altlinux.org
```

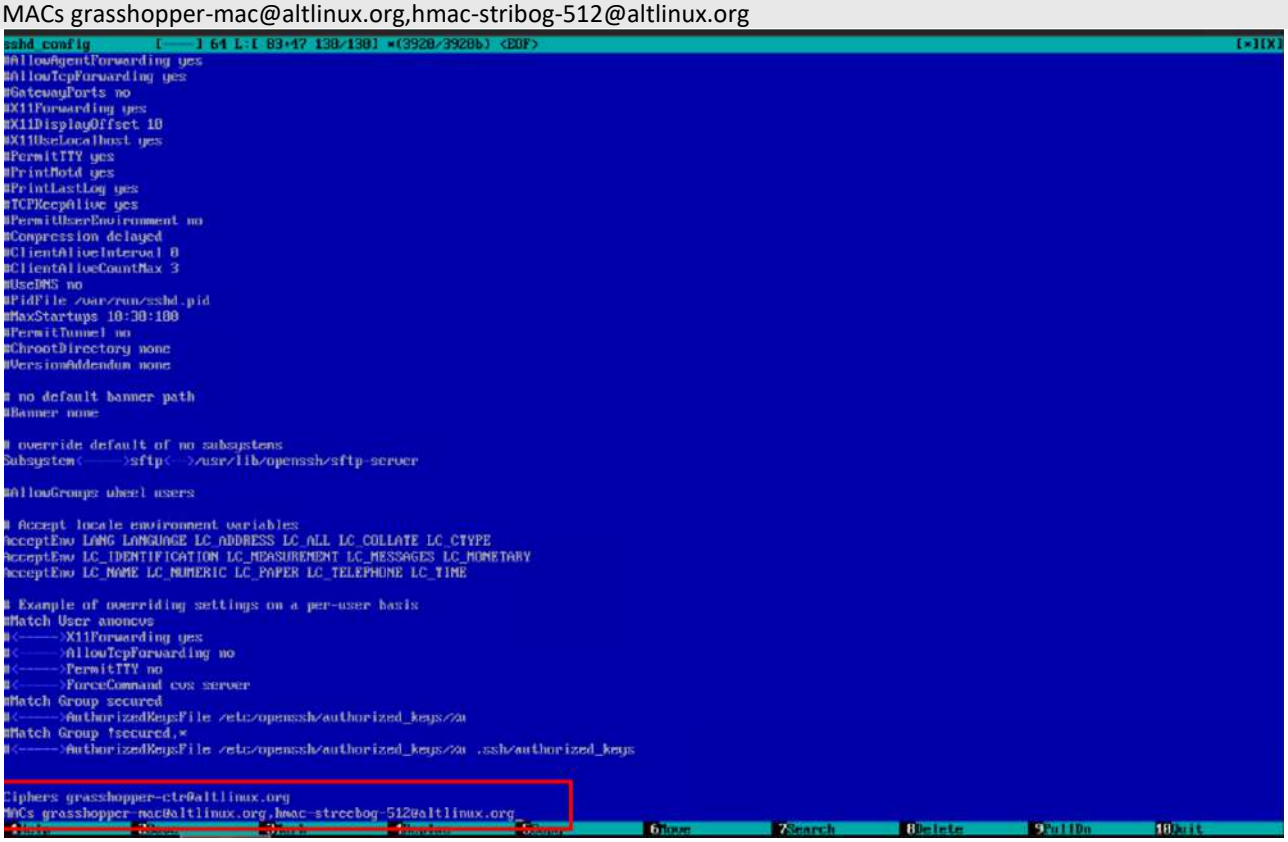

Рис. 2. Настройка sshd_config

3.1. Настройка аутентификации и ключей хоста

Для обеспечения аутентификации с использованием отечественных криптографических алгоритмов на сервере были сгенерированы ключи хоста на основе ГОСТ Р 34.10-2012 с использованием утилиты ssh-keygen, входящей в состав пакетов openssh-gostcrypto.

