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»

Лабораторная работа № 5 по курсу «Криптография»

Группа: М8О-306Б-20

Студент: И. П. Попов

Преподаватель: А. В. Борисов

Оценка:

Дата:

Москва, 2022

Задача

Порядок выполнения лабораторной работы:

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 соединение.
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.

Выбранные серверы:

1. Сервер госуслуг России
2. Сервер госуслуг Москвы
3. Сервер МАИ
4. Сервер telegram.org
5. Сервер Сбера

www.gosuslugi.ru(109.207.1.118)

Имя сервера находится в пакете Client Hello

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
      > Random: 5606ec35acad26148fe21c5bce0a14923863aaab099a8529b90e62b8c5344c75
        Session ID Length: 32
        Session ID: b0b6a2d78330566af9dbf752202a3ed0086b15c0c963e811cad83af2b7eb37ac
        Cipher Suites Length: 36
      > Cipher Suites (18 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 399
      v Extension: server_name (len=21)
          Type: server_name (0)
          Length: 21
        v Server Name Indication extension
            Server Name list length: 19
            Server Name Type: host_name (0)
            Server Name length: 16
            Server Name: www.gosuslugi.ru
      > Extension: extended_master_secret (len=0)
```

Заметим, что клиент предлагает версию протокола TLS 1.0

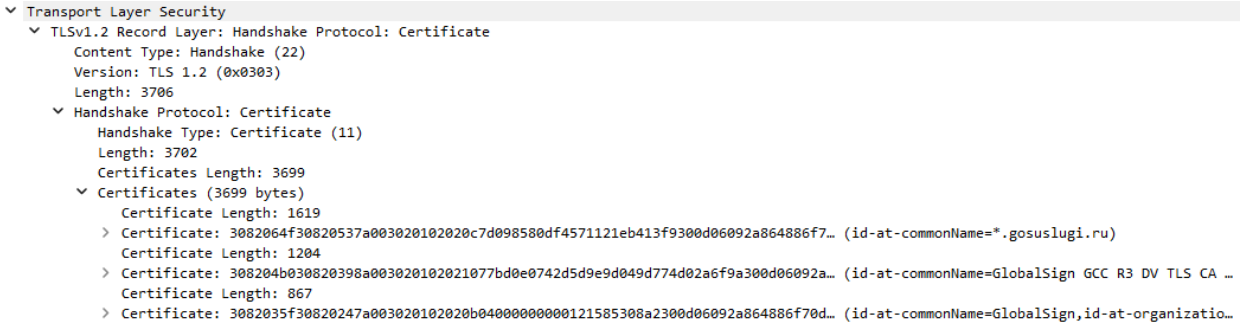
```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 100
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 96
        Version: TLS 1.2 (0x0303)
      > Random: 74ef80f47fec7b7dde89973303512b3757565c42c8de9e8232f1651fc2ea5538
        Session ID Length: 32
        Session ID: 361cd956caa18d7a9e653165b069b695a240454cf16addada724b48b82f90493
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 24
      > Extension: renegotiation_info (len=1)
      > Extension: application_layer_protocol_negotiation (len=5)
      > Extension: ec_point_formats (len=2)
      > Extension: extended_master_secret (len=0)
        [JA3S Fullstring: 771,49199,65281-16-11-23]
        [JA3S: c1108ede158e8e91e75c07b453533fb8]
```

В пакете Server Hello можно найти следующую информацию:

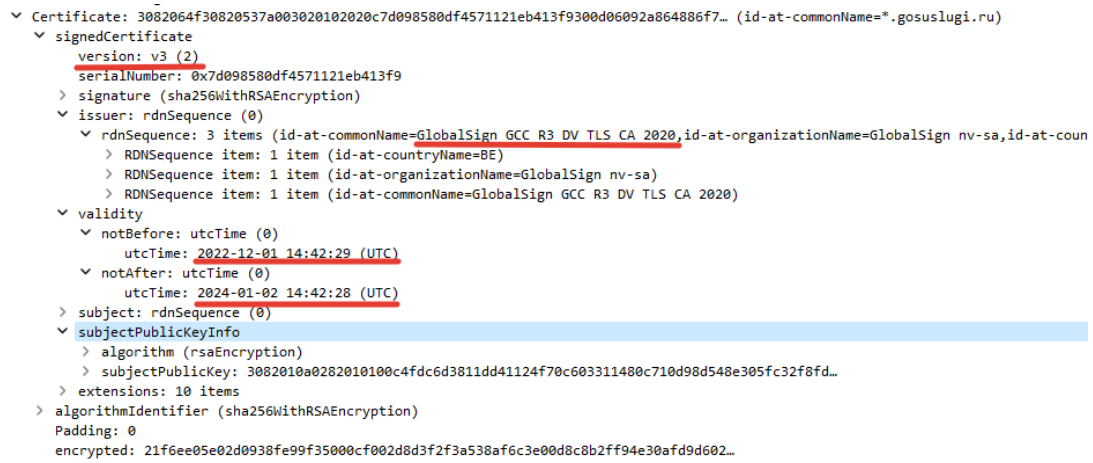
1. **Версию TLS**, которая будет использована при установке соединения, заметим, что она выше, чем предлагал клиент, а именно TLS 1.2.

2. Сгенерированное значение Random для генерации разделяемого ключа, который необходим для алгоритма Диффи-Хеллмана.
3. Набор шифров Cipher Suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) говорит о том, что будет использоваться **алгоритм Диффи-Хеллмана на эллиптических кривых ephemeral** (что говорит о том, что новые значения Random будут генерироваться и у сервера и у клиента заново при каждой новой сессии, если прошло достаточно времени после предыдущей, потому что в противном случае будет использован протокол восстановления сессии), шифрование выполняется с помощью алгоритма AES_128, режим работы GCM и для генерации MAC используется функция SHA256.

Затем сервер отправляет клиенту свой сертификат:



Здесь указаны три сертификата, для начала разберемся с сертификатом сервера.



Из этого сертификата мы можем узнать его **версию**, номер, алгоритм записи RSA, информация о выдавшем сертификат удостоверяющем центре, срок действия сертификата (**сертификат валиден**, так как действует до

2024 года), открытый ключ сервера и в encrypted - цифровую подпись удостоверяющего центра. Наш **удостоверяющий центр** - GlobalSign GCC R3 DV TLS CA 2020, но он не является корневым, поэтому нам передаются сертификаты всех его предков, вплоть до одного из корневых, о которому мы, как клиент доверяем.

Далее следует обмен **ключами** от сервера к клиенту

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
    Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
      EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: secp256r1 (0x0017)
          Pubkey Length: 65
          Pubkey: 042afa384b421c7f94db305f722968422edc168f1d3801cfbeaa324255af74f1301f1bca…
        > Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
          Signature Length: 256
          Signature: 57af5f0f96b30ec6c9913ba641311638f45400b19fa1063d9874d6a79e1327a109e858b5…
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    > Handshake Protocol: Server Hello Done
```

