

ПРОТОКОЛ № 260608-73077

от 08.06.2026 15:23 МСК

Автоматизированная фиксация информации в сети Интернет

| | |
|--------------------------|--|
| Идентификатор протокола | ede1c23628a882d63b40a466ff6e61ed |
| Зафиксировано URL | 1 |
| Время фиксации | 2026-06-08 12:23:55 UTC 2026-06-08 15:23:55 МСК |
| Удостоверение времени | Время удостоверено |
| OpenTimestamps (Bitcoin) | Хеш опубликован |



Сканируйте для проверки
протокола

Зафиксированные ресурсы

- <https://podpisal.ru>

Настоящий протокол фиксирует факт существования и содержания указанных интернет-страниц на момент фиксации. Целостность артефактов гарантируется криптографически: изменение любого зафиксированного файла приведёт к расхождению SHA-256 хешей и недействительности удостоверяющих меток времени. Подробности проверки — в разделах 5 и 6 настоящего протокола.

1. Преамбула

Настоящий протокол составлен автоматизированной системой «Подписал.ру» (<https://podpisal.ru>) по запросу инициатора фиксации и удостоверяет факт существования и содержания указанных интернет-страниц на дату и время фиксации.

1.1. Инициатор фиксации

| | |
|------------------------------|----------------------------------|
| IP-адрес инициатора | 113.22.236.228 |
| User-Agent инициатора | curl/8.7.1 |
| Идентификатор заказа | ede1c23628a882d63b40a466ff6e61ed |

1.2. Задачи фиксации

1. Установить наличие и доступность указанных интернет-страниц на момент фиксации.
2. Сохранить визуальное содержимое страниц (видимая область и полная высота).
3. Сохранить HTML-исходник, HTTP-заголовки ответа и сетевые параметры.
4. Зафиксировать целостность всех артефактов криптографически (SHA-256).
5. Удостоверить время фиксации независимой службой меток времени и публичным реестром (Bitcoin / OpenTimestamps).

1.3. Технические средства фиксации

| | |
|------------------------------|---|
| Сервер фиксации | Подписал.ру / api.podpisal.ru |
| Браузер захвата | Chrome/147.0.7727.57 |
| User-Agent захвата | Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/147.0.0.0 Safari/537.36 |
| Viewport | 1366 × 768 |
| Управляющая программа | Puppeteer (Headless Chromium API) — серверный захват |

1.4. Системное время

Перед началом фиксации зафиксировано состояние системного времени и синхронизации NTP. Полный вывод утилиты `timedatectl` приведён в Приложении А.

2. Методика обеспечения корректности фиксации

2.1. Идентификация ресурса

Каждый зафиксированный URL соответствует строгому формату RFC 3986 (Uniform Resource Identifier: Generic Syntax). Идентификация выполняется по полному URL, включая схему (http/https), хост, порт, путь и строку запроса. Для каждого URL фиксируется также финальный URL после прохождения HTTP-редиректов.

2.2. DNS-разрешение и сетевой путь

Хост каждого URL разрешается стандартным DNS-резолвером сервера фиксации. Перед захватом для каждого уникального хоста снимается TCP-trace по протоколу tcp traceroute (TCP/80) — это фиксирует сетевой путь от сервера до целевого узла на момент фиксации (см. Приложение Б).

2.3. Регистрационные данные доменов

Для каждого уникального домена выполняется WHOIS-запрос к регистратору домена. Результат сохраняется в виде текстового файла и хешируется наравне с прочими артефактами (см. Приложение Б).

2.4. Изоляция и отсутствие кэша

Захват выполняется в новом изолированном профиле браузера (без cookies, расширений и сохранённых сессий пользователя). Для каждого URL открывается отдельная вкладка, ожидается событие `networkidle0` (отсутствие сетевой активности в течение 500 мс), что гарантирует полную загрузку страницы и её динамических ресурсов.

