Интернет Банк-Клиент

Инструкция по первоначальной настройке рабочего ключа

2026 г.

Содержание

Часть I	Подготовка рабочего места
Часть II	Генерация ключевых пар
Часть III	Работа с токенами
Часть IV	Особенности настройки в ОС Astra Linux
	Контакты службы поддержки

Перед началом работы

Инструкция описывает первоначальную настройку рабочего места и создание ключа электронной подписи для работы в системе «Интернет Банк-Клиент». Части I–III относятся к ОС Windows, часть IV — к ОС Astra Linux.

Что понадобится	Компьютер с доступом в интернет и правами локального администратора; выданный Банком токен Рутокен ЭЦП; логин и пароль для входа в систему; принтер для печати актов признания ключа.
Адрес системы	https://client.isbnk.org
PIN-коды по умолчанию	Пользователь — **12345678**, администратор — **87654321** (установлены производителем токена)

Условные обозначения: названия кнопок, полей и пунктов меню приведены в кавычках «…», команды терминала — моноширинным шрифтом.

ЧАСТЬ I

Подготовка рабочего места

Выполните эти действия один раз на компьютере, с которого будет вестись работа в системе.

1. Подготовьте автоматизированное рабочее место (АРМ), соответствующее минимальным требованиям:

Процессор	Intel Pentium G4400 или производительнее
Оперативная память	8 ГБ
Накопитель	256 ГБ
Операционная система	Windows 10 или новее
Браузер	Mozilla Firefox, Яндекс Браузер, Microsoft Edge или Google Chrome (версия не позднее 135.0.7049.85)
Права пользователя	Локальный администратор

2. Установите драйвер для выданного средства криптографической защиты информации (СКЗИ) **Рутокен ЭЦП**. Скачайте с сайта производителя версию, соответствующую вашей операционной системе:
https://www.rutoken.ru/support/download/windows/

3. Установите плагин для браузера **КриптоПро ЭЦП Browser plug-in** (cadesplugin):
https://www.cryptopro.ru/products/cades/plugin/

4. Откройте в браузере страницу системы https://client.isbnk.org и добавьте этот сайт в список доверенных. Разрешите скачивание криптоплагина **BSSPluginSetup** и установите его — автоматически или вручную из папки «Загрузки».

5 Запустите приложение **«Хост для BSSPlugin»** любым удобным способом, например через меню «Пуск», или убедитесь, что оно уже запущено.

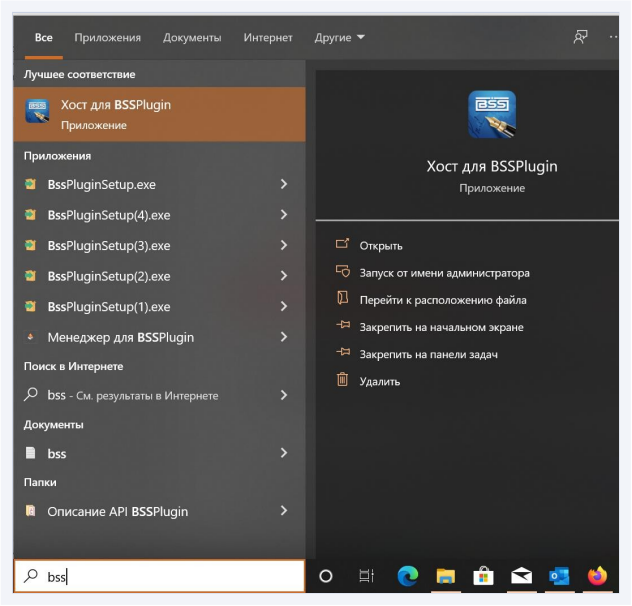

Рисунок 1. Запуск «Хоста для BSSPlugin» через меню «Пуск»

ЧАСТЬ II

Генерация ключевых пар

На этом этапе на токене создаются ключи электронной подписи и формируется запрос в Банк на выпуск сертификата.

1. Подключите токен к компьютеру, откройте страницу https://client.isbnk.org и войдите в систему, используя логин и пароль, выданные Банком.

2. Откроется мастер создания запроса на новый сертификат. Нажмите «Далее».

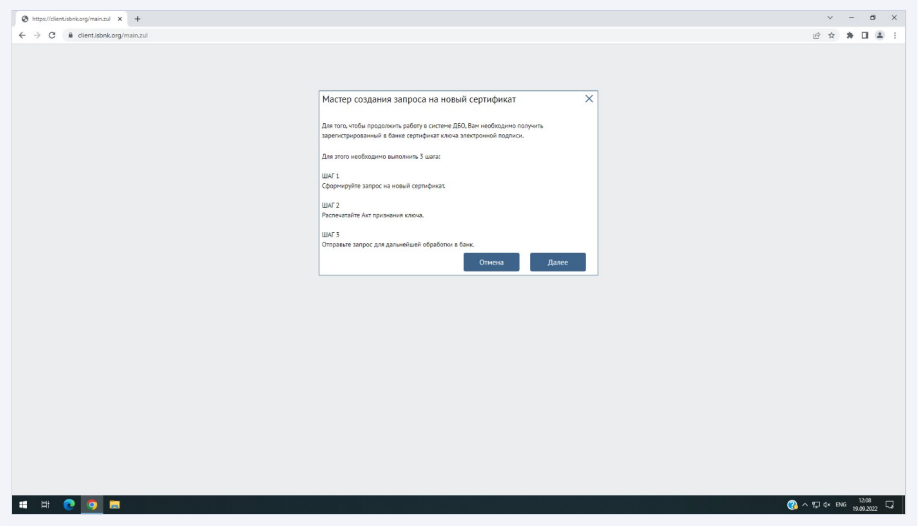

Рисунок 2. Мастер создания запроса на новый сертификат

3 Заполните поля запроса на новый сертификат:

- проверьте поля «Фамилия» и «Имя Отчество» — если они не заполнены автоматически, заполните их;
- заполните обязательные поля: «Адрес электронной почты», «Подразделение», «Адрес» и «Наименование субъекта».

> **ОБРАТИТЕ ВНИМАНИЕ**
>
> В поле «Наименование субъекта» укажите субъект Российской Федерации, например: г. Москва, Ленинградская область, Алтайский край. Если организация находится за пределами России, достаточно указать город.

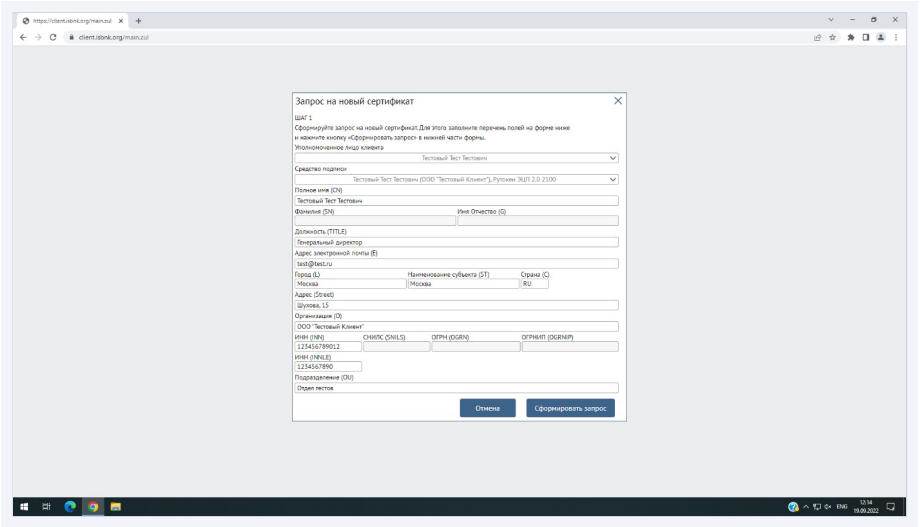

Рисунок 3. Форма запроса на новый сертификат

4 Убедитесь, что все обязательные поля заполнены, и нажмите «Сформировать запрос». Откроется окно «Результаты проверки» со списком незаполненных полей, отмеченных жёлтыми треугольниками. Поля «СНИЛС» и «ОГРНИП» заполнять не обязательно. Если в списке остались только они, нажмите «Сохранить»; если указаны другие поля, нажмите «Закрыть» и заполните их.

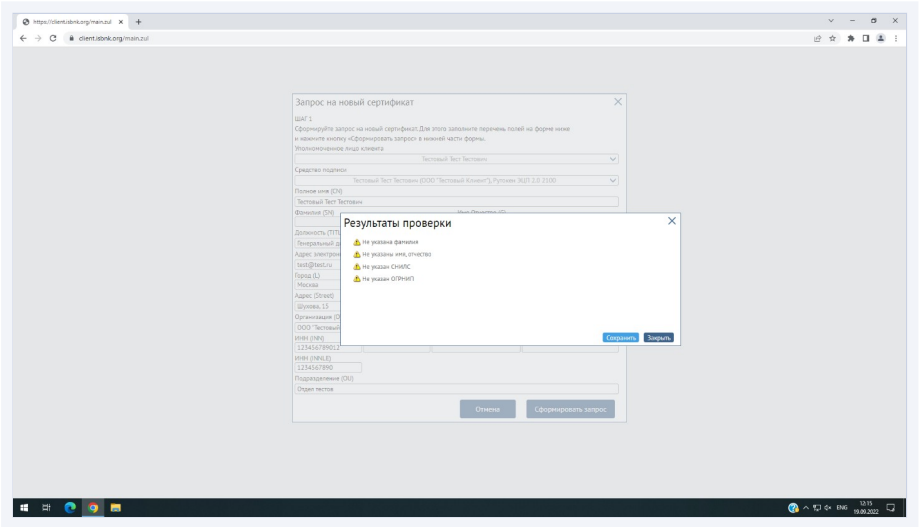

Рисунок 4. Окно «Результаты проверки»

5 Система предложит выбрать криптоконтейнер. Выберите токен в списке, щёлкнув по нему левой кнопкой мыши, и нажмите «ОК».

> **СОВЕТ**
>
> Чтобы избежать путаницы, на этом шаге к компьютеру должен быть подключён только один токен — токен текущего пользователя.

