**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»**

Курсовой проект  
по курсу «Криптография»

Группа: М8О-307Б-22

Студент: Е. С. Кострюков

Преподаватель: А. В. Борисов

Оценка:

Дата: 24.05.2025

Москва, 2025

**ОГЛАВЛЕНИЕ**

[**Тема** 3](#_Toc198981704)

[**Задание** 3](#_Toc198981705)

[**Теория** 3](#_Toc198981706)

[**Ход лабораторной работы** 4](#_Toc198981707)

[**Выводы** 8](#_Toc198981708)

# **Тема**

Аутентификация с асимметричными алгоритмами шифрования в сети Интернет

# **Задание**

Исследовать, как реализована аутентификация и шифрование на различных веб-серверах с использованием асимметричных алгоритмов в рамках TLS-протокола.

В рамках проекта необходимо:

1. Выбрать не менее трёх web-серверов, принадлежащих разным государствам и организациям.
2. Выполнить анализ TLS-соединения с каждым из них, зафиксировав:
   * версию протокола TLS,
   * используемые алгоритмы шифрования,
   * данные сертификата (версия, срок действия, валидность, удостоверяющий центр, размер ключа),
   * время установления соединения.
3. При возможности — проверить реакцию сервера на устаревшие версии TLS (1.0 / 1.1), если это позволяет браузер.
4. Провести сравнительный анализ полученных данных и сделать выводы о безопасности, корректности настройки и уровне доверия к каждому из серверов.

# **Теория**

При установке защищенного соединения между клиентом (браузером) и сервером в сети Интернет используется протокол TLS (Transport Layer Security), основанный на криптографических методах. Его задача — обеспечить:

* **аутентификацию** сервера (иногда — и клиента),
* **конфиденциальность** передаваемой информации,
* **целостность** данных.

Основой аутентификации и защиты данных служат **асимметричные алгоритмы** (например, RSA, ECDSA), которые применяются при начальном обмене ключами и проверке подлинности сертификата сервера. После завершения рукопожатия, соединение переходит к **симметричному шифрованию**, где используются ключи, согласованные ранее.

Протокол TLS существует в разных версиях: от устаревших (1.0 и 1.1), до современных (1.2 и 1.3). Версия TLS, а также используемые алгоритмы шифрования (cipher suites) и параметры сертификата определяют уровень безопасности соединения.

Также важны такие факторы, как:

* кто выдал сертификат (Certificate Authority — CA),
* срок его действия,
* тип ключа и его длина (например, RSA 2048 бит),
* поддержка современных алгоритмов, таких как AES-GCM, CHACHA20-POLY1305.

Использование устаревших версий TLS или слабых параметров шифрования может привести к уязвимостям и потенциальной компрометации защищённого соединения.

# **Ход лабораторной работы**

1. **Подготовка и запуск инструментов для анализа**
   * На этапе подготовки был выбран набор веб-ресурсов для анализа безопасности TLS-соединений: gosuslugi.ru, nalog.gov.ru, lkfl2.nalog.ru.
   * Для перехвата и анализа TLS-трафика был запущен Wireshark в режиме записи.
   * Были установлены HTTPS-соединения с указанными серверами с использованием веб-браузера. В процессе фиксировались характеристики TLS-сессий.
2. **Анализ установленных соединений**
   * В процессе установления соединений были зафиксированы параметры TLS, включая версию протокола, используемые алгоритмы шифрования, а также информацию о сертификате.
   * Для каждого сервера была выделена цепочка сертификатов, определены удостоверяющие центры, сроки действия сертификатов, назначение ключей и дополнительные атрибуты.
   * Зафиксированы типы ключей и длина ключей (например, RSA 2048 бит), алгоритмы подписи, а также поля Key Usage и Extended Key Usage.
3. **Систематизация результатов**
   * Полученные сведения были структурированы в виде отдельных таблиц по каждому серверу, с единым набором параметров для возможности дальнейшего сравнительного анализа.