И обратно

```
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 04a5b77cde34c7616ed6efe467072998acf148e547711ce06d33384c122de7a9e455157a…
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

Рассчитаем **время соединения**

No.	Time	Source	Destination	Protocol	Length	Info
566	34.559298	192.168.0.223	109.207.1.118	TLSv1.2	571	Client Hello
568	34.562350	109.207.1.118	192.168.0.223	TLSv1.2	1434	Server Hello
571	34.562387	109.207.1.118	192.168.0.223	TLSv1.2	1434	Certificate
572	34.562387	109.207.1.118	192.168.0.223	TLSv1.2	77	Server Key Exchange, Server Hello Done
574	34.565155	192.168.0.223	109.207.1.118	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
577	34.567777	109.207.1.118	192.168.0.223	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
578	34.568015	109.207.1.118	192.168.0.223	TLSv1.2	110	Application Data

34.568015 - 34.559298 = 0,008717

Первый пример я постарался разобрать подробно, последующие же будут содержать лишь информацию про рассматриваемые характеристики.

www.mos.ru(94.79.51.14)

Имя сервера

```
▼ Extension: server_name (len=15)
    Type: server_name (0)
    Length: 15
  ▼ Server Name Indication extension
      Server Name list length: 13
      Server Name Type: host_name (0)
      Server Name length: 10
      Server Name: www.mos.ru
```

Версия TLS