Генерация ключей хоста выполнялась следующей командой:

```
# ssh-keygen -t gost2012_256 -f /etc/ssh/ssh_host_gost2012_key
```

После генерации ключей в конфигурационном файле sshd_config была явно задана директива:

```
# HostKeyAlgorithms gost2012_256
```

Аналогичным образом были сформированы пользовательские ключи для аутентификации по открытому ключу (Public Key Authentication), что обеспечило использование ГОСТ-алгоритмов не только для защиты трафика, но и для процессов аутентификации и идентификации сторон SSH-соединения.

4. Настройка клиентской стороны.

На клиенте были установлены те же пакеты gostcrypto, а в системном или пользовательском конфигурационном файле SSH заданы параметры Ciphers и MACs с ГОСТ-режимами. Для более наглядного контроля использовались явные параметры при вызове клиента вида ssh gostuser@localhost -ciphers=grasshopper-ctr@altlinux.org -oMACs=grasshopper-mac@altlinux.org,hmac-streebog-512@altlinux.org.

Ссылка на пакеты: http://rsync.altlinux.ru/pub/distributions/ALTLinux/p10/branch/x86_64/RPMS.gostcrypto/

5. Постановка эксперимента (проверка политики согласования криптографических алгоритмов).

На первом этапе имитировалась атака: с клиентской машины выполнялось подключение к серверу без указания ГОСТ-алгоритмов, с типичным набором стандартных шифров OpenSSH (например, AES и ChaCha20). Сервер, настроенный предлагать только ГОСТ-режимы, отклонял соединение и возвращал ошибку несогласования алгоритмов, в которой перечислял ожидаемые типы шифрования и MAC, что видно по диагностическому выводу SSH и логам sshd (см. рисунок 3).

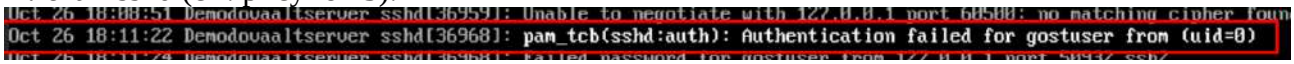

Рис. 3. Сообщение об ошибке несогласования алгоритмов при попытке подключения без ГОСТ-шифров.

6. Постановка эксперимента (легитимное подключение).

На втором этапе тот же клиент был настроен на использование ГОСТ-режимов, и попытка подключения выполнялась с явным указанием нужных Ciphers и MACs, после чего устанавливалась устойчиво функционирующая SSH-сессия под созданным пользователем. При этом сервер принимал соединение, так как набор алгоритмов полностью совпадал с его политикой, что подтверждалось отсутствием ошибок и успешным входом в систему.

Результаты

В ходе «атаки» с несоответствующим набором алгоритмов сервер ALT Linux блокировал установление SSH-сессии и возвращал диагностическое сообщение о невозможности согласовать шифрование, что подтверждает жёсткую привязку подключения к выбранным ГОСТ-алгоритмам. Таким образом, даже при знании адреса сервера и открытого порта злоумышленник не может установить канал без подбора совместимого стека шифрования.

При корректной настройке клиента на те же ГОСТ-режимы, что и на сервере, SSH-сессия успешно устанавливалась, что демонстрирует совместимость реализованных в ALT Linux пакетов openssh-gostcrypto и их пригодность для практического использования в администрировании. Сравнение логов показало, что в обоих направлениях трафик шифруется ГОСТ-алгоритмами, а любые отклонения от заданного набора приводят к немедленному разрыву соединения.

Для подтверждения корректности работы ГОСТ-шифрования в SSH-сессии был выполнен перехват сетевого трафика между клиентом и сервером с использованием утилиты Wireshark [1]. В ходе анализа зафиксировано, что после успешного согласования алгоритмов в начале сессии клиент и сервер обмениваются пакетами, в которых явно указано использование ГОСТ-алгоритмов (см. рисунок 4).