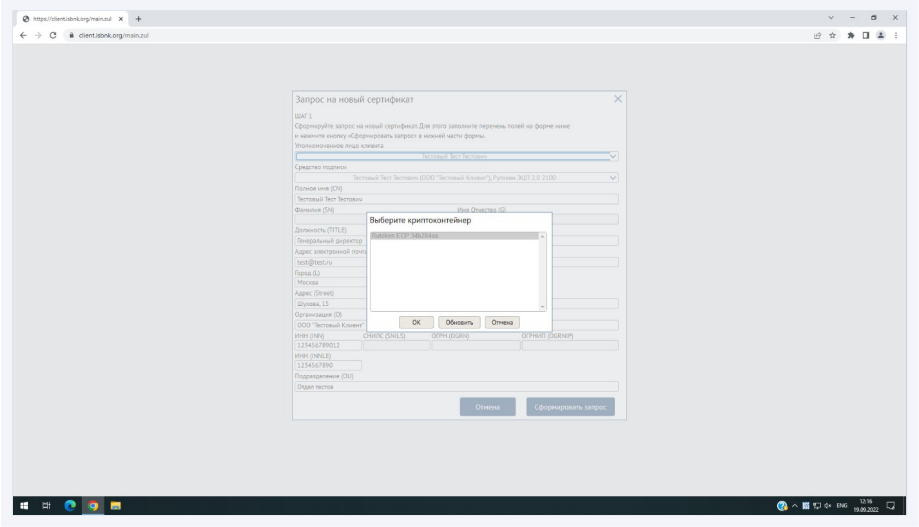

Рисунок 5. Выбор криптоконтейнера

6 Система запросит PIN-код пользователя токена. Введите его и нажмите «ОК». По умолчанию производитель устанавливает PIN-код пользователя **12345678**.

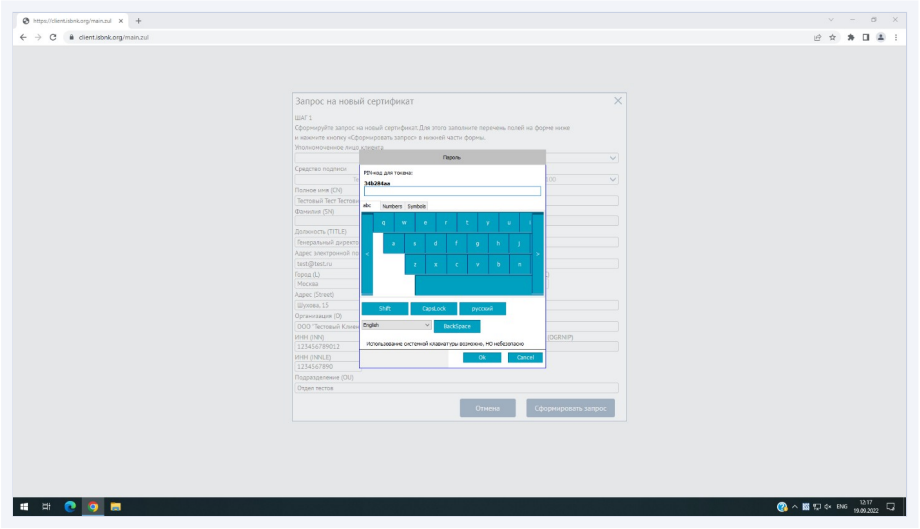

Рисунок 6. Ввод PIN-кода пользователя

7 После успешного создания ключей система предложит распечатать акт признания ключа. Распечатайте акт в двух экземплярах для каждого пользователя и нажмите «Далее».

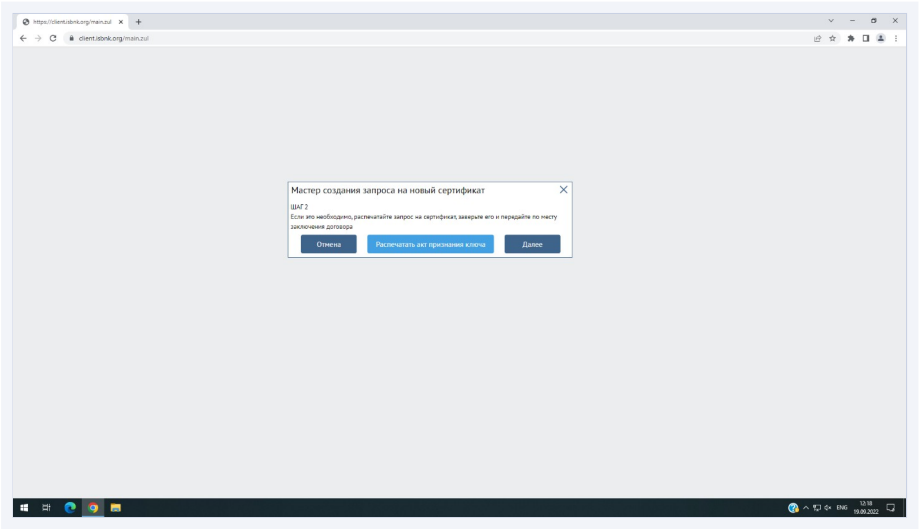

Рисунок 7. Печать акта признания ключа

8 Отправьте запрос в Банк.