2.5. Гарантии целостности

Каждый зафиксированный артефакт (PNG-скриншоты, HTML-исходник, JSON-заголовки HTTP, сетевые логи) хешируется алгоритмом SHA-256. Хеши собираются в файл `manifest.txt`; сводный хеш этого файла подписывается независимой службой меток времени (RFC 3161) и публикуется в публичном реестре OpenTimestamps, что обеспечивает публикацию хеша в блокчейне Bitcoin.

Любая модификация любого артефакта после фиксации приводит к расхождению SHA-256 хешей и автоматически делает удостоверяющие метки времени недействительными.

Где найти конкретные значения: данный раздел описывает методологию. Сами параметры этой фиксации — серийный номер RFC 3161 TSA-токена, файл OpenTimestamps-доказательства и сводный SHA-256 манифеста — приведены ниже в разделе 3 и разделе 4.

2.6. Способ фиксации

Режим захвата: **Текущий вид окна (viewport)**.

Сохранён видимый фрагмент окна браузера в момент фиксации. Размер окна: 1366 × 768 рх. Полная высота страницы за пределами видимой области в данном режиме не фиксируется.

Если требуется фиксация всей высоты страницы целиком (включая материал, скрытый прокруткой), используется отдельный режим захвата «полная страница» с пошаговой прокруткой и склейкой кадров.

3. Выполненные системой действия

В ходе фиксации система последовательно выполнила следующие действия:

| № | Действие | Результат |
|---|--|-----------|
| 1 | Снимок состояния системного времени и NTP-синхронизации (timedatectl). Полный вывод см. Приложение А. | ok |
| 2 | WHOIS-запрос для каждого уникального домена. Получено отчётов: 1. | 1 |
| 3 | TCP-traceroute для каждого уникального хоста (TCP/80). Получено трасс: 1. | 1 |
| 4 | Захват 1 URL: видимая область, полная страница, HTML-исходник, HTTP-заголовки ответа. | 1 / 1 |
| 5 | Подсчёт SHA-256 для всех артефактов (включая сетевые логи) и формирование manifest.txt. | ok |
| 6 | Запрос RFC 3161 Time-Stamp Token у независимого провайдера freetsa.org на хеш манифеста. Серийный номер токена: 0x05755A4D Время согласно TSA: 2026-06-08 12:24:08 UTC 2026-06-08 15:24:08 МСК Файл доказательства: manifest.tsr | ok |
| 7 | Публикация хеша манифеста в реестре OpenTimestamps (подтверждение в Bitcoin появляется в течение ~3 часов). Файл OTS-доказательства: manifest.txt.ots Проверка: ots verify <имя>.ots | ok |
| 8 | Формирование настоящего PDF-протокола и публикация страницы верификации. | ok |

3.1. Сводные хеши манифеста

| | |
|--|--|
| SHA-256 (RFC 6234) | fa4da23e0b43b919af2811692fed09e6728cebd3425718bbaebf6bd274b04a74 |
| Стрибог-256 (ГОСТ Р 34.11-2012) | be7074c184aa437a32106ca0af41e9195951d275e0b8ed9efd6856ffa49ae775 |

4. Криптографические гарантии

Подлинность настоящего протокола обеспечивается тремя независимыми механизмами, каждый из которых может быть проверен любой третьей стороной без участия сервиса «Подписал.ру».

4.1. Хеши артефактов: SHA-256 и Стрибог-256 (ГОСТ Р 34.11-2012)

Для каждого зафиксированного файла подсчитаны **две** независимые криптографические суммы:

- **SHA-256** — международный стандарт (RFC 6234), широко используемый в банковской и государственной сфере.
- **Стрибог-256** — национальный стандарт Российской Федерации (ГОСТ Р 34.11-2012). Используется в качестве «русского» алгоритма хеширования при работе с электронными документами в РФ.

Оба хеша собраны в файл `manifest.txt`; сводные хеши манифеста приведены в разделе 3.1 и удостоверены RFC 3161 TSA-токеном (см. раздел 4.2).

