



ViPNet PKI Client Аврора

Руководство пользователя

Версия продукта: 2.1.0

© АО «ИнфоТеКС», 2026

ФРКЕ.00175-03 34 08

Версия продукта: 2.1.0

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

Все условия эксплуатации и ограничения на использование ViPNet PKI Client Аврора приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet PKI Client Аврора.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение.....	5
О документе.....	5
Соглашения документа.....	5
О приложении	5
Комплект поставки.....	6
Системные требования.....	6
Лицензирование	6
Что нового в версии 2.1.0.....	7
Обратная связь.....	8
Установка и запуск приложения.....	9
Установка и обновление	9
Первый запуск	9
Управление сертификатами	11
Какие нужны сертификаты	11
Подготовка личного сертификата и ключа ЭП	11
Подключение ключевого носителя	12
Получение сертификата.....	12
Установка сертификатов и CRL.....	14
Проверка сертификатов.....	15
Настройка автоматического обновления CRL.....	16
Экспорт сертификатов в файлы *.cer и *.pem	17
Перенос сертификатов и ключей ЭП между устройствами	17
Удаление сертификатов и ключей ЭП	18
Использование облачных сервисов ЭП.....	20
Настройка подключения к сервису	20
Подключение к сервису	21
Изменение настроек подключения к сервису	22
Смена пароля учётной записи.....	22
Удаление настроек подключения к сервису	23
Подпись и зашифрование файлов.....	24
Требования к сертификатам для подписи и зашифрования.....	24

Подписание файла.....	24
Зашифрование файла	26
Работа с файлами, полученными от других пользователей	28
Проверка ЭП.....	28
Расшифрование файла	29
Подключение к сайтам, использующим TLS ГОСТ.....	31
Порядок настройки подключения к сайтам	31
Требования к сертификатам для работы по TLS ГОСТ	31
Установка корневого сертификата для TLS ГОСТ.....	32
Включение TLS ГОСТ	33
Настройка прокси-сервера.....	33
Подключение к сайту.....	34
Просмотр информации о TLS-соединениях.....	35
Служебные функции	36
Смена пароля хранилища ViPNet PKI Client.....	36
Обновление лицензии.....	36
Сброс настроек приложения	36
Удаление приложения.....	37
Возможные неполадки	38
Нет подключения к интернету	38
Не удаётся установить TLS-соединение через предустановленный браузер.....	38
Термины и сокращения	40

Введение

О документе

Документ описывает настройку приложения ViPNet® PKI Client Аврора (далее — ViPNet PKI Client) и работу с ним.

Предполагается, что пользователь имеет общее представление об электронной подписи и сертификатах ключа проверки электронной подписи.

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке

О приложении

С помощью ViPNet PKI Client вы можете:

- Создать [запрос на сертификат](#) для передачи в удостоверяющий центр (далее — УЦ).
- Подписать файлы и проверить [электронную подпись](#) (далее — ЭП) файлов.
- Зашифровать и расшифровать файлы.
- Подключиться к сайтам по TLS ГОСТ, в том числе с [аутентификацией пользователя](#).
Поддерживаемые версии [протокола TLS](#): 1.2 и 1.3.

ViPNet PKI Client использует российские криптографические алгоритмы:

- Алгоритм проверки ЭП: ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм создания ЭП: ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012.
- Алгоритм шифрования для TLS-соединений: ГОСТ 28147-89 и ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».
- Алгоритм шифрования для файлов: ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».

Комплект поставки

- Установочный файл *.rpm.
- Серийный номер — получаете при покупке лицензии.
- Руководство пользователя в формате PDF.

Системные требования

Требования к устройству для установки ViPNet PKI Client:

- ОС Аврора 5;
- процессор с архитектурой ARM32 или ARM64.

Для хранения сертификата и ключей ЭП можно использовать ключевые носители:

- Рутокен ЭЦП 3.0 NFC 3100;
- Смарт-карту Рутокен ЭЦП 3.0 NFC 3100;
- Рутокен ЭЦП 3.0 3220 Type-C.

Если в вашей организации для хранения сертификатов используется облачный сервис ЭП — ViPNet PKI Service версии 2.0 или выше.

Лицензирование

Для использования ViPNet PKI Client приобретите лицензию у представителя ИнфоТеКС и [активируйте приложение с помощью полученного серийного номера](#).

Что нового в версии 2.1.0

- **Дополнена проверка усиленной квалифицированной ЭП**

В соответствии с Федеральным законом 06.04.2011 № 63-ФЗ (ред. 04.08.2023) «Об электронной подписи» добавлена возможность при проверке усиленной квалифицированной ЭП проверять дополнительные параметры (например, срок действия ключа ЭП).

- **Выполнение криптографических операций на ViPNet PKI Service**

Если в вашей организации для хранения сертификатов и ключей ЭП используется ViPNet PKI Service, вы можете подключиться к нему для выполнения криптографических операций из интерфейса ViPNet PKI Client.

- **Подтверждение операций в облачном сервисе ЭП**

Теперь в ViPNet PKI Client можно выполнять операции в облачном сервисе ЭП, требующие подтверждение: подписание и расшифрование файла, а также создание запроса на сертификат.

- **Новые параметры при создании запроса на сертификат**

Теперь при создании запроса на сертификат можно:

- задать срок действия ключа ЭП;
- разрешить экспортировать ключ ЭП.

- **Экспорт сертификатов в файлы разных форматов**

Личные сертификаты или сертификаты получателей можно экспортировать в файлы *.der или *.pem, личный сертификат и соответствующий ключ ЭП — в файл *.pfx.

- **Поддержка работы с токенами и смарт-картами**

Подписывать и расшифровывать файлы можно с помощью сертификатов и ключей ЭП, хранящихся на токенах и смарт-картах.

- **Предустановленные сертификаты УЦ**

При установке ViPNet PKI Client в хранилище сертификатов устанавливаются:

- Корневые сертификаты: Минцифры России, Минцифры России НУЦ корневой.
- Промежуточный сертификат: Минцифры России НУЦ подчинённый.

- **Прекращение поддержки ОС Аврора 4**

Обратная связь

Контактная информация

- Единый многоканальный телефон:
+7 (495) 737-6192,
8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба поддержки: hotline@infotecs.ru.
Форма для обращения в службу поддержки через сайт.
Телеграм-канал поддержки: t.me/vhd21.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet](#).
- [О решениях ViPNet](#).
- [Часто задаваемые вопросы](#).
- [Форум пользователей продуктов ViPNet](#).