```
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
   Content Type: Handshake (22)
   Version: TLS 1.2 (0x0303)
   Length: 74
```

Выбранный алгоритмы шифрования

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр.

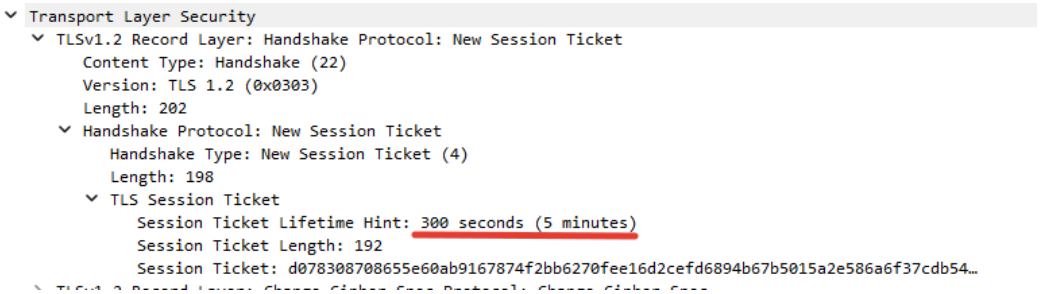
```
Certificate: 3082062a30820512a003020102020c713792700a5d690f4a665047300d06092a864886f7… (id-a
▼ signedCertificate
    version: v3 (2)
    serialNumber: 0x713792700a5d690f4a665047
  › signature (sha256WithRSAEncryption)
  ▼ issuer: rdnSequence (0)
    ▼ rdnSequence: 3 items (id-at-commonName=AlphaSSL CA - SHA256 - G2,id-at-organizationN
      › RDNSequence item: 1 item (id-at-countryName=BE)
      › RDNSequence item: 1 item (id-at-organizationName=GlobalSign nv-sa)
      › RDNSequence item: 1 item (id-at-commonName=AlphaSSL CA - SHA256 - G2)
  ▼ validity
    ▼ notBefore: utcTime (0)
        utcTime: 2022-11-03 11:46:27 (UTC)
    ▼ notAfter: utcTime (0)
        utcTime: 2023-12-05 11:46:26 (UTC)
  › subject: rdnSequence (0)
  ▼ subjectPublicKeyInfo
    › algorithm (rsaEncryption)
    › subjectPublicKey: 3082010a0282010100bcb4767b0ee8be734da7b89a1326d8cb5133b193a02e5fc5
  › extensions: 10 items
› algorithmIdentifier (sha256WithRSAEncryption)
  Padding: 0
  encrypted: 8a58c3cc00970f6d807c24e80c45b7f93c8988d6c4232750e3be41e3cd65580a7a94d9fb…
Certificate Length: 1105
```

Время установки соединения

3159…	5102.614832	192.168.0.223	94.79.51.14	TLSv1.2	571	Client Hello
3159…	5102.620480	94.79.51.14	192.168.0.223	TLSv1.2	1434	Server Hello
3159…	5102.620677	94.79.51.14	192.168.0.223	TLSv1.2	1317	Certificate, Server Key Exchange, Serv
3159…	5102.624405	192.168.0.223	94.79.51.14	TLSv1.2	180	Client Key Exchange, Change Cipher Spe
3159…	5102.628518	94.79.51.14	192.168.0.223	TLSv1.2	381	New Session Ticket, Change Cipher Spec
3159…	5102.642489	192.168.0.223	94.79.51.14	TLSv1.2	231	Application Data

5102,642489 - 5102,614832 = 0,027657

Стоит отметить, что в отличие от сайта госуслуг в процессе подключения создается New Session Ticket, благодаря которому можно не тратить время на пересчет ключей при последующей сессии, а просто восстановить их, если новая сессия была начата в пределах указанного временного промежутка.



www.mai.ru (217.9.89.254)

Имя сервера

```
Server Name Indication extension
    Server Name list length: 9
    Server Name Type: host_name (0)
    Server Name length: 6
    Server Name: mai.ru
```

Версия TLS

```
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 94
```

Выбранный алгоритмы шифрования
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр.

```
Certificate: 3082063d30820525a003020102020c3d35efef0eb9dda7d0b451ea300d06092a864886f7… (id-at-commonName=*.ma
  signedCertificate
      version: v3 (2)
      serialNumber: 0x3d35efef0eb9dda7d0b451ea
    > signature (sha256WithRSAEncryption)
    v issuer: rdnSequence (0)
      v rdnSequence: 3 items (id-at-commonName=GlobalSign GCC R3 DV TLS CA 2020,id-at-organizationName=Globa
        > RDNSequence item: 1 item (id-at-countryName=BE)
        > RDNSequence item: 1 item (id-at-organizationName=GlobalSign nv-sa)
        > RDNSequence item: 1 item (id-at-commonName=GlobalSign GCC R3 DV TLS CA 2020)
    v validity
      v notBefore: utcTime (0)
            utcTime: 2022-10-04 15:43:23 (UTC)
      v notAfter: utcTime (0)
            utcTime: 2023-11-05 15:43:22 (UTC)
    > subject: rdnSequence (0)
    > subjectPublicKeyInfo
    > extensions: 10 items
  > algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
    encrypted: 3f5922fb4d7c8ca041c007015192fbe7a182910a35ee5dd320d1754214be715063535532…
Certificate Length: 1204
```

Время установки соединения