В захваченных пакетах (например, пакет №18) отображается структура SSHv2 с указанием применяемых криптографических алгоритмов, а также длина зашифрованного пакета и его зашифрованное содержимое. Это подтверждает, что весь трафик SSH, включая служебные сообщения и данные пользователя, защищён с использованием отечественных стандартов шифрования [2,3].

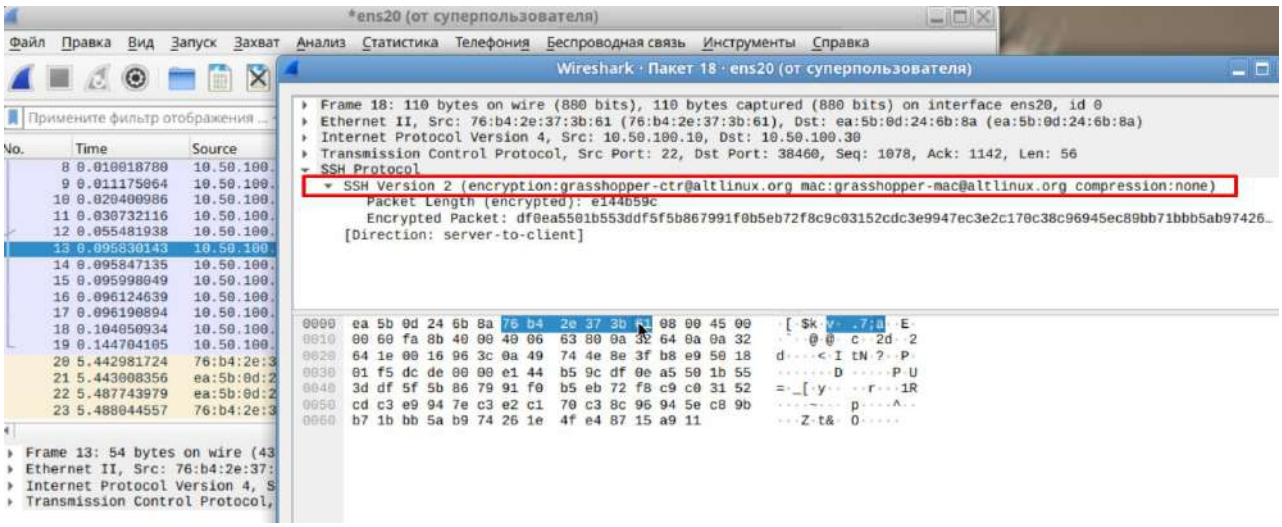

Рис. 4. Анализ SSH-трафика при успешном подключении с ГОСТ-алгоритмами.

При попытке подключения с несовместимыми алгоритмами (например, ChaCha20) Wireshark фиксировал только этап согласования алгоритмов и последующий разрыв соединения, что соответствует политике безопасности, настроенной на сервере (см. рисунок 5).

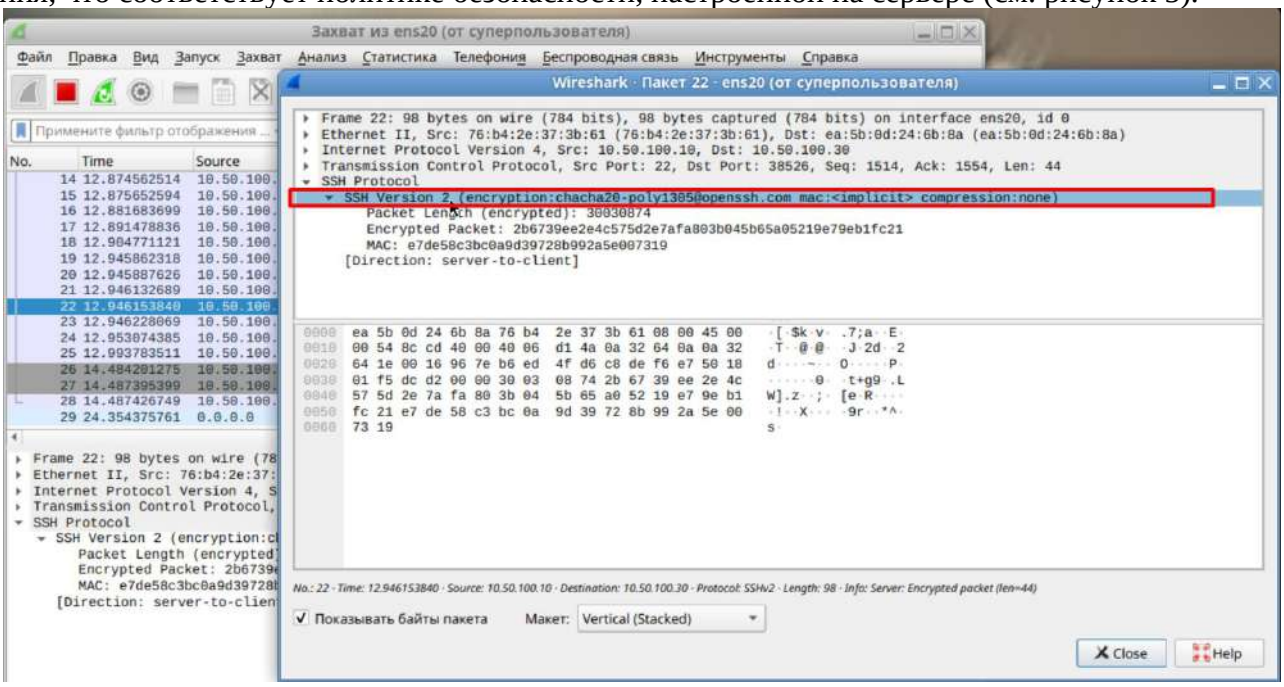

Рис. 5. Анализ SSH-трафика при неудачной попытке подключения с несовместимыми алгоритмами.

Для оценки влияния ГОСТ-шифрования на производительность SSH-подключений были проведены измерения сетевой пропускной способности с использованием утилиты iperf в рамках установленной SSH-сессии. Измерения выполнялись между виртуальными машинами (клиент и сервер) в идентичных сетевых условиях как с ГОСТ-алгоритмами, так и со стандартными алгоритмами (см. таблицу 1).

