УДК 004.056.55

Пашина Софья Александровна, студентка кафедры математических методов обеспечения безопасности систем, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

Ризванов Таир Тимурович, студент кафедры безопасности информационных технологий, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва

НАСТРОЙКА ПРОВЕРКИ SSL-СЕРТИФИКАТА С ГОСТ ШИФРОВАНИЕМ В ZABBIX: ПЕРЕХВАТ И АНАЛИЗ ТРАФИКА

Аннотация. В статье рассматривается процесс настройки защищённого подключения к веб-интерфейсу системы мониторинга Zabbix с использованием SSL-сертификатов на основе отечественных криптографических алгоритмов ГОСТ. Работа выполнена на платформе ОС Альт 10.4 с использованием инструментов OpenSSL и gost-engine. Представлена методика генерации ключей, настройки Apache и внедрения TLS-соединения, соответствующего требованиям регуляторов (ФСТЭК, ФСБ, ЦБ РФ). Проведён анализ сетевого трафика с помощью Wireshark до и после внедрения шифрования, подтверждён переход на защищённый протокол TLS 1.2 с ГОСТ-алгоритмами. Полученные результаты подтверждают возможность практического внедрения криптографической защиты в рамках политики импортозамещения и ИБ.

Annotation. This article describes the process of configuring secure access to the Zabbix monitoring system’s web interface using SSL certificates based on Russian cryptographic algorithms (GOST). The implementation was carried out on the ALT Linux 10.4 platform using OpenSSL and the gost-engine module. The study presents a methodology for key generation, Apache configuration, and the deployment of TLS encryption in compliance with Russian regulatory standards (FSTEC, FSB, Central Bank). Network traffic analysis using Wireshark was performed before and after TLS activation, confirming a transition to a secure TLS

1.2 channel with GOST encryption. The results demonstrate the practical feasibility of implementing cryptographic protection under the import substitution and information security policies.
Ключевые слова: Zabbix, ГОСТ-шифрование, SSL-сертификат, ОС Альт, информационная безопасность, криптография.
Keywords: Zabbix, GOST encryption, SSL certificate, ALT Linux, information security, cryptography.

1 Введение

В условиях роста требований к ИБ и импортозамещению важно использовать отечественные криптоалгоритмы. С 2020 года в системах РФ применяется только российская криптография и TLS-сертификаты. Система Zabbix, применяемая для мониторинга, должна поддерживать защищённое соединение. Внедрение SSL/TLS с ГОСТ-алгоритмами позволяет соответствовать требованиям регуляторов и защищать передаваемые данные.
Цель работы – настроить безопасное взаимодействие с веб-интерфейсом Zabbix с проверкой SSL-сертификата, использующего ГОСТ-шифрование, а также перехватить и проанализировать сетевой трафик для подтверждения работы шифрования. Задачи исследования включают:

1. Установка системы Zabbix на платформе ОС Альт 10.4;
2. Генерация ключей и SSL-сертификатов с использованием ГОСТ-алгоритмов;
3. Настройка веб-сервера Apache;
4. Перехват и анализ трафика.

Объектом исследования является информационная безопасность при передаче данных в системе мониторинга Zabbix, предметом исследования –настройка и использование SSL-сертификатов с ГОСТ-шифрованием для защиты взаимодействия между веб интерфейсом Zabbix и клиентом, включая перехват и анализ трафика.

2 Теоретические основы

2.1 Архитектура системы Zabbix

Zabbix – это комплексная система мониторинга, состоящая из нескольких ключевых компонентов. Их взаимодействие образует распределённую архитектуру, обеспечивающую сбор, хранение и анализ данных о состоянии сети и серверов. В состав архитектуры обычно входят: Zabbix-сервер, Веб-интерфейс, База данных, Zabbix Agent, Прокси-сервер.

2.2 Принципы протоколов SSL/TLS

SSL/TLS – криптографические протоколы, предназначенные для обеспечения защищенной передачи данных между клиентом и сервером. Основная задача TLS – гарантировать трех ключевых свойства безопасности при обмене данными: конфиденциальность, аутентификация сторон, целостность данных. Для этого TLS использует асимметричное шифрование при установлении соединения и симметричное — для передачи данных. Во время TLS-рукопожатия стороны обмениваются ключевой информацией, а затем устанавливают общий секрет и переходят на симметричное шифрование.