```
48830 791.382206    192.168.0.223    217.9.89.254     TLSv1.2   571 Client Hello
48849 791.384338    217.9.89.254     192.168.0.223    TCP        60 443 → 53273 [ACK] Seq=1 Ack=518 Win=64128 Len=0
48852 791.385334    217.9.89.254     192.168.0.223    TLSv1.2  1434 Server Hello
48853 791.385457    217.9.89.254     192.168.0.223    TCP      1434 443 → 53273 [ACK] Seq=1381 Ack=518 Win=64128 Len=1380
48855 791.385490    192.168.0.223    217.9.89.254     TCP        54 53273 → 443 [ACK] Seq=518 Ack=2761 Win=262144 Len=0
48856 791.385615    217.9.89.254     192.168.0.223    TLSv1.2  1384 Certificate, Server Key Exchange, Server Hello Done
48859 791.387492    192.168.0.223    217.9.89.254     TLSv1.2   147 Client Key Exchange, Change Cipher Spec, Encrypted Har
48868 791.389453    217.9.89.254     192.168.0.223    TCP        60 443 → 53273 [ACK] Seq=4091 Ack=611 Win=64128 Len=0
48869 791.389731    217.9.89.254     192.168.0.223    TLSv1.2   312 New Session Ticket, Change Cipher Spec, Encrypted Hanc
48871 791.389741    217.9.89.254     192.168.0.223    TLSv1.2   123 Application Data
```

791,389741 - 791,382206 = 0,007535

www.telegram.org (149.154.167.99)

Имя сервера

```
▼ Extension: server_name (len=26)
      Type: server_name (0)
      Length: 26
   ▼ Server Name Indication extension
         Server Name list length: 24
         Server Name Type: host_name (0)
         Server Name length: 21
         Server Name: zws2.web.telegram.org
```

Версия TLS

```
▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 80
      Version: TLS 1.2 (0x0303)
```

Выбранный алгоритмы шифрования
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр.

```
▼ Certificate: 3082069b30820583a003020102020900a81e3a49e69cc64b300d06092a864886f70d0101… (id-at-commonName=*.we
   ▼ signedCertificate
        version: v3 (2)
        serialNumber: 0x00a81e3a49e69cc64b
      › signature (sha256WithRSAEncryption)
      ▼ issuer: rdnSequence (0)
        ▼ rdnSequence: 6 items (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationa
          › RDNSequence item: 1 item (id-at-countryName=US)
          › RDNSequence item: 1 item (id-at-stateOrProvinceName=Arizona)
          › RDNSequence item: 1 item (id-at-localityName=Scottsdale)
          › RDNSequence item: 1 item (id-at-organizationName=GoDaddy.com, Inc.)
          › RDNSequence item: 1 item (id-at-organizationalUnitName=http://certs.godaddy.com/repository/)
          › RDNSequence item: 1 item (id-at-commonName=Go Daddy Secure Certificate Authority - G2)
      ▼ validity
        ▼ notBefore: utcTime (0)
            utcTime: 2022-08-29 00:39:34 (UTC)
        ▼ notAfter: utcTime (0)
            utcTime: 2023-09-30 00:39:34 (UTC)
      › subject: rdnSequence (0)
      › subjectPublicKeyInfo
      › extensions: 10 items
   › algorithmIdentifier (sha256WithRSAEncryption)
     Padding: 0
     encrypted: 36794b61dedd98290c03a75334a5da88891ee15aedc7fb862fe61b2f3a7ac6068cfc54da…
  Certificate Length: 1236
```

Время установки соединения

```
81447 547.745014    192.168.0.223     149.154.167.99    TLSv1.2   571 Client Hello
81461 547.792970    149.154.167.99    192.168.0.223     TLSv1.2  1294 Server Hello
81466 547.793821    149.154.167.99    192.168.0.223     TLSv1.2  1294 Certificate
81467 547.793821    149.154.167.99    192.168.0.223     TLSv1.2   257 Server Key Exchange, Server Hello Done
81469 547.794688    192.168.0.223     149.154.167.99    TLSv1.2   147 Client Key Exchange, Change Cipher Spec, E
81473 547.842975    149.154.167.99    192.168.0.223     TLSv1.2   344 New Session Ticket, Change Cipher Spec, En
81474 547.843462    192.168.0.223     149.154.167.99    TLSv1.2   693 Application Data
```

547,843462 - 547,745014 = 0,098448

www.sberbank.ru (194.54.14.168)

Имя сервера

```
▼ Server Name Indication extension
      Server Name list length: 16
      Server Name Type: host_name (0)
      Server Name length: 13
      Server Name: s.sberbank.ru
```

Версия TLS

```
▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 100
      Version: TLS 1.2 (0x0303)
```

Выбранный алгоритмы шифрования
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр.