Что это даёт: любое изменение хотя бы одного байта в любом из артефактов одновременно изменяет оба хеша — и протокол можно немедленно опровергнуть проверкой любым из двух алгоритмов. Использование двух независимых хеш-функций исключает риск теоретической коллизии в одном из них.

Алгоритм Стрибог-256 является односторонней функцией без секретного ключа и не выполняет шифрования; его реализация не относится к СКЗИ и не требует получения лицензий ФСБ России.

4.2. RFC 3161 Time-Stamp Authority (независимая третья сторона)

| | |
|-----------------------|--|
| Провайдер | freetza.org |
| Время согласно TSA | 2026-06-08 12:24:08 UTC 2026-06-08 15:24:08 МСК |
| Серийный номер токена | 0x05755A4D |
| Файл доказательства | manifest.tsr |
| Статус | Время удостоверено |

Что это даёт: независимая (не подконтрольная сервису «Подписал.ру») сторона цифровой подписью удостоверила, что хеш манифеста существовал в указанный момент времени. Стандарт описан в RFC 3161 и широко применяется в юридической практике.

4.3. OpenTimestamps — публикация в Bitcoin

| | |
|---------------------|---|
| Файл доказательства | manifest.txt.ots |
| Текущий статус | Хеш опубликован |
| Подтверждение в BTC | Автоматически появляется в течение ~3 часов и записывается на странице верификации. |

Что это даёт: хеш манифеста публикуется в публичном неизменяемом реестре сети Bitcoin. Это означает, что подделать задним числом дату фиксации невозможно даже совместными усилиями сервиса и TSA — Bitcoin-блокчейн контролируется тысячами независимых узлов по всему миру.

5. Юридическое основание и проверка

Настоящий протокол составлен в соответствии с пунктом 55 Постановления Пленума Верховного Суда Российской Федерации от 23 апреля 2019 г. № 10 «О применении части четвёртой Гражданского кодекса Российской Федерации» и подтверждает факт существования и содержания указанных интернет-страниц на момент фиксации.

Согласно указанному постановлению Пленума ВС РФ и сложившейся судебной практике, нотариальное удостоверение скриншотов не является обязательным при наличии иных средств подтверждения подлинности — в частности, независимых криптографических меток времени и открытой возможности проверки целостности артефактов любым заинтересованным лицом.

Время фиксации удостоверено независимой службой меток времени (RFC 3161 Time-Stamp Protocol, провайдер freetsa.org) и зафиксировано в публичном реестре OpenTimestamps (сеть Bitcoin). Целостность зафиксированных файлов обеспечивается математически.

5.1. Способ проверки протокола любой третьей стороной

- Открыть публичную страницу верификации (см. ниже) и сверить SHA-256 хеши артефактов с приведёнными в настоящем протоколе.
- Загрузить файл RFC 3161 TSA-токена и проверить его средствами `openssl ts -verify`. Информация о провайдере: <https://freetsa.org/>.
- Загрузить OpenTimestamps-доказательство и проверить публикацию хеша в сети Bitcoin утилитой `ots verify`. Открытая спецификация и инструменты: <https://opentimestamps.org/>.



Страница верификации:

<https://api.podpisal.ru/tools/verify/edelc23628a882d63b40a466ff6e61ed>

Страница доступна публично и не требует регистрации. На ней можно сверить SHA-256 манифеста с реестром и проверить статус подтверждения в Bitcoin.

6. Технические детали

Раздел адресован юристу, эксперту-криминалисту и оппоненту, желающим самостоятельно проверить целостность настоящего протокола. Все указанные команды выполняются на стандартном Linux/macOS окружении с установленным OpenSSL и опционально пакетом `opentimestamps-client`.

6.1. Хеширование

Каждый файл артефакта подписан двумя криптографическими хешами — SHA-256 (международный стандарт RFC 6234) и Стрибог-256 (ГОСТ Р 34.11-2012). Двойное хеширование исключает зависимость от любой одной криптосистемы: для подделки протокола потребовалось бы одновременно найти коллизию в обоих алгоритмах, что считается вычислительно невозможным.