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ИнфоТеКС регулируется [политикой ответственного разглашения](#).

Установка и запуск приложения

Установка и обновление



Внимание! При обновлении ViPNet PKI Client версии 2.0 до версии 2.1:

- сохранится лицензия;
- будут сброшены настройки приложения и удалены сертификаты и ключи ЭП.

Через Аврора Маркет

- 1 Получите у администратора параметры подключения к витрине.
- 2 В списке приложений выберите **ViPNet PKI Client** и нажмите **Установить** или **Обновить**.

Через файловый менеджер

- 1 Скопируйте установочный файл *.rpm на устройство. Этот файл входит в комплект поставки.
- 2 Запустите приложение **Файлы**.
- 3 Перейдите в папку с установочным файлом.
- 4 Выберите этот файл и нажмите **Установить**.

Через Аврора Центр

ViPNet PKI Client устанавливает администратор. См. [документацию ОС Аврора](#).

Первый запуск

- 1 Убедитесь, что на устройстве есть доступ в интернет.
- 2 Запустите ViPNet PKI Client.
- 3 Чтобы разрешить доступ ViPNet PKI Client к интернету, к файлам на устройстве и съёмных носителях, нажмите **Подтвердить**.
- 4 Задайте и подтвердите пароль хранилища ViPNet PKI Client и ключей ЭП.



Внимание! Запомните пароль хранилища ViPNet PKI Client, его нельзя восстановить.

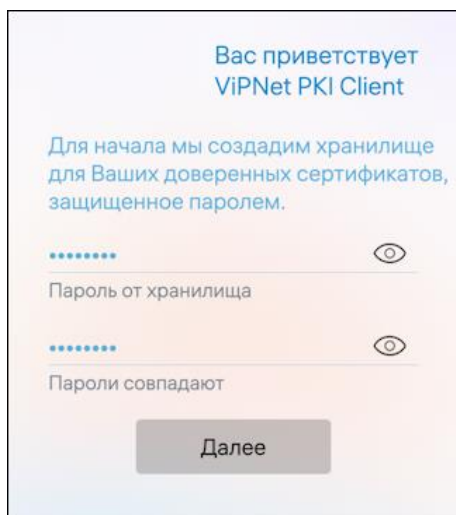


Рисунок 1. Задание пароля хранилища ViPNet PKI Client

- 5 Следуйте указаниям на экране для создания последовательности случайных чисел.
- 6 После сообщения **Безопасное хранилище создано** проведите по экрану справа налево.
- 7 Активируйте приложение:
 - 7.1 Введите номер телефона и серийный номер (вы получили его при покупке лицензии).
 - 7.2 Нажмите **Активировать**, вам придет СМС с кодом активации.
 - 7.3 Введите полученный код.
- 8 После сообщения **Приложение активировано** проведите по экрану справа налево.

Управление сертификатами

Какие нужны сертификаты

- Личный сертификат — для подписи, расшифровки файлов, подключения к сайтам, использующим TLS ГОСТ с аутентификацией пользователя. Получите его в УЦ по запросу и [установите в хранилище ViPNet PKI Client](#) или на [ключевой носитель](#).
- Сертификаты получателей — для зашифрования файлов. Запросите их у получателей файлов и [установите в хранилище ViPNet PKI Client](#).
- Сертификаты УЦ — для проверки личного сертификата. Получите их в УЦ и [установите в хранилище ViPNet PKI Client](#).

Для подтверждения действительности сертификатов могут использоваться:

- [CRL](#) — в этом случае вы можете:
 - Настроить автоматическое обновление CRL путём опроса [точек распространения CRL](#). URL этих точек содержится в сертификатах, изданных УЦ, в поле **Точки распространения списков отзыва (CRL)**.
 - Получить CRL в УЦ и установить их вручную.
- Информация от [OCSP-службы](#). Список поддерживаемых OCSP-служб содержится в сертификатах, изданных УЦ, в поле **Доступ к информации о центрах сертификации**. CRL в этом случае не используются.

Подготовка личного сертификата и ключа ЭП

Если нет сертификата и ключа ЭП

- 1 [Создайте запрос на сертификат и передайте его в УЦ.](#)
- 2 [Установите полученные сертификаты и CRL.](#)

Если есть сертификат и ключ ЭП в файле *.pfx

- 1 [Импортируйте сертификат и ключ ЭП.](#)
- 2 [Установите сертификаты:](#)
 - [корневой сертификат УЦ](#) и CRL;

- сертификаты и CRL вышестоящих УЦ — если сертификат УЦ подписан вышестоящим УЦ.

Если есть сертификат на ключевом носителе

- 1 Подключите ключевой носитель.
- 2 Установите сертификаты:
 - [корневой сертификат УЦ](#) и CRL;
 - сертификаты и CRL вышестоящих УЦ — если сертификат УЦ подписан вышестоящим УЦ.

Если вы хотите хранить сертификат в облачном сервисе ЭП

- 1 [Настройте подключение к облачному сервису ЭП](#). В разделе **Сертификаты** появятся сертификаты, хранимые в облачном сервисе ЭП.
- 2 Если у вас нет сертификата в облачном сервисе ЭП или вам нужно его обновить:
 - 2.1 [Создайте запрос на сертификат с сохранением ключа ЭП в облачном сервисе ЭП](#).
 - 2.2 Получите сертификат в УЦ.
 - 2.3 [Установите сертификат в облачный сервис ЭП](#).

Подключение ключевого носителя

- 1 Если вы будете подключать NFC-токен, в настройках устройства включите NFC.
- 2 На главном экране проведите сверху вниз и выберите **Настройки**.
- 3 Выберите **Токены**.
- 4 Подключите ключевой носитель к устройству. Способ подключения зависит от исполнения ключевого носителя — см. документацию производителя ключевого носителя и следуйте указаниям на экране устройства.

Чтобы просмотреть сертификаты, хранимые на ключевом носителе, на главном экране проведите сверху вниз и выберите **Сертификаты**. Сертификаты отмечены значком .

Получение сертификата

При создании запроса на сертификат создаётся [контейнер ключей](#). С помощью этих ключей вы будете подписывать и расшифровывать файлы.

Чтобы создать запрос на сертификат:

- 1 Чтобы ключи ЭП хранились:
 - на ключевом носителе — [подключите носитель к устройству](#);
 - в облачном сервисе ЭП — [подключитесь к облачному сервису ЭП](#).