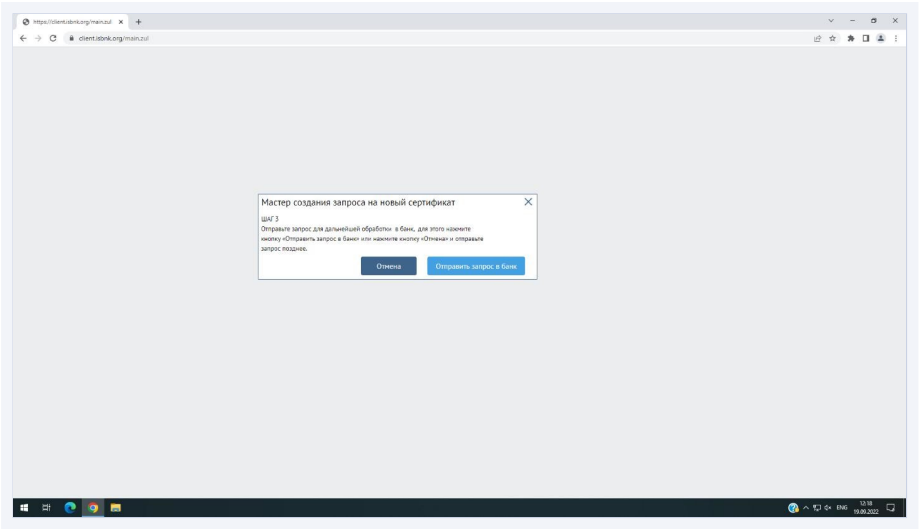

Рисунок 8. Отправка запроса в Банк

9 Дважды нажмите «ОК». При успешной отправке появится сообщение «Успешно отправлено: 1».

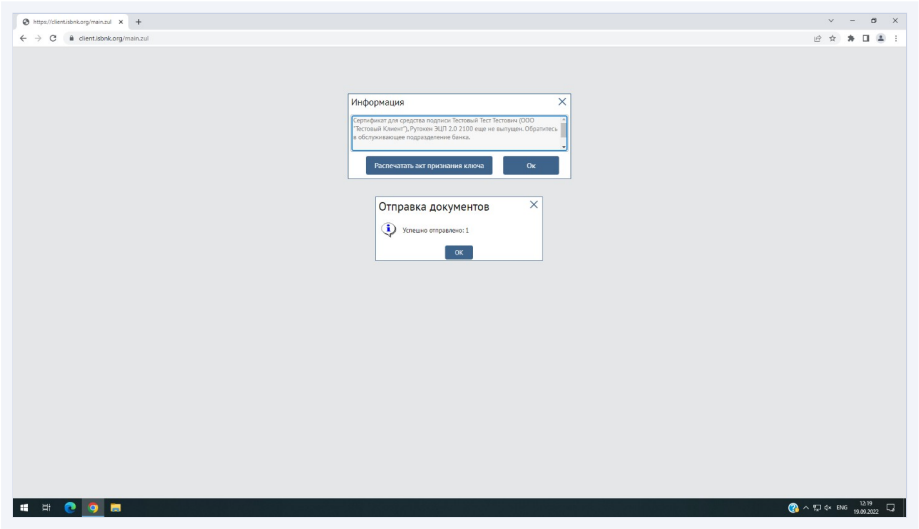

Рисунок 9. Подтверждение успешной отправки запроса

РЕЗУЛЬТАТ

Ключевые пары созданы и записаны на ваш токен, акты признания ключа распечатаны.

10 Для начала работы в системе оформите акты признания ключа:

- подпишите акт(ы) личной подписью уполномоченного лица;
- подпишите акт(ы) личной подписью руководителя организации;
- заверьте акт(ы) печатью организации;
- передайте акт(ы) в Банк.

11 После того как Банк подтвердит ваши ключи и выпустит сертификаты, вы сможете работать в системе.

ЧАСТЬ III

Работа с токенами

Раздел описывает обслуживание токенов: удаление ключей и смену PIN-кодов. При повседневной работе в системе эти действия не требуются.

1 Для управления токенами используется программа **«Панель управления Рутокен»**. Её можно запустить из Панели управления Windows или с помощью ярлыка на рабочем столе.