Локальная проверка SHA-256 любого файла из архива:

```
openssl dgst -sha256 manifest.txt
sha256sum manifest.txt
```

Полученный хеш должен совпасть с тем, что указан в самом `manifest.txt` и в разделе 3.1 настоящего протокола.

6.2. RFC 3161 Timestamp

Дата и время заверения подтверждены TSA (Time-Stamping Authority) по протоколу RFC 3161. TSR (Time-Stamp Response) лежит в архиве в файле `manifest.tsr`. Локальная проверка TSR через OpenSSL:

```
openssl ts -verify \
-in manifest.tsr \
-data manifest.txt \
-CAfile <CA-сертификат-TSA>
```

CA-сертификат TSA и URL провайдера (по умолчанию `freetsa.org`) указаны в файле `tsa-info.txt` архива. Команда возвращает `Verification: OK`, если TSR действителен и относится именно к данному манифесту.

6.3. OpenTimestamps / Bitcoin-якорь

Хеш манифеста дополнительно зафиксирован в блокчейне Bitcoin через сервис OpenTimestamps — бесплатный публичный сервис, разработан Питером Тоддом (Peter Todd, один из соавторов протокола Bitcoin). Файл `manifest.txt.ots` в архиве можно проверить командой:

```
ots verify manifest.txt.ots
# нужен пакет: pip install opentimestamps-client
```

После 1–6 часов после момента заверения хеш попадает в один из блоков сети Bitcoin и становится практически неподделываемым: для изменения даты задним числом потребовалось бы переписать историю одной из крупнейших публичных распределённых баз данных в мире.

6.4. Структура архива артефактов

Архив `ede1c23628a882d63b40a466ff6e61ed_artifacts.zip` содержит:

| | |
|---|--|
| screenshots/ или url-N/ | Финальные скриншоты по каждому URL: <code>viewport.png</code> , <code>stitched.png</code> (для fullpage), <code>source.html</code> , <code>headers.json</code> . |
| url-N/frames/ | Исходные кадры пошагового захвата (только для fullpage). По каждому кадру — отдельный <code>frame_NNN.png</code> со своим SHA-256 и Стрибог-256 в <code>manifest</code> . |
| manifest.txt | Список всех файлов архива с двумя хешами на каждый файл. Этот файл и есть «то, что подписано» TSA и зафиксировано в Bitcoin. |
| manifest.tsr | RFC 3161 Time-Stamp Response от провайдера <code>freetsa.org</code> . |
| manifest.txt.ots | OpenTimestamps-доказательство: путь от хеша манифеста до блока Bitcoin. |
| network/ | Сетевые приложения: <code>timedatectl.txt</code> (состояние NTP), <code>whois-*.txt</code> (регистрационные данные доменов), <code>tcptraceroute-*.txt</code> (сетевой путь до целевых узлов). |
| tsa-info.txt | Информация о провайдере TSA, URL и ссылка на CA-сертификат для проверки TSR. |
| README.txt | Инструкция по проверке архива на двух уровнях: «для пользователя» (<code>drag&drop</code> в <code>verify</code> -странице) и «для эксперта» (OpenSSL-команды). |
| ede1c23628a882d63b40a466ff6e61ed.pdf | Копия настоящего протокола. |

7. Памятка для юриста: использование протокола в суде

7.1. Допустимость

Протокол является письменным доказательством согласно ст. 71 ГПК РФ и ст. 75 АПК РФ.

Согласно п. 55 Постановления Пленума Верховного Суда РФ № 10 от 23.04.2019 «О применении части четвёртой Гражданского кодекса Российской Федерации» допустимы скриншоты, заверенные участником процесса, при условии указания адреса страницы, точного времени и средства автоматической фиксации. Все эти атрибуты содержатся в настоящем протоколе.