2.3 Алгоритмы криптографии ГОСТ

Национальные стандарты криптографических алгоритмов, обозначаемые как ГОСТ, играют ключевую роль в обеспечении информационной безопасности в России. В сфере SSL/TLS нас интересуют три стандарта: алгоритм электронной цифровой подписи (ЭЦП) – ГОСТ Р 34.10-2012, алгоритм хэширования – ГОСТ Р 34.11-2012 и симметричный блочный шифр – ГОСТ Р 34.12-2015. Они поддерживаются версией OpenSSL 1.1.1 и могут быть реализованы с помощью пакета gost-engine.

3 Практическая реализация

3.1 Подготовка среды и установка Zabbix

На виртуальной машине ALT1 устанавливаем Zabbix-сервер с базой данных mysql и веб-интерфейсом на веб-сервере apache. На машине ALT2 установлен

Zabbix-агент. Машины соединены через интерфейсы enp0s8 и могут свободно общаться. Данные передаются в незашифрованном виде, что представляет угрозу кражи данных. Например, при авторизации с ALT2 в веб-интерфейсе в трафике видны логин и пароль Zabbix-сервера. Далее перейдем к генерации и установки SSL-сертификатов, чтобы добиться шифрованного трафика.

3.2 Генерация и настройка SSL-сертификатов с ГОСТ-алгоритмами

Для генерации сертификатов с ГОСТ-алгоритмами устанавливаем плагин (engine) с их поддержкой openssl-gost-engine и включаем ГОСТ-движок в глобальной конфигурации OpenSSL */etc/openssl/openssl.cnf*, после чего openssl может использовать ГОСТ-алгоритмы.

 # apt-get install openssl-gost-engine

 # control openssl-gost enabled

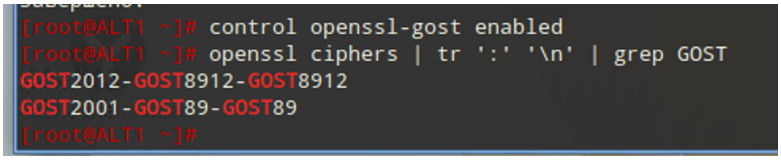

Рисунок №1 – Проверка доступности ГОСТ алгоритмов в openssl

На рисунке №1 видим, что openssl может работать с нужыми шифрами.

Создаем приватный ключ CA с использованием ГОСТ Р 34.10-2012 (256 бит), параметр набора A. Этот ключ будет использоваться для подписания всех других сертификатов:

 # openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out ca.key

Далее генерируем самоподписанный корневой сертификат CA, который будет использоваться как доверенный корень для подписания других сертификатов:

 # openssl req -new -x509 -md_gost12_256 -days 3650 -key ca.key -out ca.cer -subj "/C=RU/L=City/O=MyTestCA/CN=zabbix.gost"

Генерируем приватный ключ для сервера Zabbix, который будет использоваться веб-сервером Apache для установления HTTPS-соединения:

 # openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out zabbix.gost.key

Создаем запрос на подпись сертификата (CSR), включающий публичный ключ и информацию о владельце. Этот файл отправляется для подписания CA:

 # openssl req -new -md_gost12_256 -key zabbix.gost.key -out zabbix.gost.csr -subj "/C=RU/L=City/O=MyTestCA/CN=zabbix.gost"

CA (ca.key, ca.cer) подписывает запрос zabbix.gost.csr и выпускает сертификат zabbix.gost.cer, действительный 10 лет.

Корневой сертификат копируем в каталог, где хранятся доверенные корневые сертификаты, используемые всей системой. После перегенерируем хранилище доверенных CA на основе содержимого /anchors:

 # cp ca.cer /etc/pki/ca-trust/source/anchors/

 # update-ca-trust

Переименуем и скопируем все нужные файлы в папку, откуда их сможет использовать веб-сервер Apache. В конфигурационном файле пропишем пути до сертификатов и ключей, что приведено на рисунке №2:

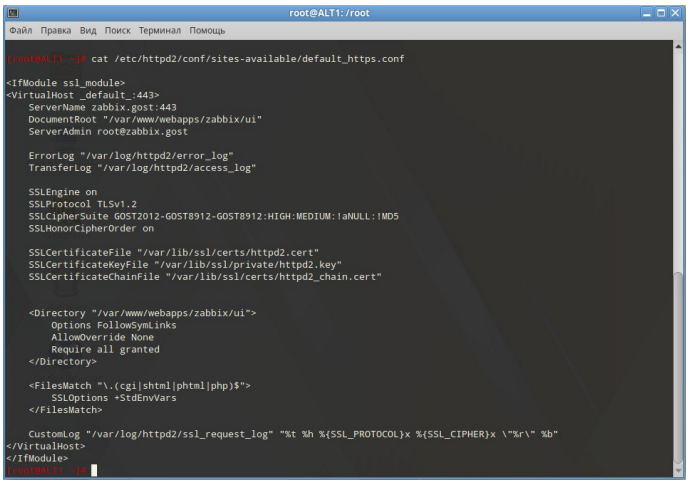

Рисунок №2 – Конфигурация веб-сервера apache

Далее активируем виртуальный хост и перезапускаем Apache:

 # ln -s /etc/httpd2/conf/sites-available/default_https.conf /etc/httpd2/conf/sites-enabled/

 # systemctl restart httpd2

На этом шаге может появиться ошибка:

httpd2-cert-sh[5742]: Generating httpd2 SSL certificate

httpd2-cert-sh[5752]: error: Unable to create sign request

Это связано с работой специального скрипта в ОС Альт, который при старте Apache пытается автоматически создать или обновить SSL-сертификат, но он не поддерживает работу с ГОСТ-алгоритмами, поэтому появляется ошибка. Автоматическую генерацию можно отключить в файле */lib/systemd/system/httpd2.service*

Теперь Apache должен запуститься без ошибки. Переходим к запуску через браузер. Для этого устанавливаем на две ВМ chromium-gost.

Запускаем браузер с флагами --cipher-suite-blacklist="" --enable-gost-ciphers --no-sandbox, чтобы он принимал даже самоподписанные сертификаты. Но при запуске браузер выдает ошибку, что протокол неподдерживаемый, хотя всё настроено верно.

Это связано с тем, что возможность использования TLS с ГОСТ обеспечивается с помощью вызова функций СКЗИ КриптоПро CSP, поэтому скачиваем криптопровайдер с официального сайта. Скачанный архив распаковываем и запускаем скрипт-установщик:

#./install_gui.sh

После установки открываем браузер, на рисунке №3 видно, что https работает и ошибки больше нет:

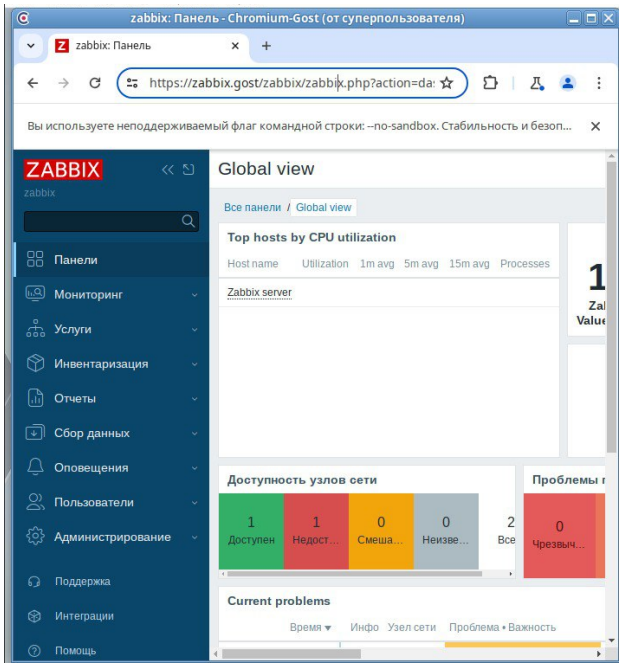

Рисунок №3 – Проверка HTTPS в браузере

3.3 Перехват и анализ сетевого трафика

Проверим, что после настройки TLS с ГОСТ-алгоритмами трафик между сервером и агентом предается в зашифрованном виде, и что браузер не отправляет данные в открытом виде. Wireshark фиксирует запрос GET-http с полностью читаемыми полями User-Agent, Host, Accept, Cookie, Accept-Language, и т.д. На рисунке №4 видно, что это обычный незашифрованный HTTP-трафик по порту 80.