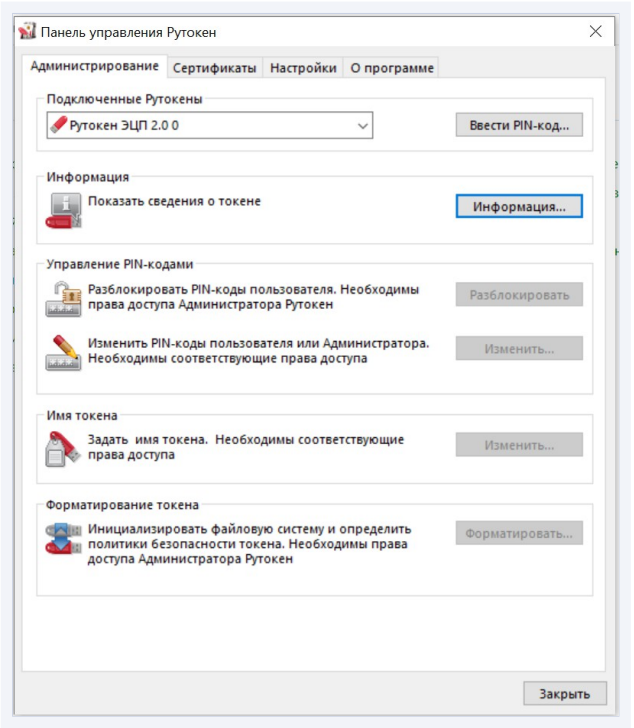

Рисунок 10. Панель управления Рутокен, вкладка «Администрирование»

Панель понадобится, чтобы удалить с токена устаревшие ключи, сменить PIN-коды и настроить токен в соответствии с политикой информационной безопасности вашей организации.

2 **Удаление ключевых пар.** Введите PIN-код администратора (по умолчанию — **87654321**), выберите ключевую пару, которую нужно удалить, и нажмите «Удалить».

> **ВНИМАНИЕ**
> Удалённые с токена ключи уничтожаются безвозвратно и не подлежат восстановлению. Банк не хранит копии ваших ключей — после удаления потребуется сгенерировать новые.

3 **Смена PIN-кодов.** Введите текущий PIN-код и воспользуйтесь функцией «Изменить PIN-коды пользователя или Администратора» на вкладке «Администрирование».

> **ВНИМАНИЕ**
> Новые PIN-коды будут известны только вам. В случае их утраты Банк не сможет помочь в восстановлении.

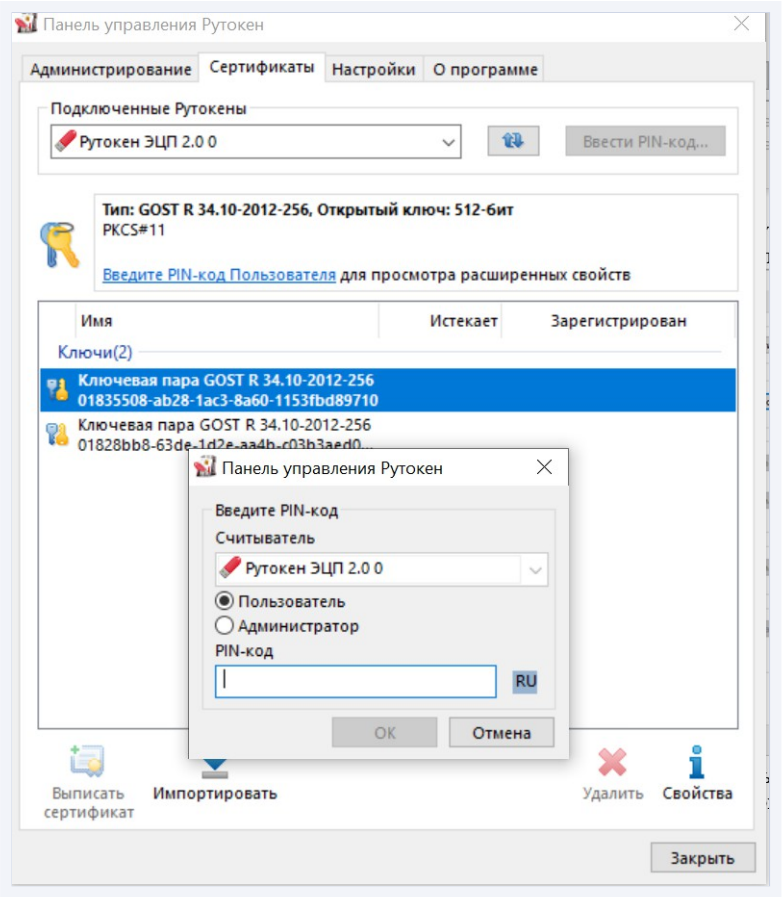

Рисунок 11. Ввод PIN-кода в Панели управления Рутокен

ЧАСТЬ IV

Особенности настройки в ОС Astra Linux

Выполните эти действия, если рабочее место работает под управлением ОС Astra Linux. После их завершения ключи создаются так же, как в Windows.

1. Требуется ОС **Astra Linux версии 1.7 или выше**.

2. В актуальных версиях Astra Linux дополнительные драйверы для Рутокен ЭЦП не требуются: токен поддерживается штатно благодаря библиотеке libccid (версии 1.4.2 и выше). При необходимости установите компоненты по рекомендациям производителя, например:

```
sudo apt install libccid pcscd libpcsclite1 pcsc-tools
pcsc_scan    # проверка: токен должен отображаться в списке
```

Список пакетов — по данным справочного центра Astra Linux.

3. Установите браузер **Яндекс Браузер** по инструкции производителя.

4. Откройте страницу входа в систему https://client.isbnk.org и введите логин и пароль, выданные Банком.