7.2. Чек-лист для приобщения к делу

- Ссылка на зафиксированную страницу (полный URL) — раздел 1 и Приложение Г настоящего протокола.
- Точное время заверения с указанием TSA — раздел 4.2: провайдер freetsa.org, серийный номер токена 0x05755A4D.
- Хеши манифеста (SHA-256 и Стрибог-256) и способ их проверки — раздел 3.1 и раздел 6.1 настоящего протокола.
- Ссылка на публичную страницу верификации — где судья, оппонент или эксперт может проверить целостность файла независимо, без обращения в сервис «Подписал.ру»:
<https://api.podpisa.ru/tools/verify/ede1c23628a882d63b40a466ff6e61ed>

7.3. Что делать при оспаривании

Сторона, оспаривающая протокол, обязана указать конкретное несоответствие. Все исходные данные открыты и проверяемы:

- SHA-256 + Стрибог-256 манифеста — пересчитываются локально в одну команду (см. раздел 6.1).
- RFC 3161 TSR от независимой TSA — проверяется средствами OpenSSL (см. раздел 6.2).
- OpenTimestamps-якорь в Bitcoin — проверяется утилитой `ots verify` (см. раздел 6.3).

Эксперт может скачать архив с публичной страницы верификации, локально пересчитать хеши всех файлов и сравнить их с указанными в настоящем протоколе и в RFC 3161 TSR. Любое расхождение хотя бы на один байт мгновенно делает протокол недействительным — и наоборот, совпадение хешей при действительном TSR / OTS исключает возможность подделки.

7.4. Контакт службы заверения

| | |
|--|---|
| Электронная почта поддержки | support@podpisa1.ru |
| Страница верификации настоящего протокола | https://api.podpisa1.ru/tools/verify/ede1c23628a882d63b40a466ff6e61ed |
| Описание принципа работы сервиса | https://podpisa1.ru/kak-eto-rabotaet/ |

Приложение А. Состояние системного времени

Снимок состояния NTP-синхронизации системного времени сервера фиксации, сделанный до начала захвата страниц. Файл: `network/timedatectl.txt`.

```
Local time: Mon 2026-06-08 15:23:54 MSK
Universal time: Mon 2026-06-08 12:23:54 UTC
RTC time: Mon 2026-06-08 12:23:54
Time zone: Etc/UTC (MSK, +0300)
System clock synchronized: yes
NTP service: n/a
RTC in local TZ: no
```

Хеш этого файла включён в общий `manifest.txt` и удостоверен RFC 3161 TSA — изменение времени фиксации задним числом без потери удостоверяющих меток невозможно.

Приложение Б.1. WHOIS — podpisal.ru

Регистрационные данные домена, полученные от регистратора в момент фиксации. Файл: network/whois_podpisal.ru.txt.

```
% TCI Whois Service. Terms of use:
% https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian)
% https://tcinet.ru/documents/whois_su.pdf (in Russian)
```

```
domain:      PODPISAL.RU
nserver:     ns1.netangels.ru.
nserver:     ns2.netangels.ru.
state:       REGISTERED, DELEGATED, VERIFIED
person:      Private Person
registrar:   REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created:     2025-01-11T13:32:17Z
paid-till:   2027-01-11T13:32:17Z
free-date:   2027-02-11
source:      TCI
```

```
Last updated on 2026-06-08T12:23:01Z
```