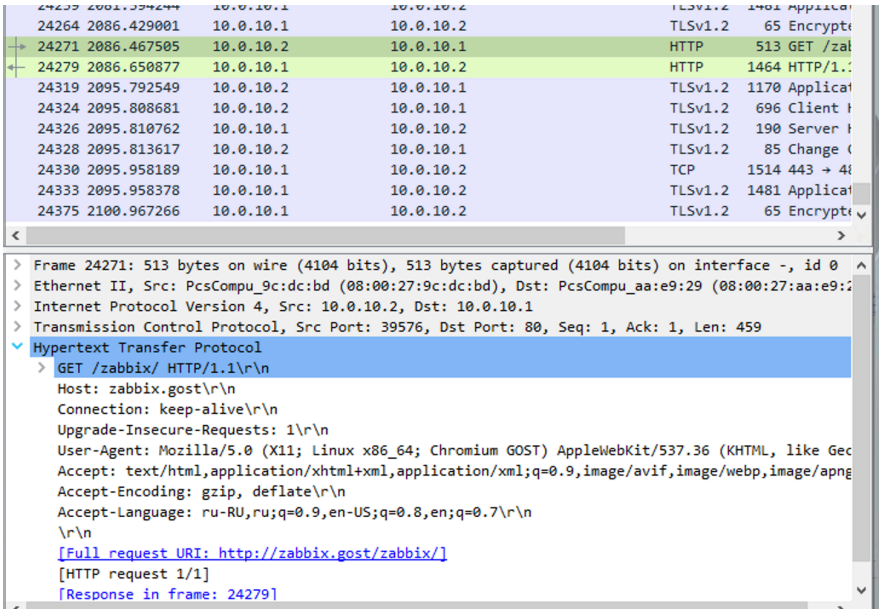

Рисунок №4 – Трафик в WireShark

Wireshark показывает Соединение от клиента 10.0.10.2 к серверу 10.0.10.1 по порту 443. На рисунке №5 видно TLS-рукопожатие между сервером и клиентом, после завершения согласования параметров обе стороны переходят в режим шифрования. Все последующие пакеты содержат *TLSv1.2 Record Layer: Application Data Protocol: http-over-tls*

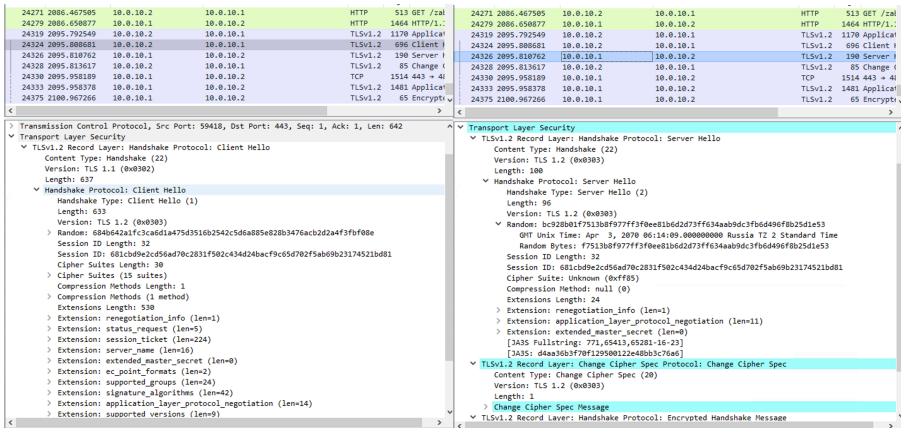

Рисунок №5 – Трафик в WireShark

На рисунке №6 видно, что сетевой трафик между агентом и сервером работает с протоколом https с использованием TLSv1.2. Wireshark не может прочитать содержимое, так как у него нет ключей сессии, все данные зашифрованы. В правой части открыта панель мониторинга Zabbix, веб-интерфейс доступен только через защищенное соединение. Сертификат принят.