Таблица 1 – Сравнение пропускной способности SSH-сессий с разными алгоритмами шифрования

Тип шифрования	Алгоритм шифрования	Пропускная способность	Средняя пропускная способность	Отклонение	Переданный объем данных	Нагрузка на ЦПУ	Использование памяти
ГОСТ-алгоритм	grasshopper-ctr@altlinux.org	30.8 Гбит/с	30.5 Гбит/с	±1.0 Гбит/с (3.2%)	35.8 ГБ	60–64%	0.2%
		30.9 Гбит/с			36.0 ГБ		
		29.9 Гбит/с			36.0 ГБ		
	chacha20-poly1305@openssh.com	31.9 Гбит/с	31.7 Гбит/с		36.9 ГБ	60-62%	0.2%
		30.6 Гбит/с			35.7 ГБ		

Стан-дарт-ный алгоритм		32.6 Гбит/с		±0.6 Гбит/с (1.8%)	37.1 ГБ		

Проведённые измерения демонстрируют, что использование ГОСТ-шифрования (grasshopper-ctr) в SSH-сессиях обеспечивает пропускную способность, сопоставимую со стандартными алгоритмами (chacha20-poly1305). Средняя скорость передачи данных составила 30.5 Гбит/с для ГОСТ (см. рисунок 6) против 31.7 Гбит/с для ChaCha20 (см. рисунок 7), что указывает на незначительное снижение производительности (около 3.8%).