Приложение В.1. TCP-trace до podpisal.ru

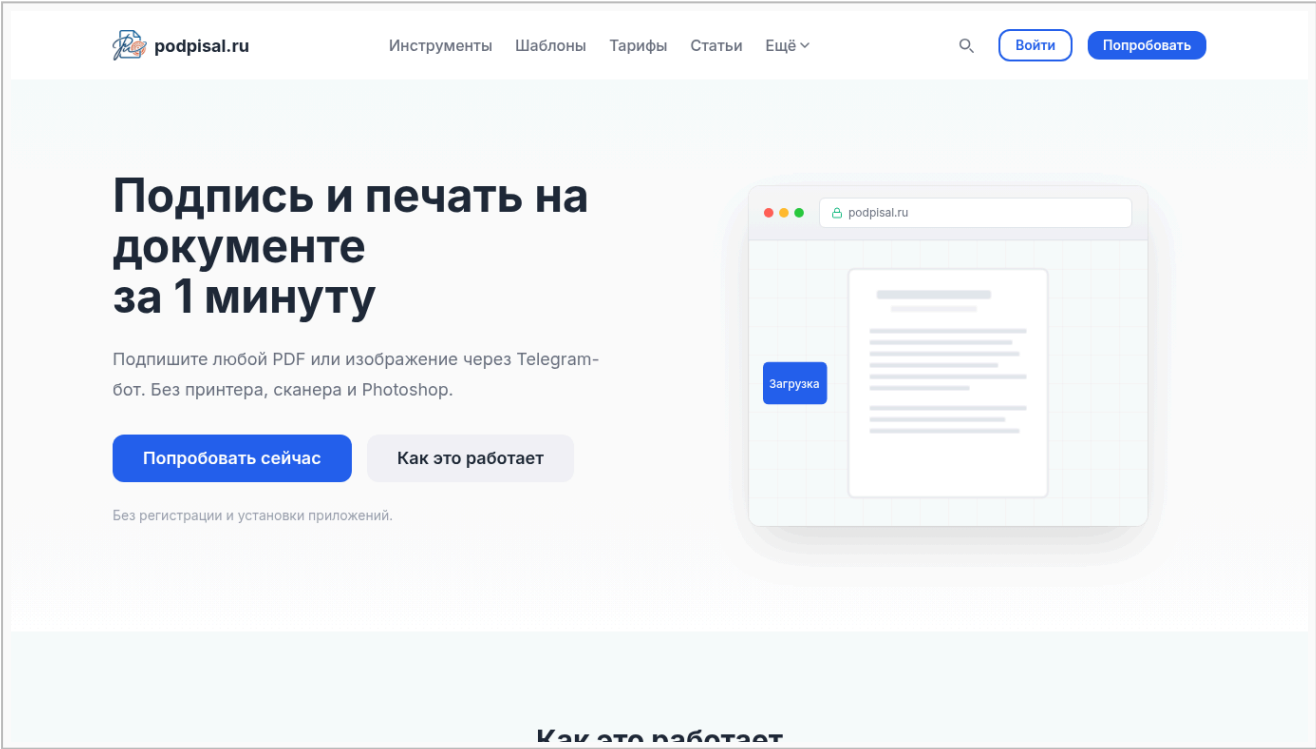
Сетевой путь от сервера фиксации до целевого узла по протоколу TCP/80. Файл: network/tcptracero
ute_podpisa.ru.txt.

```
1 45.86.39.118 [open] 0.082 ms 0.034 ms 0.094 ms
Selected device lo, address 45.86.39.118, port 54133 for outgoing packets
Tracing the path to podpisa.ru (45.86.39.118) on TCP port 80 (http), 12 hops max
```