- 2 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 3 Проведите сверху вниз и выберите **Запрос на сертификат**.
- 4 Заполните данные о сертификате и его владельце.

Запрос на сертификат

Физическое лицо
Шаблон сертификата

Локальное хранилище
Место хранения ключа

Личное присутствие
Идентификация заявителя

Характеристики сертификата

ГОСТ 34.10-2012/1024
Алгоритм ключа проверки ЭП

Набор параметров А (ТК 26)
Параметры ключа проверки ЭП

Электронная подпись и шифрование
Назначение ключа

36
Срок действия ключа ЭП, мес

☒ **Разрешить экспортировать ключ ЭП**

Владелец сертификата

Иванов
Фамилия

Иван Иванович
Имя и отчество

Иванов Иван Иванович
Общее имя

Российская Федерация
Страна

Регион
Регион

Населенный пункт
Населенный пункт

Улица, дом
Улица, дом

12345678901
СНИЛС

123456789012
ИНН физического лица

@ivanov@example.com
Электронная почта

Создать запрос

Рисунок 2. Создание запроса на сертификат

- 5 Нажмите **Создать запрос**.



Примечание. Если вы выбрали местом хранения контейнера ключей ЭП облачное хранилище, может потребоваться подтверждение операции. Введите код подтверждения.

- 6 В зависимости от места хранения ключей ЭП:

- хранилище ViPNet PKI Client — введите пароль;
- облачный сервис ЭП — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло);
- ключевой носитель — введите PIN-код.



Примечание. Если вы введёте неверный пароль хранилища ViPNet PKI Client 10 раз подряд, ViPNet PKI Client заблокируется на 15 минут.

- 7 Нажмите **Подтвердить**.
- 8 Сохраните файл запроса.
- 9 После сообщения **Файл сохранен** проведите по экрану справа налево.
- 10 Передайте запрос на сертификат в УЦ.
- 11 Получите в УЦ:
 - личный сертификат;
 - корневой сертификат УЦ и CRL;
 - сертификаты и CRL вышестоящих УЦ — если сертификат УЦ подписан вышестоящим УЦ.
- 12 [Установите полученные сертификаты и CRL](#).

Установка сертификатов и CRL



Примечание. Если в УЦ используются точки распространения CRL или OCSP-служба и они доступны на устройстве, устанавливать CRL вручную не нужно.

- 1 Чтобы установить сертификат на ключевой носитель, [подключите его к устройству](#).
- 2 Перенесите на устройство сертификаты или CRL.
- 3 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 4 Проведите сверху вниз и выберите **Установить сертификат** или **Установить CRL**.

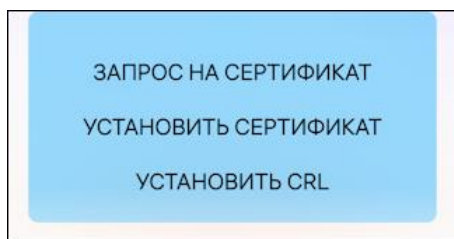


Рисунок 3. Установка сертификатов и CRL

- 5 Выберите сертификат или CRL.
- 6 Проверьте информацию о сертификате или CRL и нажмите **Подтвердить**.

- 7 Выберите место установки сертификата. Если вы не подключили ключевой носитель, сертификат автоматически установится в хранилище ViPNet PKI Client.



Примечание. Если после установки сертификата в строке с именем владельца появилось предупреждение, см. [Проверка сертификатов](#).

- 8 Повторите шаги 4–7 для установки следующего сертификата или CRL.
- 9 После установки всех сертификатов и CRL [настройте автоматическое обновление CRL](#).

Проверка сертификатов

При установке сертификата в ViPNet PKI Client автоматически проверяется [действительность сертификата](#). Сертификаты, статус которых не удалось проверить, и недействительные сертификаты нельзя использовать для подписи и шифрования.

После установки сертификата в строке с именем владельца может появиться значок:

- — сертификат не удалось проверить;
- — сертификат недействителен.

Что делать в этом случае, см. таблицу ниже.

Таблица 1. Описание статусов сертификатов

Статус	Действия
• Не найден сертификат издателя • Ошибка построения цепочки сертификатов • Корневой сертификат не установлен в хранилище	Установите в хранилище все сертификаты цепочки
• Не найден действительный CRL • Срок действия CRL истёк • Срок действия CRL не наступил • Цепочка содержит сертификат, который не удалось проверить	Получите в УЦ актуальный CRL и установите его в хранилище
Сертификат недействителен	Если это личный сертификат, получите новый сертификат и установите его. Если это сертификат получателя, запросите у получателя новый сертификат

Настройка автоматического обновления CRL

Если в сертификате заданы **точки распространения CRL**, включите автоматическое обновление CRL:

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Выберите **Точки распространения CRL**.
- 3 Выберите сертификат и нажмите **Изменить**.
- 4 Задайте адрес и период опроса точки.
- 5 Нажмите на переключатель справа от названия сертификата. CRL будут загружены, а затем будут обновляться автоматически с заданным периодом опроса.

Задайте адреса точек распространения CRL вручную, если:

- на смартфоне нет доступа к точкам, указанным в сертификате, и в вашей корпоративной сети есть локальная точка;
- в сертификате не указаны точки.

Для этого:

- 1 Узнайте URL точки у администратора вашей корпоративной сети.
- 2 На главном экране проведите сверху вниз и выберите **Настройки**.
- 3 Выберите **Точки распространения CRL**.
- 4 Нажмите на строку с названием УЦ, нажмите **Изменить** и задайте адрес точки. Поддерживается протокол HTTP. Если точек несколько, нажмите **Добавить адрес**.
- 5 Задайте период опроса точек.



Рисунок 4. Настройка автоматического обновления CRL

Для сертификатов, в которых не указаны точки распространения CRL, настройте автоматическое обновление CRL:

- 1 На экране **Точки распространения** проведите сверху вниз и нажмите **Добавить**.
- 2 На экране **Добавление CDP** выберите сертификаты, затем проведите по экрану справа налево. Сертификаты будут добавлены в список.
- 3 Задайте URL и период опроса точек.

Экспорт сертификатов в файлы *.cer и *.pem

Чтобы экспортировать личные сертификаты и сертификаты получателей, установленные в ViPNet PKI Client, в файлы *.cer и *.pem (например, для архивирования или передачи другим пользователям):



Примечание. Об экспорте сертификата с ключом ЭП см. [ниже](#).

