**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский Авиационный Институт»**

**(Национальный Исследовательский Университет)**

**Институт: №8 «Информационные технологии   
и прикладная математика»   
Кафедра: 806 «Вычислительная математика   
и программирование»**

Отчёт по курсовому проекту по курсу

«Криптография»

Группа: М8О-312Б-22

Студент(ка): Л. Д, Андрюшин

Преподаватель: А. В. Борисов

Оценка:

Дата: 24.05.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[**1** **Тема** 3](#_Toc199008432)

[**2** **Задание** 3](#_Toc199008433)

[**3** **Ход лабораторной работы** 4](#_Toc199008434)

[**4** **Выводы** 5](#_Toc199008435)

# **Тема**

Курсовой проект. Аутентификация с асимметричными алгоритмами шифрования в сети Интернет.

# **Задание**

Порядок выполнения лабораторной работы:

1. Выбрать не менее 3-ёх web-серверов сети Интернет различной организационной и государственной принадлежности.

2. Запустить Wireshark/tcpdump в режиме записи.

3. Используя Firefox/Chrome/Safari/ИнойБраузер установить https соединение с выбранным сервером и убедиться в установке соединения.

4. Сохранить данные необходимы для последующего сравнительного анализа:

\* Имя сервера, его характеристики.

\* Версия TLS.

\* Выбранные алгоритмы шифрования.

\* Полученный сертификат: версия, действителен ли сертификат, правильность ключа, удостоверяющий центр. \* Время установки соединения (от ClientHello до Finished)

5. Если список исследуемых серверов не исчерпан выбрать другой сервер и повторить соединение.

6. Если браузер поддерживал соединение TLS 1.2 / 1.3 принудительно изменить параметры TLS (для соединения в Firefox на TLS 1.0 / 1.1 в браузере перейти по адресу “about:config” и изменить раздел SSL\TLS, security.tls.version.enable-deprecated) и провести попытки соединения с выбранными серверами.

7. Провести сравнительный анализ полученной информации.

8. В качестве отчета представить результаты сравнительного анализа, выводы в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и

# **Ход лабораторной работы**

Для начала я скачал Wireshark, разобрался как с ним работать и решил с какими сайтами я буду работать, я остановился на следующих трёх сайтах: <https://www.wikipedia.org/>, <https://www.twitch.tv/>, <https://2ch.hk/>

Потом я ввел в консоли команду «ping \*сайт\*», чтобы выяснить их ip адрес. Он нам нужен, чтобы среди кучи различной информации, которую перехватывает Wireshark, мы отслеживали только нужную нам. Например с помощью команды ip.addr == 185.15.59.224 && tls. По сути это одна из двух команд, которую я использовал. Еще одна выглядела вот так: tls.handshake.type == 1 || tls.handshake.type == 20, ее я использовал для отслеживания времени подключения к сайту. Вот итоговая информация, которую я собрал по всем трем сайтам:

***wikipedia.org***

1. Версия TLS 1.3

(*Не смотря на подобный вывод:*

*Transport Layer Security*

*TLSv1.3 Record Layer*

*Handshake Protocol: Server Hello*

*Version: TLS 1.2 (0x0303),*

*Который казалось бы указывает нам на версию 1.2, в Extension: supported\_versions (0x002b) мы получаем подобный вывод: Supported Version: TLS 1.3 (0x0304), аналогично и во всех остальных трех сайтах*)

1. Алгоритм шифрования: TLS\_AES\_128\_GCM\_SHA256
2. Сертификат Wikipedia:

- Удостоверяющий центр: DigiCert TLS Hybrid ECC SHA384 2020 CA1

- Алгоритм подписи: ECDSA SHA-384

- Публичный ключ: ECC P-256

- Срок действия: 26.09.2024 – 17.10.2025

1. Время установки соединения – 0.185 сек

***twitch.tv***

1. Версия TLS 1.3
2. Алгоритм шифрования: TLS\_AES\_128\_GCM\_SHA256
3. Сертификат Twitch.tv:

- Удостоверяющий центр: GlobalSign Atlas R3 DV TLS CA 2025 Q2

- Алгоритм подписи: RSA-PSS SHA-256

- Публичный ключ: RSA 2048 бит

- Срок действия: 07.05.2025 – 08.06.2026

4. Время установки соединения – 0.267 сек

***2ch.hk***

1. Версия TLS 1.3
2. Алгоритм шифрования: TLS\_AES\_128\_GCM\_SHA256
3. Сертификат 2ch.hk:

- Удостоверяющий центр: Google Trust Services LLC (GTS WE1)

- Алгоритм подписи: ECDSA SHA-256

- Публичный ключ: ECC P-256

- Срок действия: 21.05.2025 – 19.08.2025

1. Время установки соединения – 0.203 сек

Для проверки поддержки устаревших версий TLS в браузере Firefox я изменил параметры security.tls.version.enable-deprecated и security.tls.version.min. При установке минимальной версии TLS 1.0 ни один из исследуемых сайтов (wikipedia.org, twitch.tv, 2ch.hk) не смог установить соединение, возвращая ошибку SSL\_ERROR\_UNSUPPORTED\_VERSION.

# **Выводы**

В ходе выполнения работы было проведено исследование поддержки устаревших версий TLS (1.0 и 1.1) на выбранных веб-серверах. Принудительное изменение параметров TLS в браузере Firefox через настройку security.tls.version.enable-deprecated и установка security.tls.version.min=0 (для TLS 1.0) продемонстрировали, что современные серверы (wikipedia.org, twitch.tv и 2ch.hk) корректно настроены с точки зрения безопасности - они категорически отвергают соединения по устаревшим и небезопасным протоколам. При попытке подключения с TLS 1.0 браузер возвращал ошибку SSL\_ERROR\_UNSUPPORTED\_VERSION, что свидетельствует о намеренном отключении поддержки уязвимых версий протокола на серверной стороне.

Сравнительный анализ полученных данных позволяет сделать следующие выводы. Все исследованные серверы используют актуальную версию TLS 1.3, что соответствует современным требованиям информационной безопасности. При этом наблюдаются различия в используемых алгоритмах: Wikipedia и 2ch.hk применяют более современные ECC-ключи (P-256) с подписью ECDSA, в то время как Twitch использует традиционное RSA-2048 с подписью RSA-PSS. Время установки соединения варьировалось от 0.185 до 0.267 секунды, что демонстрирует высокую эффективность TLS 1.3. Особого внимания заслуживает разница в сроках действия сертификатов: если Wikipedia и Twitch используют долгосрочные сертификаты (1-1.5 года), то 2ch.hk придерживается политики короткоживущих сертификатов (3 месяца), что считается более безопасным подходом, так как уменьшает возможный ущерб в случае компрометации ключа.

С учетом организационной принадлежности исследуемых серверов можно заключить, что международные IT-компании демонстрируют образцовую настройку криптографических параметров. Все серверы корректно реализуют современные стандарты безопасности, полностью отказавшись от поддержки устаревших версий TLS. Полученные результаты подтверждают, что современный веб в целом перешел на безопасные версии протоколов, а использование TLS 1.0 и 1.1 становится исключением, а не правилом. Это соответствует глобальным тенденциям усиления защиты интернет-соединений и снижения рисков криптографических атак.