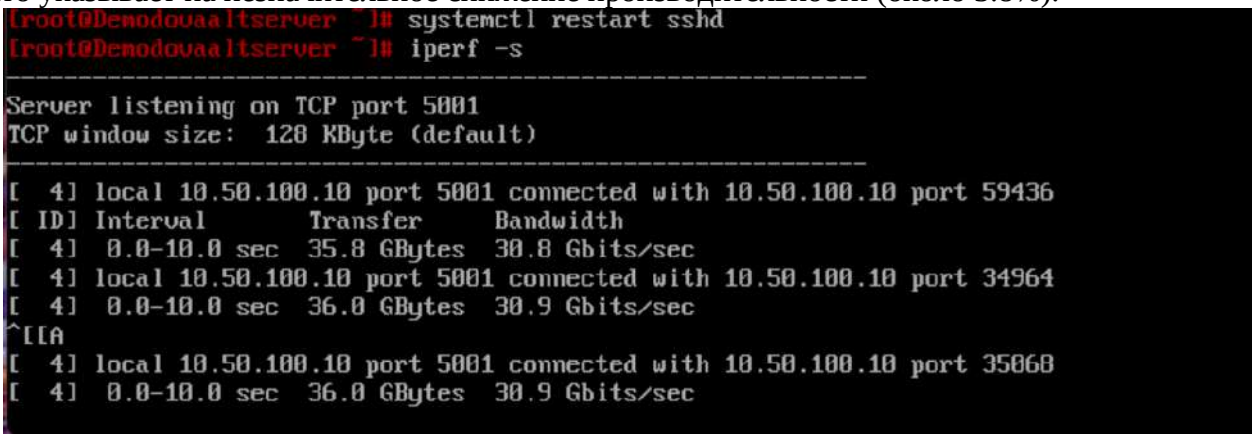

Рис. 6. Измерение пропускной способности SSH-сессии с ГОСТ-шифрованием.

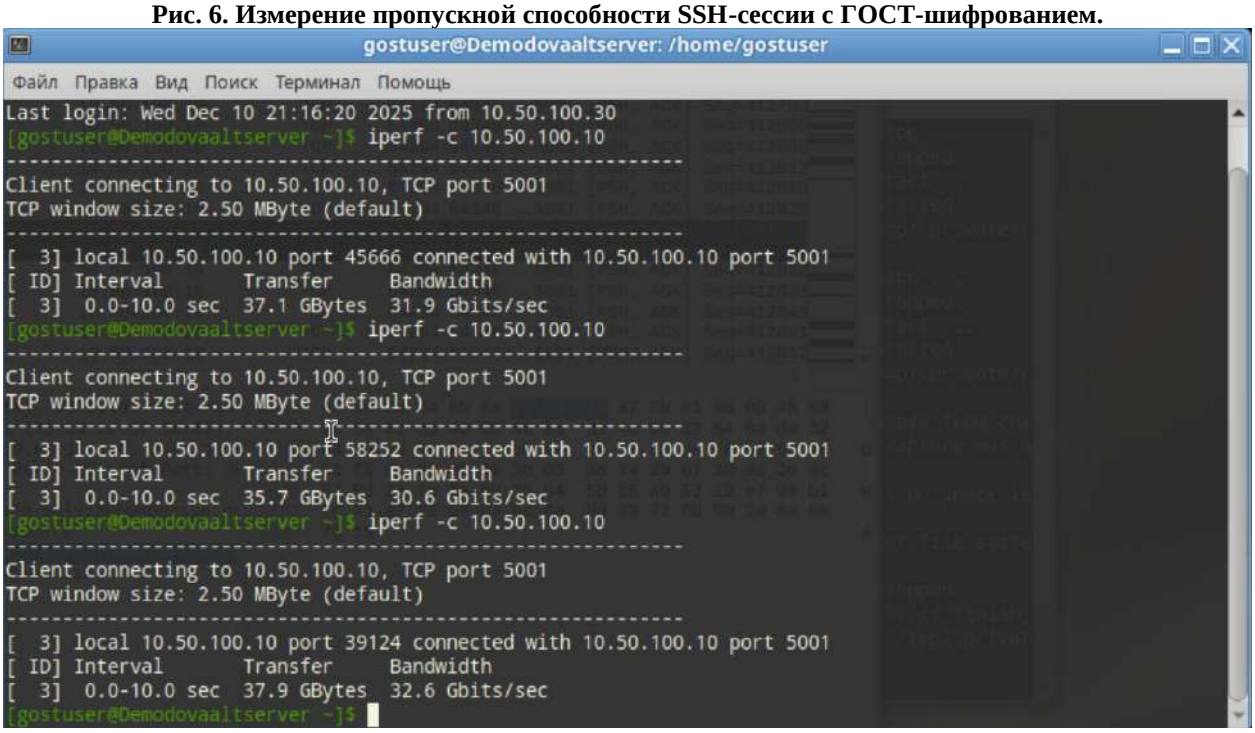

Рис. 7. Измерение пропускной способности SSH-сессии со стандартным алгоритмом.