- 1 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 2 Нажмите и удерживайте строку сертификата.
- 3 Выберите **Экспортировать сертификат**.
- 4 В поле **Формат файла** выберите формат файла экспорта.
- 5 Нажмите **Экспортировать сертификат**.
- 6 Нажмите **Сохранить файл**.
- 7 Укажите имя и папку для сохранения файла.
- 8 Вверху справа нажмите **Выбрать**.
- 9 После сообщения **Файл сохранен** проведите по экрану справа налево.

Перенос сертификатов и ключей ЭП между устройствами

Экспорт сертификата и ключа ЭП в PFX-файл



Внимание! Вы можете экспортировать сертификат вместе с ключом ЭП, только если при создании запроса на этот сертификат было разрешено экспортировать ключ ЭП.

- 1 На главном экране проведите сверху вниз и выберите **Сертификаты**.

- 2 Нажмите и удерживайте строку сертификата.
- 3 Выберите **Экспортировать сертификат и ключ ЭП**.
- 4 Введите пароль хранилища ViPNet PKI Client и нажмите **Подтвердить**.
- 5 Выберите алгоритм шифрования или оставьте значение по умолчанию.
- 6 Нажмите **Экспортировать сертификат**.
- 7 Задайте пароль PFX-файла и нажмите **Продолжить**.
- 8 Нажмите **Сохранить файл**.
- 9 Укажите имя и папку для сохранения PFX-файла.
- 10 Вверху справа нажмите **Выбрать**.
- 11 После сообщения **Файл сохранен** проведите по экрану справа налево.

Сертификат и ключ ЭП будут сохранены в PFX-файл, который вы можете перенести на другое устройство.



Внимание! Переносите файл с сертификатом и ключом ЭП на другое устройство только доверенным способом. Например, используйте защищённый канал или внешнее устройство, но не электронную почту или сетевые хранилища.

Импорт сертификата и ключа ЭП из PFX-файла

- 1 Перенесите PFX-файл на устройство.
- 2 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 3 Проведите сверху вниз и выберите **Установить сертификат**.
- 4 Выберите PFX-файл.
- 5 Введите пароль PFX-файла и нажмите **Продолжить**.
- 6 Нажмите **Импортировать сертификат**.
- 7 Введите пароль хранилища ViPNet PKI Client и нажмите **Продолжить**.



Примечание. Если после установки сертификата в строке с именем владельца появилось предупреждение, см. [Проверка сертификатов](#).

Удаление сертификатов и ключей ЭП

Вы можете удалить:

- сертификат и соответствующий ключ ЭП — например, аннулированный личный сертификат с ключом ЭП;

- только сертификат — например, неиспользуемый сертификат получателя.

Удаление сертификата и ключа ЭП

- 1 Если сертификат и ключ ЭП хранятся:
 - на ключевом носителе — [подключите носитель к устройству](#);
 - в облачном сервисе ЭП — [подключитесь к облачному сервису ЭП](#).
- 2 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 3 Нажмите и удерживайте строку сертификата.
- 4 Нажмите **Удалить сертификат и ключ ЭП**.



Рисунок 5. Удаление сертификата и ключа ЭП

- 5 В зависимости от места хранения сертификата:
 - хранилище ViPNet PKI Client — введите пароль;
 - облачный сервис ЭП — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло);
 - ключевой носитель — введите PIN-код.



Примечание. Если вы введёте неверный пароль хранилища ViPNet PKI Client 10 раз подряд, ViPNet PKI Client заблокируется на 15 минут.

Удаление сертификата

- 1 На главном экране проведите сверху вниз и выберите **Сертификаты**.
- 2 Нажмите и удерживайте строку сертификата.
- 3 Нажмите **Удалить сертификат**.

Использование облачных сервисов ЭП

Настройка подключения к сервису

Если в вашей организации используется ViPNet PKI Service, настройте подключение к нему. Это позволит создавать запросы на сертификаты, сохранять личные сертификаты и ключи ЭП в защищённом хранилище ViPNet PKI Service и использовать их для [подписи](#) и [расшифрования](#) файлов на любом устройстве с ViPNet PKI Client.

Чтобы настроить подключение к облачному сервису ЭП:

- 1 У оператора сервера подписи получите:
 - Адрес ViPNet PKI Service. Поддерживаемый протокол — HTTPS.
 - Имя и пароль учётной записи пользователя.
 - Корневой сертификат УЦ, в котором издан сертификат ViPNet PKI Service, а также все сертификаты цепочки и соответствующие CRL.
- 2 [Установите полученные сертификаты и CRL.](#)

На главном экране проведите сверху вниз и выберите **Настройки**.

- 1 Нажмите **Облачные сервисы**.
- 2 Выберите  **Использовать облачные сервисы** и задайте:
 - Название облачного сервиса.
 - Адрес ViPNet PKI Service и порт 9441 в формате `https://<IP-адрес>:9441`.

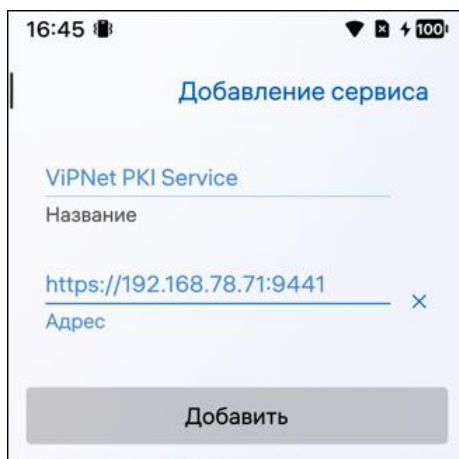


Рисунок 6. Настройка подключения к ViPNet PKI Service

- 3 Нажмите **Добавить**.
- 4 Подключитесь к облачному сервису ЭП.

Подключение к сервису

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Облачные сервисы**.
- 3 В списке выберите облачный сервис ЭП и нажмите **Подключить**.
- 4 Введите имя и пароль учётной записи.

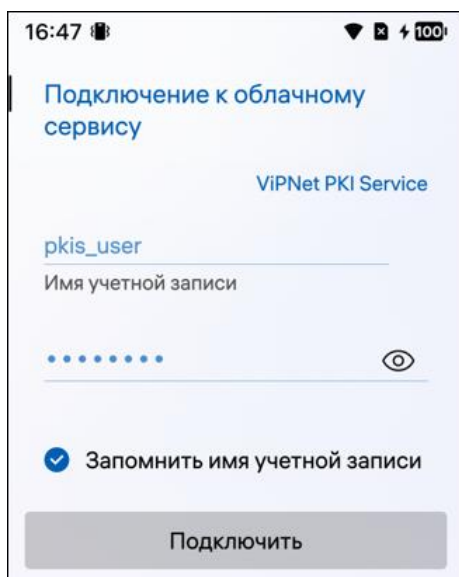


Рисунок 7. Подключение к облачному сервису ЭП

- 5 Нажмите **Подключить**.
- 6 Если вы подключаетесь впервые:

6.1 Введите разовый пароль, полученный у оператора сервера подписи, затем задайте и подтвердите постоянный.