```
▼ Certificate: 308207f6308205dea003020102020e018360611856ccadafb3ce29b047300d06092a8648… (id-at-commonName=s.sbe
  ▼ signedCertificate
      version: v3 (2)
      serialNumber: 0x018360611856ccadafb3ce29b047
    ▶ signature (sha256WithRSAEncryption)
    ▼ issuer: rdnSequence (0)
      ▼ rdnSequence: 3 items (id-at-commonName=Russian Trusted Sub CA,id-at-organizationName=The Ministry of D
        ▶ RDNSequence item: 1 item (id-at-countryName=RU)
        ▶ RDNSequence item: 1 item (id-at-organizationName=The Ministry of Digital Development and Communicat
        ▶ RDNSequence item: 1 item (id-at-commonName=Russian Trusted Sub CA)
    ▼ validity
      ▼ notBefore: utcTime (0)
          utcTime: 2022-09-21 14:08:39 (UTC)
      ▼ notAfter: utcTime (0)
          utcTime: 2023-09-21 14:08:39 (UTC)
    ▶ subject: rdnSequence (0)
    ▶ subjectPublicKeyInfo
    ▶ extensions: 9 items
  ▶ algorithmIdentifier (sha256WithRSAEncryption)
    Padding: 0
    encrypted: df53243e1156e8cc31738e2ab82346e33e58510b7f170246283debeaa59edd3e30fae8c7…
Certificate Length: 1862
```

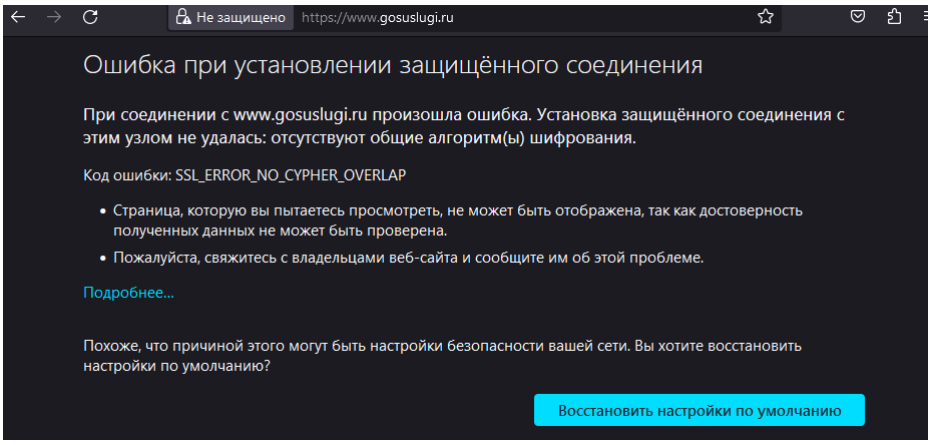
Время установки соединения

No.	Time	Source	Destination	Protocol	Length	Info
6611	38.165600	192.168.0.223	194.54.14.168	TLSv1.2	571	Client Hello
6638	38.170591	194.54.14.168	192.168.0.223	TLSv1.2	1078	Server Hello
6641	38.170591	194.54.14.168	192.168.0.223	TLSv1.2	1078	Certificate
6642	38.170591	194.54.14.168	192.168.0.223	TLSv1.2	336	Server Key Exchange, Server Hello Done
6649	38.173951	192.168.0.223	194.54.14.168	TLSv1.2	180	Client Key Exchange, Change Cipher Spec,
