**Отчет по лабораторной работе №5 по курсу «Криптография»**

Выполнил Лисин Роман Сергеевич, М8О-306Б-20.

***Задание***

1. Выбрать не менее 5-ти веб-серверов различной организационной и государственной

принадлежности.

2. Запустить Wireshark и используя Firefox установить https соединение с выбранным

сервером.

3. Провести анализ соединения.

4. Сохранить данные необходимы для последующего сравнительного анализа:

Имя сервера, его характеристики.

Версия TLS.

Выбранные алгоритмы шифрования.

Полученный сертификат: версия. Валидность сертификата, валидность ключа,

удостоверяющий центр.

Время установки соединения (от ClientHello до Finished)

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

соединие.

6. Если браузер поддерживал соединение TLS 1.2 принудительно изменить параметры TLS

соединения в Firefox на TLS 1.0 (в браузере перейти по “about:config” и изменить раздел

SSL\TLS) 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

государственной принадлежности.

***Ход работы***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Имя сервера, его характеристики (домен, заголовок, content-type, последнее изменение) | Версия TLS | Алгоритмы шифрования | Версия сертификата | Валидность сертификата, валидность ключа, удостоверяющий центр | Время установки соединения, сек. |
| ec2-3-72-181-255.eu-central-1.compute.amazonaws.com, [www.group-ib.com](http://www.group-ib.com/), Cybersecurity Services, Solutions & Products. Global Provider | Group-IB, text/html; charset=UTF-8, 28 апреля 2023 г. в 17:51:09 GMT+3 | 1.3 | RSA, SHA-256 | 3.0 | Валиден (с Tue, 28 Jun 2022 00:00:00 GMT до Wed, 28 Jun 2023 23:59:59 GMT), не отозван, Sectigo Limited | 0.006635084999999998 |
| 217.9.89.254, mai.ru, МАИ, text/html; charset=UTF-8, 29 апреля 2023 г. в 17:08:26 GMT+3 | 1.2 | RSA, SHA-256 | 3.0 | Валиден (с Tue, 04 Oct 2022 15:43:23 GMT до Sun, 05 Nov 2023 15:43:22 GMT), не отозван, GlobalSign nv-sa | 0.007487533999999997 |
| 20.53.203.50, [www.microsoft.com](http://www.microsoft.com/), Microsoft — облачные технологии, приложения и игры, text/html; charset=UTF-8, 29 апреля 2023 г. в 17:16:06 GMT+3 | 1.3 | RSA, SHA-384 | 3.0 | Валиден (с Tue, 04 Oct 2022 23:23:11 GMT до Fri, 29 Sep 2023 23:23:11 GMT), не отозван, Microsoft Corporation | 0.006321244999999996 |
| 185.85.15.26, [www.kaspersky.com](http://www.kaspersky.com/), Kaspersky Cyber Security Solutions for Home and Business | Kaspersky, text/html; charset=UTF-8, 29 апреля 2023 г. в 23:02:39 GMT+3 | 1.3 | RSA, SHA-256 | 3.0 | Валиден (с Tue, 28 Mar 2023 00:00:00 GMT до Wed, 27 Mar 2024 23:59:59 GMT), не отозван, DigiCert Inc | 0.003409893000000004 |
| 213.59.254.7, [www.gosuslugi.ru](http://www.gosuslugi.ru/), Портал государственных услуг Российской Федерации, text/html; charset=UTF-8, 29 апреля 2023 г. в 17:10:25 GMT+3 | 1.2 | RSA, SHA-256 | 3.0 | Валиден (с Thu, 01 Dec 2022 14:42:29 GMT до Tue, 02 Jan 2024 14:42:28 GMT), не отозван, GlobalSign nv-sa | 0.007643109000000002 |

***Вывод***

Первое отличие, которое бросается в глаза, это то, что у сайтов, у которых TLS 1.2 версии, TLS handshake происходит в среднем немного дольше, чем у сайтов с TLS 1.3. Также хочется отметить, что среди компаний с TLS 1.3 у Лаборатории Касперского соединение установилось быстрее, потому что их сервер находится в Цюрихе, Швейцария, а у Microsoft в Сиднее, Австралия и Group-IB использует облачный сервис AWS. Почти у всех одинаковые алгоритмы шифрования RSA, SHA-256, кроме Microsoft, они используют SHA-384 (производный алгоритм от SHA-512). Версии SSL сертификатов у всех самые новые. Все сертификаты валидны.

Таким образом, все исследуемые веб-серверы имеют хорошую защиту и корректную настройку.