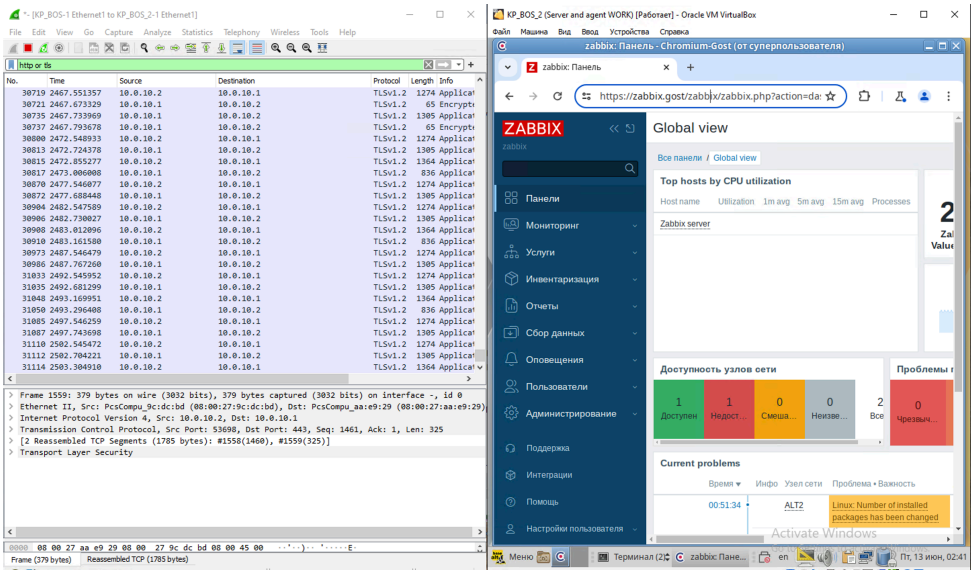

Рисунок №6 – Трафик в WireShark и веб интерфейс Zabbix в браузере

4 Заключение

В рамках работы была выполнена настройка защищённого HTTPS-доступа к веб-интерфейсу Zabbix с использованием ГОСТ-шифрования на базе ОС Альт 10.4. Были сгенерированы ключи и сертификаты по алгоритмам ГОСТ, настроен Apache с поддержкой соответствующих параметров шифрования и доверенной цепочки.

С помощью Wireshark проведён анализ трафика: после активации TLS-взаимодействия данные между клиентом и сервером передаются в зашифрованном виде, что подтверждает корректную работу защиты.

Эксперимент подтвердил, что ОС Альт предоставляет все необходимые средства для реализации ГОСТ-шифрования, а полученные результаты пригодны для внедрения в системах, подчинённых требованиям регуляторов по ИБ.

Литература

1. 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;
2. Работа с КриптоПро CSP в linux // КриптоПро URL: https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/390 (Дата обращения 13.06.2025);
3. TLS с ГОСТ на nginx/Apache // КриптоПро URL: https://www.cryptopro.ru/products/csp/tls/gost-nginx-apache (Дата обращения 10.06.2025);
4. Система мониторинга Zabbix // docs.altlinux.org URL: https://docs.altlinux.org/ru-RU/alt-server-e2k/10.1/html/alt-server-e2k/ch37.html (Дата обращения 10.06.2025);
5. ОС Альт. Руководство администратора. URL: https://www.altlinux.org/Документация (Дата обращения 10.06.2025);

Literature

1. Uymin, A. G. Demonstration Examination of Basic Level: Network and System Administration – Practicum. Textbook for Universities. Saint Petersburg: Lan Publishing, 2024. 116 pp. (Higher Education). ISBN 978-5-507-48647-2. EDN BZJRIQ;
2. CryptoPro. Working with CryptoPro CSP in Linux. https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/390 (accessed June 13, 2025);
3. CryptoPro. TLS with GOST on Nginx/Apache. https://www.cryptopro.ru/products/csp/tls/gost-nginx-apache (accessed June 10, 2025);
4. Zabbix Monitoring System. Alt Linux Documentation. https://docs.altlinux.org/ru-RU/alt-server-e2k/10.1/html/alt-server-e2k/ch37.html (accessed June 10, 2025);

5. ALT Linux OS. Administrator’s Guide. https://www.altlinux.org/Documentation (accessed June 10, 2025);