6.2 Нажмите **Сменить пароль**.



Примечание. Если вы забыли постоянный пароль, обратитесь к оператору сервера подписи и получите новый разовый пароль.

В разделе **Сертификаты** появятся сертификаты, хранимые в облачном сервисе. Они будут отмечены значком .

Продолжительность сессии — 1 час. После этого потребуется повторное подключение.

Изменение настроек подключения к сервису

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Облачные сервисы**.
- 3 Нажмите на облачный сервис ЭП.
- 4 Нажмите  **Изменить**.

Смена пароля учётной записи

Срок действия постоянного пароля учётной записи — 6 месяцев. По истечении этого срока при подключении к облачному сервису ЭП потребуется сменить пароль.

Чтобы сменить пароль до истечения этого срока:

На главном экране проведите сверху вниз и выберите **Настройки**.

- 1 Нажмите **Облачные сервисы**.
- 2 Нажмите на облачный сервис ЭП.
- 3 Нажмите  **Сменить пароль**.
- 4 Введите текущий пароль, затем задайте и подтвердите новый.
- 5 Нажмите **Сменить пароль**.

Удаление настроек подключения к сервису

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Облачные сервисы**.
- 3 Нажмите на облачный сервис ЭП.
- 4 Нажмите  **Удалить**.

Подпись и зашифрование файлов

Требования к сертификатам для подписи и зашифрования

- [Сертификат действителен](#).
- ЭП сертификата действительна.
- Личный сертификат, который используется для подписи, содержит расширение **Использование ключа** со значением **Цифровая подпись**.
- Сертификат получателя, который используется для зашифрования, содержит расширение **Использование ключа** со значением **Согласование ключей**.



Внимание! Если ваш сертификат или сертификат получателя не соответствует указанным требованиям, вы не сможете выбрать его для подписи или зашифрования.

Подписание файла



Примечание. Максимальный размер файла для подписания прикреплённой или откреплённой подписью — 300 Мбайт, для подписания XAdES-подписью — 10 Мбайт.

- 1 Если сертификат для подписи хранится:
 - на ключевом носителе — [подключите носитель к устройству](#);
 - в облачном сервисе ЭП — [подключитесь к облачному сервису ЭП](#).
- 2 На главном экране выберите **Подписание файла**.
- 3 Выберите файл для подписи.
- 4 Выберите сертификат.
- 5 Проведите по экрану слева направо.
- 6 Выберите **Тип подписи**:

- **CAdES-подпись (прикрепленная)** — документ и подпись сохраняются в одном файле (выбрано по умолчанию);
- **CAdES-подпись (открепленная)** — подпись сохраняется отдельно от подписываемого файла;
- **XAdES-подпись (enveloped)** — XML-подпись, добавляется в документ (для файлов формата XML).

7 Чтобы добавить к ЭП подтверждение точного времени подписания файла:

Внимание! При подписании файла с помощью сертификата и ключа ЭП, хранящегося в облачном сервисе ЭП:



- в облачном сервисе ЭП должен быть установлен сертификат УЦ, издавшего сертификат TSP-службы, а также при наличии сертификаты всех УЦ из цепочки и соответствующие CRL;
 - облачный сервис ЭП должен иметь доступ к TSP-службе.
-

7.1 Нажмите **Штамп времени** и включите **Прикрепить штамп времени к подписи**.

7.2 Введите адрес **TSP-службы** и проведите по экрану слева направо.

Рисунок 8. Подписание файла

8 Нажмите **Подписать**.



Примечание. Если для подписания файла вы выбрали сертификат, хранящийся в облачном сервисе ЭП, может потребоваться подтверждение операции. Введите код подтверждения.

9 В зависимости от места хранения ключей ЭП:

- хранилище ViPNet PKI Client — введите пароль;
- облачный сервис ЭП — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло);
- ключевой носитель — введите PIN-код.



Примечание. Если вы введёте неверный пароль хранилища ViPNet PKI Client 10 раз подряд, ViPNet PKI Client заблокируется на 15 минут.

10 В окне сообщения об успешном выполнении операции нажмите **Сохранить файл**.

11 После сообщения **Файл сохранен** проведите по экрану справа налево.



Примечание. К расширению файлов с прикреплённой ЭП добавляется *.sig, с откреплённой — *.detached.sig. Не изменяйте эти расширения.

Зашифрование файла

- 1 Если сертификат для зашифрования файла хранится:
 - на ключевом носителе — [подключите носитель к устройству](#);
 - в облачном сервисе ЭП — [подключитесь к облачному сервису ЭП](#).
- 2 На главном экране нажмите **Зашифрование файла**.
- 3 Выберите файл для зашифрования.



Примечание. Максимальный размер файла для зашифрования — 300 Мбайт.

- 4 Выберите один или несколько сертификатов получателей.
- 5 Проведите по экрану слева направо.
- 6 Выберите алгоритм шифрования или оставьте значение по умолчанию.

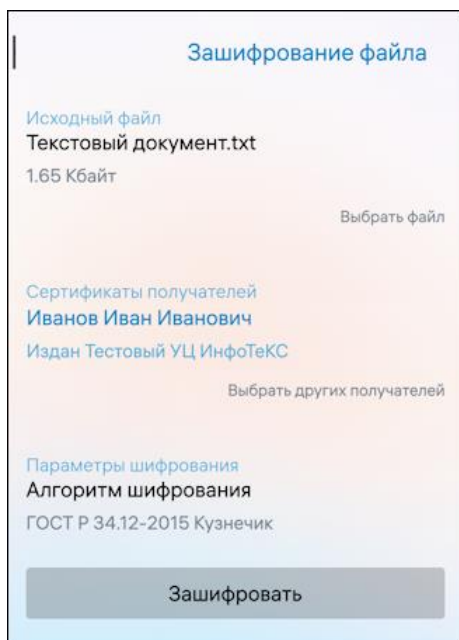


Рисунок 9. Зашифрование файла

- 7 Нажмите **Зашифровать**.
- 8 На экране **Файл зашифрован** нажмите **Сохранить файл**.
- 9 После сообщения **Файл сохранен** проведите по экрану справа налево.