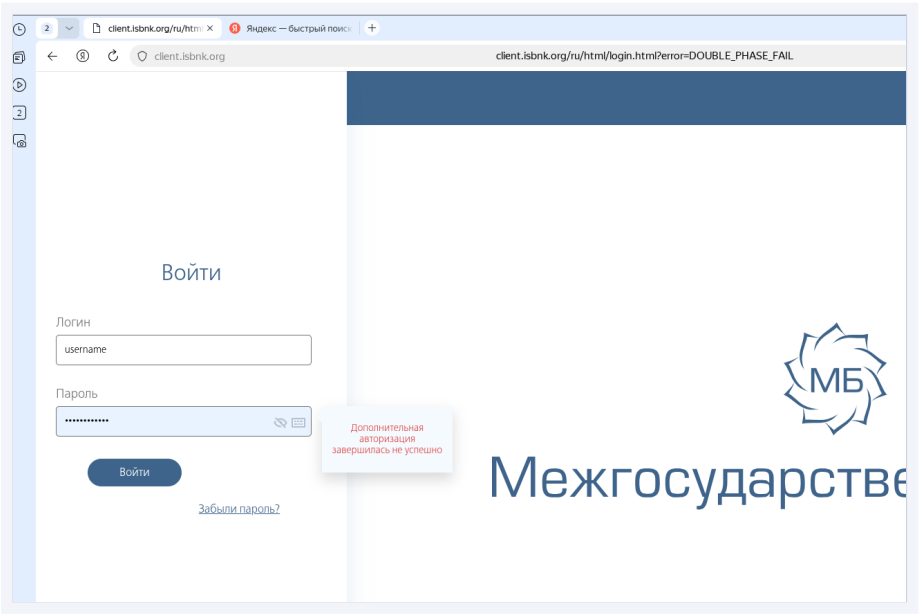

Рисунок 12. Страница входа в систему

5 Страница предложит скачать криптоплагин — нажмите «Да».

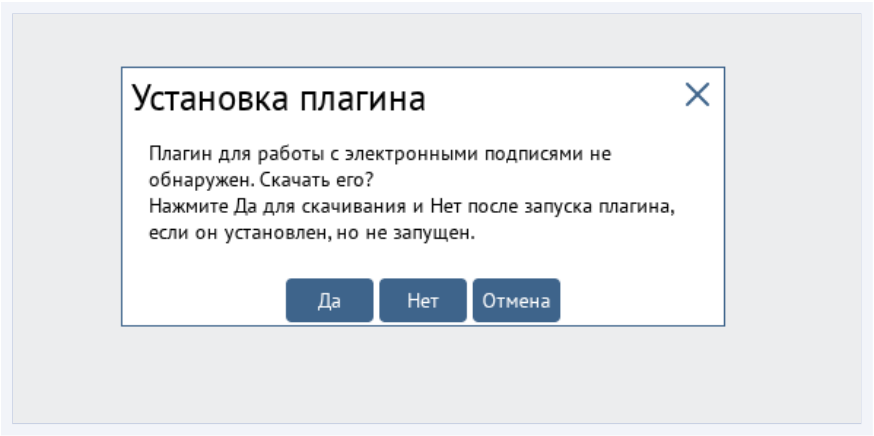

Рисунок 13. Запрос на установку плагина

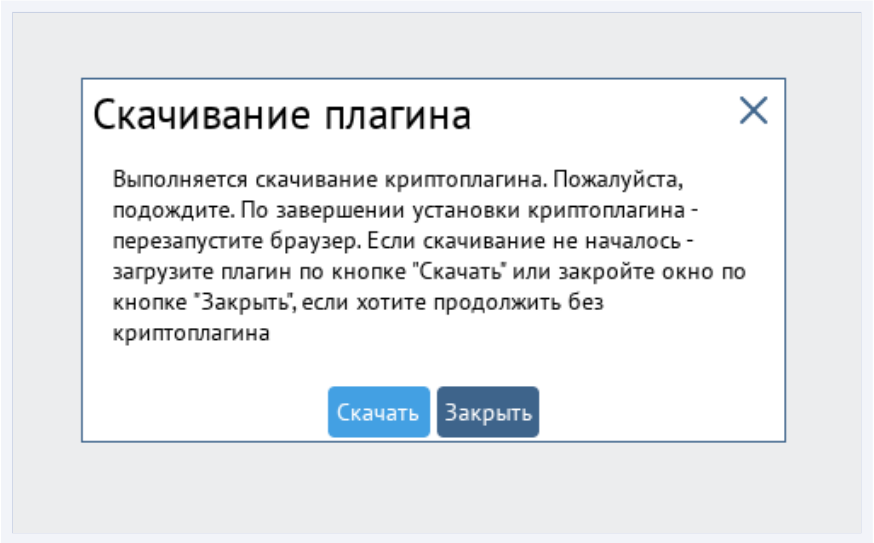

Рисунок 14. Скачивание плагина

6 Браузер сохранит файл криптоплагина (в примере — `bssCryptoPlugin4_4.0.2.25.deb.run`). По умолчанию у этого файла нет прав на запуск.