При этом нагрузка на ЦПУ в обоих случаях была практически идентичной (60–64%), что подтверждает вычислительную эффективность реализации алгоритма «Кузнечик» в ALT Linux. Использование памяти оставалось минимальным (0.2% от доступной ОЗУ), что свидетельствует об отсутствии существенных накладных расходов на хранение криптографических контекстов.

Таким образом, внедрение ГОСТ-шифрования в SSH-подключения не приводит к критичному падению производительности, что делает его практичным решением для организаций, требующих соответствия отечественным стандартам криптозащиты без существенных компромиссов в скорости передачи данных.

Вывод

Проведённое исследование показало, что настройка SSH в ALT Linux на использование только ГОСТ-алгоритмов позволяет эффективно контролировать криптографический

профиль подключений и предотвращать установление сессий с неподходящими алгоритмами. Несмотря на то, что потенциальный злоумышленник теоретически может установить у себя те же криптографические библиотеки, на практике необходимость точного совпадения режимов шифрования и MAC-функций задаёт дополнительный барьер и упрощает формирование строгой криптополитики в инфраструктуре организации.

В результате исследования была составлена сравнительная таблица пропускной способности SSH-сессий. С точки зрения производительности, реализация ГОСТ-шифрования в ALT Linux демонстрирует высокую эффективность: средняя пропускная способность SSH-сессий с алгоритмом «Кузнечик» составляет 30.5 Гбит/с, что лишь на 3.8% ниже, чем при использовании оптимизированного стандартного алгоритма ChaCha20-Poly1305 (31.7 Гбит/с). При этом нагрузка на ЦПУ и потребление памяти остаются сопоставимыми, что подтверждает технологическую зрелость отечественных криптографических реализаций.

Анализ сетевого трафика с использованием Wireshark подтвердил корректность работы ГОСТ-алгоритмов на транспортном уровне SSH: в захваченных пакетах явно указываются используемые криптографические режимы, а весь трафик проходит в зашифрованном виде, что соответствует требованиям защиты передаваемых данных.

Библиографический список

1. Алицар, А. Wireshark для всех. Лайфхаки на каждый день [Электронный ресурс] / А. Алицар // Habr. – 2021. – 14 июня. – URL: https://habr.com/ru/companies/vdsina/articles/562110/ (дата обращения: 01.12.2025).
2. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Москва : Стандартинформ, 2012.
3. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – Москва : Стандартинформ, 2015.
4. Официальный репозиторий пакетов ALT Linux [Электронный ресурс] // ALT Linux Packages. – URL: https://packages.altlinux.org/ (дата обращения: 10.11.2025).
5. OpenSSH GOSTCrypto [Электронный ресурс] // ALT Linux Packages. – URL: https://packages.altlinux.org/ru/p10/srpms/openssh-gostcrypto/ (дата обращения: 11.12.2025).
6. OpenSSL GOST Engine [Электронный ресурс] // ALT Linux Packages. – URL: https://packages.altlinux.org/ru/p10/srpms/openssl-gost-engine/ (дата обращения: 11.12.2025).
7. Создание SSH-туннелей, использующих контроль целостности заголовков IP-пакетов в соответствии с ГОСТ Р 34.12-2015 [Электронный ресурс] // Документация ALT Linux. ALT Workstation 10.2. – URL: https://docs.altlinux.org/ru-RU/alt-workstation/10.2/html/alt-workstation/ssh_t.html (дата обращения: 11.12.2025).