Примечание. К зашифрованным файлам добавляется расширение *.enc. Не изменяйте это расширение.

Работа с файлами, полученными от других пользователей

Если вы получили файл с расширением:

- *.sig, *.xml — проверьте ЭП.
- *.enc — расшифруйте.
- *.sig.enc, *.xml.enc — расшифруйте, а затем проверьте ЭП.

Проверка ЭП

- Если вы получили файл *.sig, использовалась [прикреплённая ЭП](#).
- Если вы получили документ и файл подписи *.sig или *.detached.sig, использовалась [откреплённая ЭП](#).
- Если вы получили файл *.xml, использовалась XML-подпись.

Примечание.



- Максимальный размер файла для проверки прикреплённой и откреплённой ЭП — 500 Мбайт.
 - Максимальный размер XML-документа для проверки ЭП — 15 Мбайт.
-

Чтобы проверить ЭП:

- 1 Для проверки подписи в облачном сервисе ЭП [подключитесь к нему](#).
- 2 На главном экране нажмите **Проверка подписи файла**.
- 3 Выберите вид ЭП.
- 4 Выберите файл, подпись которого вы хотите проверить.

Если использовалась откреплённая ЭП, выберите файл подписи, а затем в окне **Проверка подписи** выберите исходный файл.

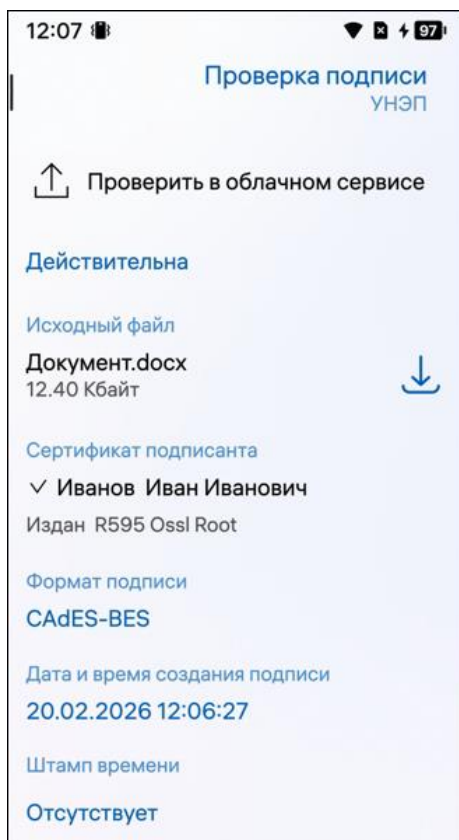


Рисунок 10. Проверка ЭП

- 5 Чтобы проверить подпись в облачном сервисе ЭП, нажмите  **Проверить в облачном сервисе**.
- 6 После проверки подписи вы можете:
 - Сохранить исходный файл, если использовалась прикреплённая ЭП — нажмите  напротив имени файла.
 - Просмотреть информацию о сертификате подписанта — нажмите на название сертификата.

Расшифрование файла



Примечание. Максимальный размер файла для расшифрования — 500 Мбайт.

- 1 Если сертификат для расшифрования файла хранится:
 - на ключевом носителе — [подключите носитель к устройству](#);
 - в облачном сервисе ЭП — [подключитесь к облачному сервису ЭП](#).
- 2 На главном экране нажмите **Расшифрование файла**.

- 3 Выберите файл для расшифрования.
- 4 Выберите сертификат для расшифрования.



Примечание. Если для расшифрования файла вы используете сертификат, хранящийся в облачном сервисе ЭП, может потребоваться подтверждение операции. Введите код подтверждения.

- 5 В зависимости от места хранения ключей ЭП:
 - хранилище ViPNet PKI Client — введите пароль;
 - облачный сервис ЭП — приложение проверит связь с сервисом. Может потребоваться повторное подключение (например, если время сессии истекло);
 - ключевом носителе — введите PIN-код.
-



Примечание. Если вы введёте неверный пароль хранилища ViPNet PKI Client 10 раз подряд, ViPNet PKI Client заблокируется на 15 минут.

- 6 В окне сообщения об успешном выполнении операции нажмите **Сохранить файл**.

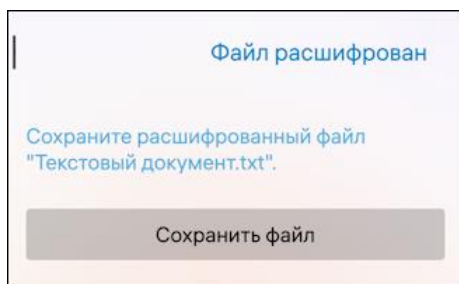


Рисунок 11. Расшифрование файла

- 7 После сообщения **Файл сохранен** проведите по экрану справа налево.

Подключение к сайтам, использующим TLS ГОСТ

Порядок настройки подключения к сайтам

- 1 Если вы будете подключаться к сайтам с аутентификацией пользователя, убедитесь, что ваш сертификат соответствует [требованиям](#).
- 2 Настройте TLS-соединение:
 - 2.1 На главном экране проведите сверху вниз и выберите **Настройки**.
 - 2.2 Нажмите **TLS ГОСТ**.
 - 2.3 [Установите корневой сертификат УЦ и соответствующий CRL](#).
 - 2.4 [Установите корневой сертификат для TLS ГОСТ в хранилище устройства](#).
 - 2.5 [Включите TLS ГОСТ](#).
 - 2.6 Настройте прокси-сервер для вашего подключения к интернету.
- 3 [Подключитесь к сайту](#).
- 4 При необходимости [посмотрите информацию о текущих TLS-соединениях](#).

Требования к сертификатам для работы по TLS ГОСТ

Сертификат сервера

При подключении к сайту, использующему TLS ГОСТ проверяется, что:

- Сертификат [действителен](#).
- ЭП сертификата действительна.
- Сертификат содержит адрес сайта.
- Сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности сервера**;

- **Использование ключа** с одним или несколькими значениями: **Цифровая подпись**, **Шифрование ключей**, **Согласование ключей**.



Внимание! Если для сертификата не будет выполнено хотя бы одно из требований, вы не сможете подключиться к сайту.