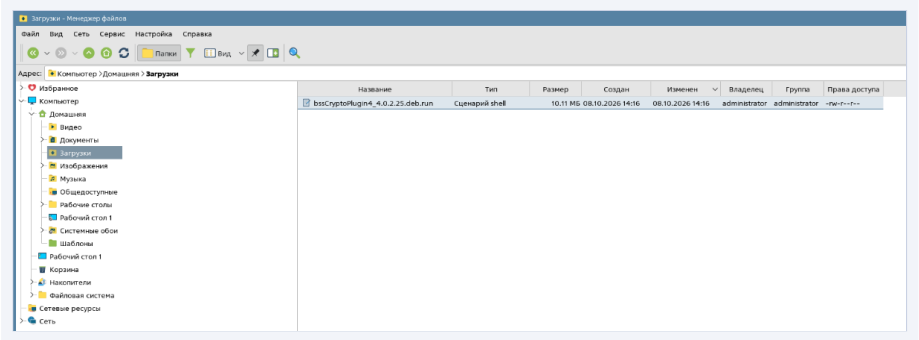

Рисунок 15. Сохранённый файл криптоплагина

7 Выдайте файлу права на запуск. В примере файл сохранён в каталоге `/home/administrator/Загрузки`, у вас путь может отличаться:

```
cd ~/Загрузки
chmod +x bssCryptoPlugin4_*.deb.run
```

> **ОБРАТИТЕ ВНИМАНИЕ**
>
> На снимке экрана использована команда `chmod 777`. Она открывает файл для записи всем пользователям системы, поэтому её применять не рекомендуется — для запуска достаточно `chmod +x`.

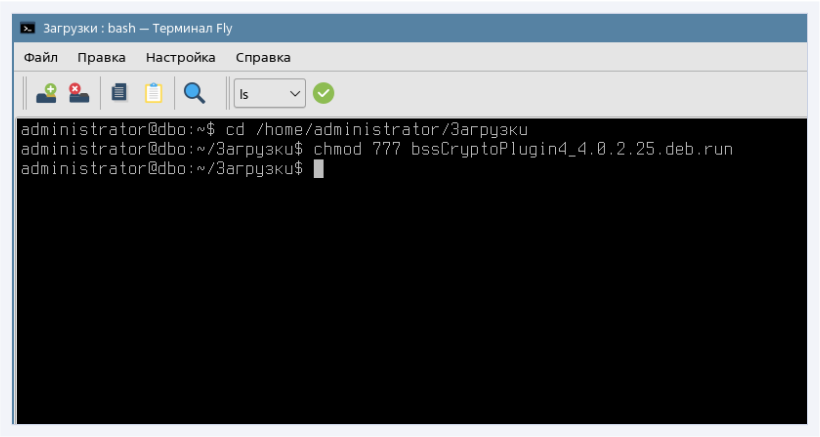

Рисунок 16. Назначение прав на запуск в терминале

8 Запустите установку пакета двойным щелчком по файлу и подтвердите действие в окне установщика.

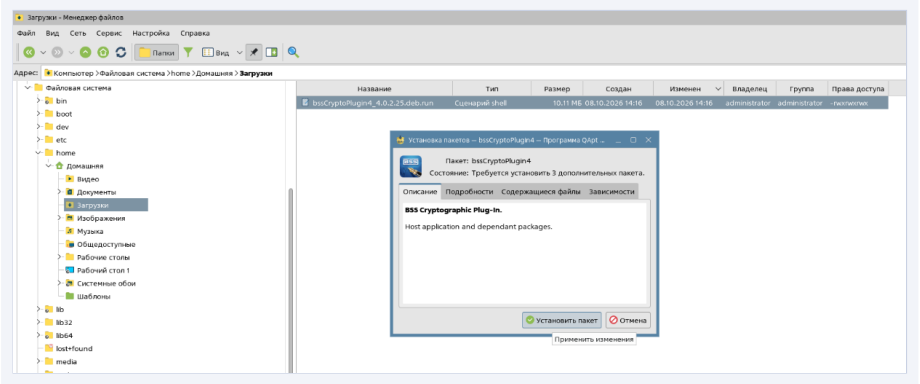

Рисунок 17. Запуск установщика

9 Введите пароль администратора.

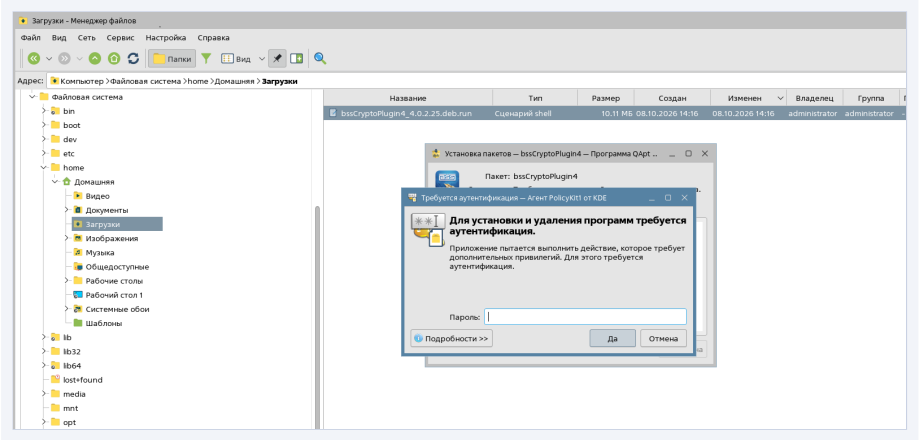

Рисунок 18. Запрос пароля администратора

10 При успешной установке появится сообщение об этом.