Анализ TLS-соединения — Сервер: **gosuslugi.ru**:

| **Параметр** | **Значение** |
| --- | --- |
| Имя сервера (CN) | \*.gosuslugi.ru |
| Версия TLS | TLS 1.3 |
| Алгоритм шифрования (Cipher) | TLS\_AES\_128\_GCM\_SHA256 |
| Сила шифра (bit) | 128 |
| Центр сертификации (CA) | GlobalSign GCC R3 DV TLS CA 2020 (GlobalSign nv-sa, Бельгия) |
| Доверие к сертификату | passed / trust is via wildcard |
| Дата начала действия | 22 октября 2024 |
| Дата окончания действия | 23 ноября 2025 |
| Алгоритм подписи | SHA256 with RSA |
| Тип и длина ключа | RSA 2048 бит |
| Назначение ключа (Key Usage) | Digital Signature, Key Encipherment |
| Дополнительное назначение (EKU) | TLS Web Server Authentication, TLS Web Client Authentication |

Анализ TLS-соединения — Сервер: **nalog.gov.ru**:

| **Параметр** | **Значение** |
| --- | --- |
| Имя сервера (CN) | \*.nalog.gov.ru |
| Версия TLS | TLS 1.3 |
| Алгоритм шифрования (Cipher) | TLS\_AES\_256\_GCM\_SHA384 |
| Сила шифра (bit) | 256 |
| Центр сертификации (CA) | R11 (Let's Encrypt, США) |
| Доверие к сертификату | passed / trust via SAN (SNI mandatory) |
| Дата начала действия | 4 апреля 2025 |
| Дата окончания действия | |  | | --- | |  |   3 июля 2025 |
| Алгоритм подписи | SHA256 with RSA |
| Тип и длина ключа | RSA 2048 бит |
| Назначение ключа (Key Usage) | Digital Signature, Key Encipherment |
| Дополнительное назначение (EKU) | TLS Web Server Authentication, TLS Web Client Authentication |

Анализ TLS-соединения — Сервер: **lkfl2.nalog.ru**:

| **Параметр** | **Значение** |
| --- | --- |
| Имя сервера (CN) | \*.lkfl2.nalog.ru |
| Версия TLS | TLS 1.2 |
| Алгоритм шифрования (Cipher) | ECDHE-RSA-AES128-GCM-SHA256 |
| Сила шифра (bit) | 128 |
| Центр сертификации (CA) | GlobalSign GCC R3 DV TLS CA 2020 (GlobalSign nv-sa, Бельгия) |
| Доверие к сертификату | passed / trust via wildcard (SAN + CN) |
| Дата начала действия | 12 декабря 2024 |
| Дата окончания действия | 13 января 2026 |
| Алгоритм подписи | SHA256 with RSA |
| Тип и длина ключа | RSA 2048 бит |
| Назначение ключа (Key Usage) | Digital Signature, Key Encipherment |
| Дополнительное назначение (EKU) | TLS Web Server Authentication, TLS Web Client Authentication |

# **Выводы**

В ходе лабораторной работы была выполнена диагностика TLS-соединений для трёх государственных ресурсов с использованием сетевого анализа. Результаты показали следующее:

* **Протоколы безопасности:** Все исследуемые серверы используют современные версии TLS (1.2 или 1.3), однако один из них (lkfl2.nalog.ru) не поддерживает TLS 1.3, что может считаться менее безопасным по сравнению с другими.
* **Шифрование:** Применяются стойкие алгоритмы шифрования — от AES-128 до AES-256, с режимами GCM. Сила шифра соответствует современным требованиям.
* **Сертификаты:** Все серверы используют действительные X.509-сертификаты, выданные авторитетными удостоверяющими центрами (например, Let's Encrypt и GlobalSign). Сроки действия сертификатов находятся в допустимом диапазоне, признаки компрометации или ошибок в цепочке доверия отсутствуют.
* **Назначение ключей:** Все сертификаты содержат корректные поля Key Usage и Extended Key Usage, указывающие на то, что они предназначены для веб-аутентификации.

Таким образом, можно сделать вывод, что исследованные веб-серверы в целом настроены корректно и соответствуют современным требованиям безопасности TLS. Тем не менее, рекомендуется обновление конфигурации сервера lkfl2.nalog.ru с переходом на поддержку TLS 1.3, что повысит уровень защиты и снизит риск использования устаревших протоколов.