Сертификат пользователя

При подключении к сайту, использующему TLS ГОСТ с аутентификацией пользователя, проверяется, что:

- **Сертификат действителен.**
- ЭП сертификата действительна.
- Сертификат содержит расширения:
 - **Расширенное использование ключа** со значением **Проверка подлинности клиента**.
 - **Использование ключа** со значением **Цифровая подпись** и (или) **Согласование ключей**.



Внимание! Если для сертификата не будет выполнено хотя бы одно из требований, вы не сможете выбрать сертификат при подключении к сайту.

Установка корневого сертификата для TLS ГОСТ

1 Запустите приложение **Terminal**.

2 Получите права суперпользователя:

```
$ devel-su
```

3 Установите сертификат:

```
# cp /home/<имя  
пользователя>/local/share/ru.infotecs/vipnetpkiclient/.itcs/certs/root_aurora.pem  
/etc/pki/ca-trust/source/anchors/ && update-ca-trust
```



Совет. Вы можете скопировать команду из приложения. Для этого на экране **Настройка TLS ГОСТ** нажмите и удерживайте текст шага 2, а затем нажмите **Скопировать**.

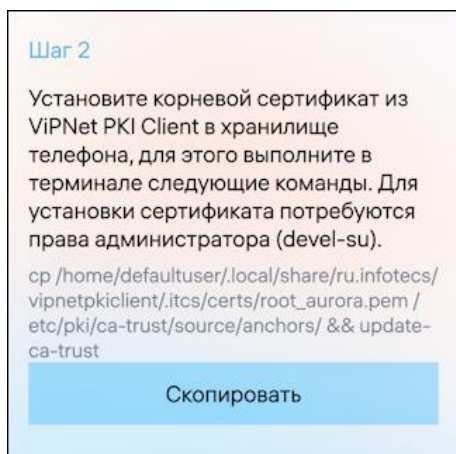


Рисунок 12. Копирование команды для установки корневого сертификата

- 4 Выполните перезагрузку.

Включение TLS ГОСТ



Внимание! Если вы настроили локальный прокси-сервер для подключения к интернету и не разрешили соединение по TLS ГОСТ, подключение к интернету будет недоступно.

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **TLS ГОСТ**.
- 3 Чтобы включить поддержку TLS-соединений по алгоритмам ГОСТ, нажмите **Разрешить соединение**.
На экране отобразятся адрес и порт прокси-сервера. Если вы впервые включаете TLS ГОСТ, перед подключением к сайтам [настройте прокси-сервер](#).
- 4 Чтобы устанавливать соединения по TLS ГОСТ при отсутствии доверия к сертификату сервера, нажмите **Разрешать небезопасные соединения**.



Внимание! Подключайтесь к сайтам с недоверенными сертификатами, только если вы уверены в их надёжности. Иначе злоумышленники могут получить доступ к вашим личным данным.

Настройка прокси-сервера

После первого [включения TLS ГОСТ](#) настройте прокси-сервер для подключения к интернету:



Примечание. Если после настройки прокси-сервера нет подключения к интернету, см. [Возможные неполадки](#).

- 1 В настройках устройства выберите **WLAN** или **Мобильная сеть**.
- 2 Проведите сверху вниз и выберите **Расширенные настройки**.
- 3 Для параметра **Конфигурация прокси-серверов** установите значение **Вручную**.
- 4 В поле **Адрес прокси-сервера** введите `localhost`.
- 5 В поле **Номер порта** задайте порт, указанный в настройках TLS-соединения (по умолчанию — 9991).
- 6 Включите **Глобальный прокси-сервер**.

Если TLS ГОСТ включён, настройки прокси-сервера можно также посмотреть в ViPNet PKI Client на экране **Настройки**.

Подключение к сайту

Чтобы подключиться к сайту, использующему TLS ГОСТ, в браузере введите адрес сайта:

- Если для подключения не требуется аутентификация пользователя, соединение будет установлено.
- Если для подключения требуется аутентификация пользователя, выберите сертификат и введите пароль хранилища ViPNet PKI Client или PIN-код ключевого носителя. Соединение будет установлено.

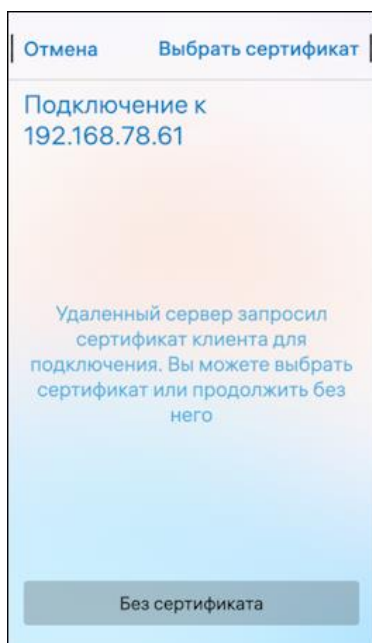


Рисунок 13. Подключение с аутентификацией пользователя

При первом подключении к сайту выбранный сертификат сохраняется в кеш, и при последующих подключениях к этому сайту в текущей сессии выбирать сертификат не потребуется.

Чтобы выбрать другой сертификат для подключения, удалите сертификат из кеша:

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **TLS ГОСТ**.
- 3 Нажмите **Очистить кеш сертификатов**.

Просмотр информации о TLS-соединениях

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **TLS ГОСТ > История подключений**.
- 3 Чтобы посмотреть подробные сведения о соединении, нажмите на строку с адресом сайта.

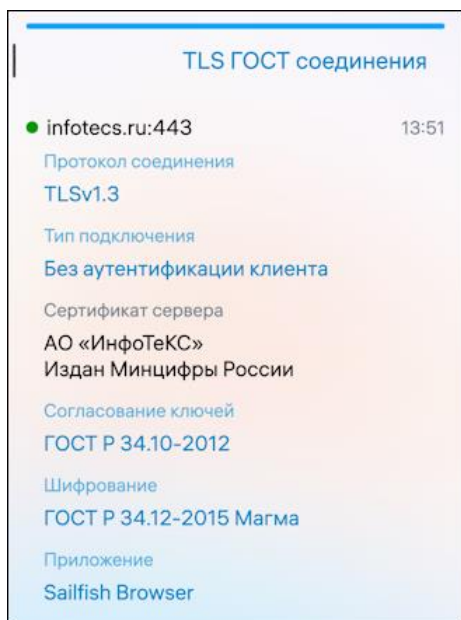


Рисунок 14. Сведения о TLS-соединениях

- 4 Чтобы посмотреть подробные сведения о сертификате сервера, нажмите на строку сертификата.