6675	38.177610	192.168.0.223	194.54.14.168	TLSv1.2	85	Encrypted Alert
6679	38.178463	194.54.14.168	192.168.0.223	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake
6680	38.178463	194.54.14.168	192.168.0.223	TLSv1.2	110	Application Data

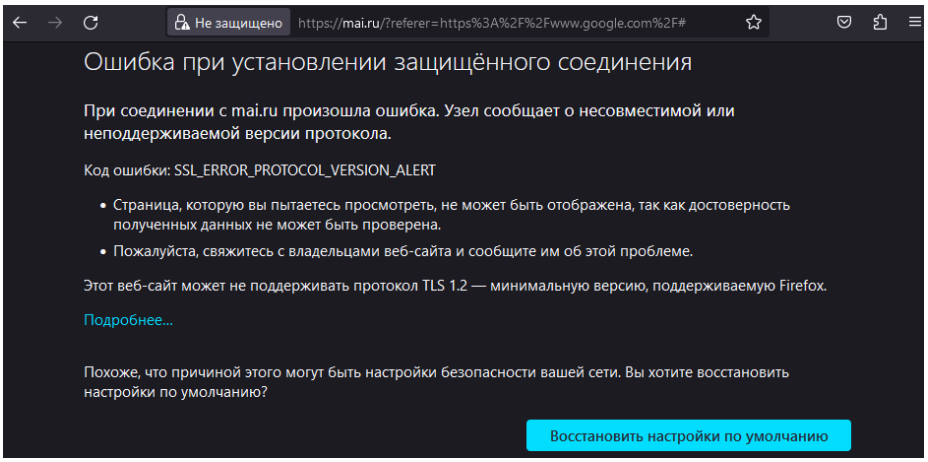
38,178463 - 38,165600 = 0,012863

Принудительное изменение параметров TLS соединения в Firefox на TLS 1.0

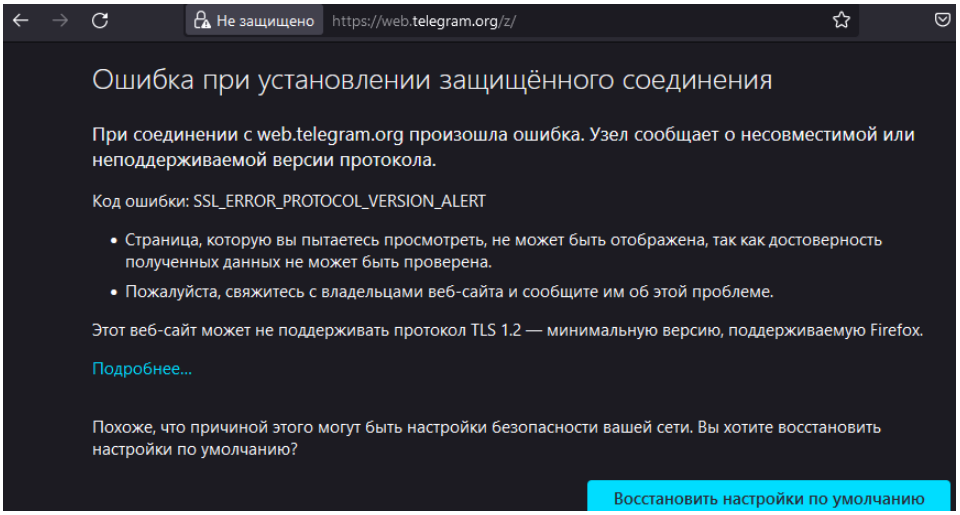
gosuslugi.ru



mai.ru



telegram.org



Три сервера из представленных выше не поддерживают TLS 1.0, оставшиеся *продолжили работу, но на других наборах шифров.*

Уязвимости TLS 1.0 и TLS 1.1

В TLS 1.0 и TLS 1.1 есть целый ряд известных уязвимостей, которые могут быть эксплуатированы хакерами. К ним относятся:

- POODLE (Padding Oracle On Downgraded Legacy Encryption),
- BEAST (Browser Exploit Against SSL/TLS),
- CRIME (Compression Ratio Info-leak Made Easy),
- FREAK (Factoring Attack on RSA-EXPORT Keys),
- LOGJAM (Diffie-Hellman Key Exchange Weakness).

Эти уязвимости позволяют выполнять атаки по типу «человек посередине», расшифровывать чувствительную информацию и перехватывать сеансы пользователей. Отключая на своём сервере TLS 1.0 и TLS 1.1, вы можете защитить себя от этих атак.

Выводы

В ходе этой лабораторной работы мною был изучен протокол защиты транспортного уровня - TLS с помощью утилиты Wireshark. Познакомился с различными угрозами перехвата / подмены пакетов и средствами защиты от них. Сравнительный анализ времени ответов серверов показал, что в большей мере на время ответа влияет загруженность сервера, а самый популярный криптографический протокол - алгоритм Диффи - Хеллмана.