Приложение Г.1. Фиксация URL

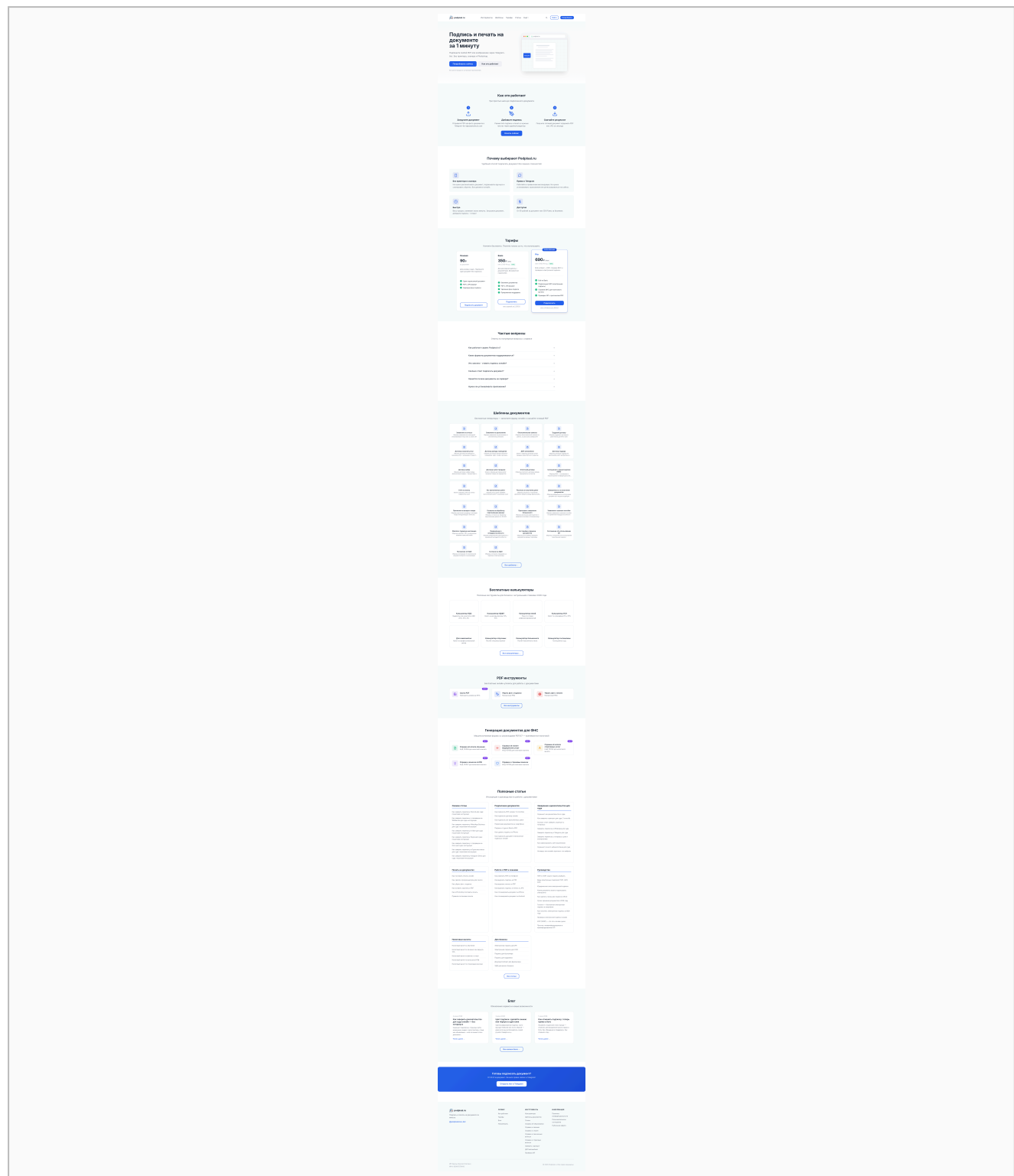
| | |
|-------------------------|--|
| Запрошенный URL | https://podpisal.ru |
| Финальный URL | https://podpisal.ru/ |
| HTTP-статус | 200 |
| SHA-256 viewport.png | 9978f2a60754aa96cd6b1bc368105366084b719e7361ba42e935e031e68780d6 |
| SHA-256 fullpage.png | a8a2d98d7cb7a97e14b0228c208663e096891dabaa3b52100b7ebff864f8da51 |
| SHA-256 source.html | b8f4e8ac50887e13b95b0b28ef078f98162ab0cbcd3a7105f6ca3236e10024a |
| SHA-256 headers.json | c2315dedce381b433d15609645c78466fe2a8fc4d7cbeee78fe4ff95c75989c8 |

Видимая область (viewport 1366×768)



Приложение Г.1 (продолжение). Полная страница

URL: <https://podpisal.ru>



Скриншот всей высоты страницы (полная прокрутка)