Служебные функции

Смена пароля хранилища ViPNet PKI Client

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Смена пароля хранилища телефона**.
- 3 Введите текущий пароль, затем укажите и повторите новый.
- 4 Нажмите **Сменить пароль**.

Обновление лицензии

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Данные об активации**.
- 3 Проведите сверху вниз и выберите **Обновление лицензии**.
- 4 Введите номер телефона и серийный номер, который вы получили при покупке лицензии.
- 5 Нажмите **Активировать**, вам придет SMS с кодом активации.
- 6 Введите полученный код.
- 7 После сообщения **Приложение активировано** проведите по экрану справа налево.

Сброс настроек приложения

Вам может потребоваться сбросить настройки приложения, удалить сертификаты и ключи ЭП без удаления приложения:

- чтобы продолжить работу с приложением, если вы забыли пароль хранилища ViPNet PKI Client;
- удалить личную информацию, если вы передаёте устройство другому пользователю.

Для этого:

- 1 На главном экране проведите сверху вниз и выберите **Настройки**.
- 2 Нажмите **Удаление данных**.

3 Чтобы удалить лицензию, выберите **Удалить данные о регистрации**. Для продолжения работы потребуется заново активировать приложение.

4 Нажмите **Удалить**.

Чтобы продолжить работу с приложением:

1 [Создайте хранилище ViPNet PKI Client](#).

2 [Установите сертификаты](#).

Удаление приложения

Удалите приложение стандартными средствами ОС Аврора. При этом:

- лицензия, все установленные сертификаты и ключи ЭП удаляются автоматически;
- подписанные и зашифрованные файлы не удаляются.

Возможные неполадки

Нет подключения к интернету

Если вы [настроили прокси-сервер](#) для подключения к интернету, но не [включили TLS ГОСТ в настройках приложения](#), при работе с сайтами в браузере может возникнуть ошибка.

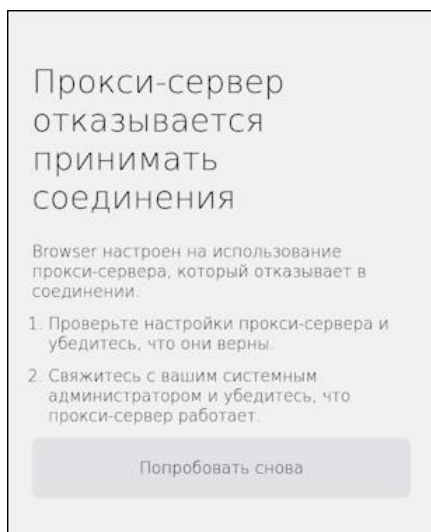


Рисунок 15. Ошибка при подключении к интернету

Выполните одно из действий:

- Если больше не требуется подключаться к сайтам, использующим TLS ГОСТ, [отключите использование прокси-сервера](#) для подключения к интернету.
- [Включите TLS ГОСТ](#).

Не удаётся установить TLS-соединение через предустановленный браузер

На устройствах под управлением Аврора версии 5.2 может не устанавливаться TLS-соединение через предустановленный браузер.

Возможная причина

В ярлыке браузера нет разрешения `WebView`.

Способ устранения



Совет. Перед внесением изменений сохраните копию файла

`/usr/share/applications/ru.omp.browserpwa.desktop` в произвольную папку.

- 1 В любом текстовом редакторе откройте файл
`/usr/share/applications/ru.omp.browserpwa.desktop` от имени администратора.
- 2 Если в списке разрешений `Permissions` нет разрешения `WebView`, добавьте его через разделитель, например:
`Permissions=<разрешение 1>;<разрешение 2>;...<разрешение n>;WebView`
- 3 Сохраните файл.
- 4 Перезагрузите устройство.

Термины и сокращения

CRL

Список серийных номеров сертификатов, которые были аннулированы, отозваны или действие которых было прекращено.

OCSP-служба (служба проверки статуса сертификатов)

Доверенный субъект инфраструктуры открытых ключей, предоставляющий информацию о статусах сертификатов по запросам в режиме реального времени.

TLS (Transport Layer Security)

Криптографический протокол транспортного уровня для защищённой передачи данных между узлами в интернете. Использует асимметричные ключи, симметричное шифрование данных и коды аутентичности сообщений.

TSP-служба (служба штампов времени)

Доверенный субъект инфраструктуры открытых ключей, оказывающий услуги по созданию штампов времени.

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

Действительность сертификата

Сертификат, для которого выполняются условия:

- срок действия сертификата наступил и не истёк;
- сертификат не отозван;
- цепочка сертификатов полна, и все сертификаты цепочки действительны;
- электронная подпись сертификата верна.

Запрос на сертификат

Документ с информацией, которая требуется для издания сертификата ключа проверки электронной подписи в удостоверяющем центре (владелец, срок действия, назначение сертификата и прочее).

Ключ электронной подписи (ключ ЭП)

Секретный (закрытый) ключ из пары асимметричных ключей, который представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Корневой сертификат

Самоподписанный сертификат головного удостоверяющего центра. Используется для подписи сертификатов, издаваемых головным удостоверяющим центром, с целью обеспечения доверия к ним.

Отзыв сертификата

Признание сертификата недействительным до истечения срока действия.

Открепленная подпись

Тип электронной подписи, при использовании которой электронная подпись файла помещается в отдельный контейнер. Для проверки такой электронной подписи требуется контейнер с электронной подписью и исходный файл.

Прикрепленная подпись

Тип электронной подписи, при использовании которой исходный файл и электронная подпись помещаются в один контейнер. Для проверки электронной подписи требуется только этот контейнер.

Точка распространения CRL

Источник, из которого можно получить актуальные CRL для проверки статуса отзыва сертификата. URL таких точек указываются в сертификатах, издаваемых удостоверяющим центром, в поле **Точка распределения списка отзыва (CRL)**.

Удостоверяющий центр (УЦ)

Организация, уполномоченная издавать сертификаты ключа проверки электронной подписи для физических и юридических лиц, а также управлять жизненным циклом этих сертификатов.

Цепочка сертификатов

Иерархия сертификатов, в которой каждый сертификат подписан вышестоящим сертификатом вплоть до корневого (самоподписанного) сертификата. Наличие для сертификата полной цепочки действительных сертификатов подтверждает доверие к этому сертификату.

Электронная подпись (ЭП)

Созданная криптографической операцией дополнительная информация, с помощью которой можно подтвердить авторство и неизменность основной информации.