8. Уймин, А. Г. Определение отечественной технологической платформы в рамках создания киберполигона: «Сетевое и системное администрирование» / А. Г. Уймин // Текущие вызовы в подготовке кадров. Обучение специалистов по современным направлениям информационных технологий, кибербезопасности и ИКТ-электроники, актуальным для экономики данных : сборник научных трудов. – Тверь, 2024. – С. 122–123.

References

1. Alitsar, A. (2021, June 14). Wireshark for everyone: Life hacks for every day. Habr. https://habr.com/ru/companies/vdsina/articles/562110/
2. GOST R 34.10–2012. (2012). Information technology. Cryptographic protection of information. Processes of digital signature generation and verification. Standartinform.
3. GOST R 34.12–2015. (2015). Information technology. Cryptographic protection of information. Block ciphers. Standartinform.

4. ALT Linux Packages. (n.d.). Official repository of ALT Linux packages. https://packages.alt-linux.org/
5. ALT Linux Packages. (n.d.). OpenSSH GOSTCrypto. https://packages.alt-linux.org/ru/p10/srpms/openssh-gostcrypto/
6. ALT Linux Packages. (n.d.). OpenSSL GOST Engine. https://packages.alt-linux.org/ru/p10/srpms/openssl-gost-engine/
7. ALT Linux Documentation. (n.d.). Creating SSH tunnels using IP packet header integrity control in accordance with GOST R 34.12-2015. https://docs.altlinux.org/ru-RU/alt-workstation/10.2/html/alt-workstation/ssh_t.html
8. Uimin, A. G. (2024). Definition of a domestic technological platform within the framework of creating a cyber polygon: Network and system administration. In Current challenges in personnel training: Training of specialists in modern areas of information technology, cybersecurity, and ICT electronics relevant to the data economy (pp. 122–123).

Информация об авторах

Демидова Дарья Владимировна — студент кафедры математических методов обеспечения безопасности систем, Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, г. Москва, e-mail: dariavdemidova@gmail.com.

Комнацкая Елизавета Дмитриевна — студент кафедры математических методов обеспечения безопасности систем, Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, г. Москва, e-mail: komnatskayay@bk.ru.

ISSUES OF SSH CONNECTION PROTECTION BASED ON GOST ENCRYPTION IN ALT OS

D. V. Demidova[1], E. D. Komnatskaya[1]

[1]Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation

Abstract. The paper examines ways to improve the security of remote administration by using Russian cryptographic algorithms when establishing SSH connections in the ALT Linux operating system. The relevance of the study is determined by the need to comply with national information security requirements and to reduce dependence on foreign cryptographic solutions. The research problem consists in assessing the stability of SSH connections based on GOST algorithms and in analyzing how the selected cryptographic policy affects unauthorized access attempts and connection performance. The object of the study is the process of establishing and maintaining an SSH connection, while the subject is the server behavior when the cryptographic algorithm sets of the client and the server do not match. To solve the problem, an experimental SSH server and client configuration was performed in ALT Linux using gostcrypto packages that implement the Grasshopper and Magma algorithms and Stribog-based integrity control functions. The methodology included modeling legitimate and illegitimate connection attempts, analyzing network traffic with Wireshark, and measuring bandwidth and resource load. The experiments showed that a server configured to use only GOST algorithms effectively blocks connections with incompatible cryptographic parameters. When the client is configured correctly, the session is established stably and follows the specified security policy. The performance measurements demonstrate that GOST encryption provides throughput comparable to standard OpenSSH algorithms with a similar computational load. The results confirm the practical applicability of GOST-based SSH encryption for secure administration in domestic operating systems.

Keywords: SSH connection; GOST cryptography; ALT Linux; information security; remote administration; network encryption.

Information about the authors

Demidova Daria Vladimirovna — student of the Department of Mathematical Methods of System Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: dariavdemidova@gmail.com.

Komnatskaya Elizaveta Dmitrievna — student of the Department of Mathematical Methods of System Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: komnatskayay@bk.ru.