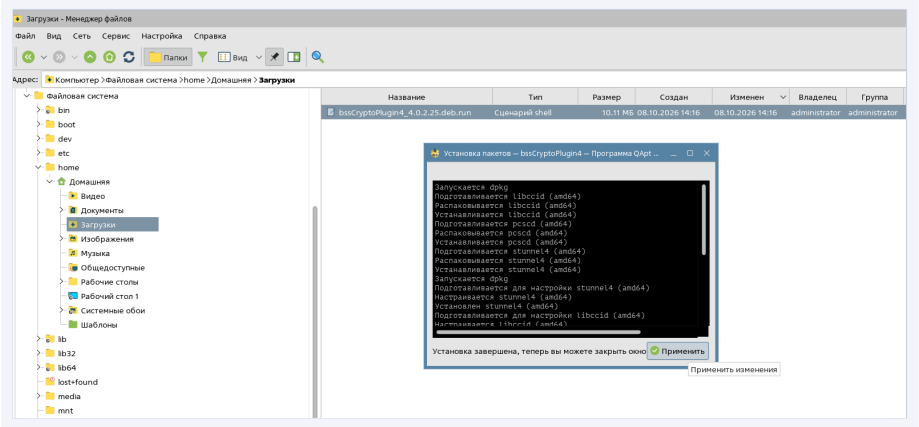

Рисунок 19. Сообщение об успешной установке

11 Криптоплагин запросит разрешение на HTTPS-соединения с сертификатами зарубежных удостоверяющих центров (УЦ). Подтвердите — нажмите «Yes».

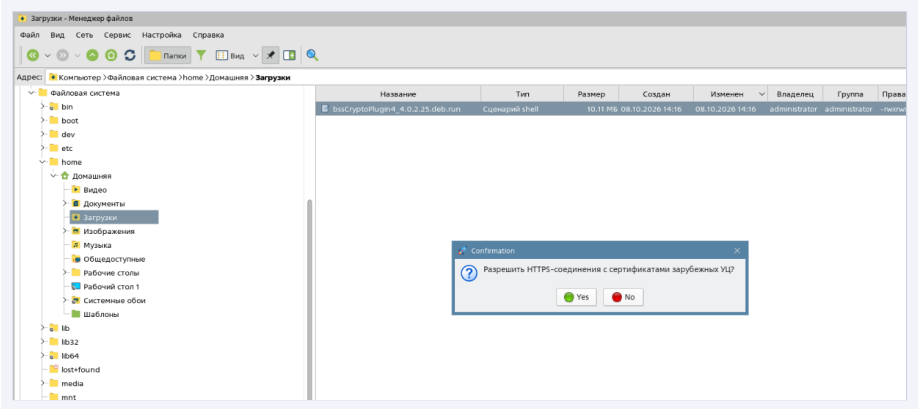

Рисунок 20. Разрешение HTTPS-соединений

12 Убедитесь, что значок криптоплагина появился в системном трее в правом нижнем углу экрана. В примере установлена версия 4.0.2.25; у вас она может отличаться.

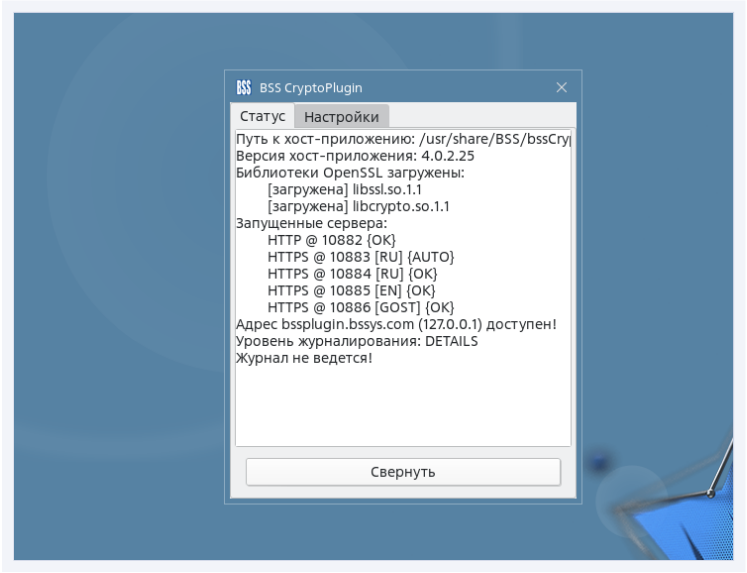

Рисунок 21. Окно состояния BSS CryptoPlugin

13 Вернитесь в браузер и разрешите сайту доступ к приложениям на устройстве.

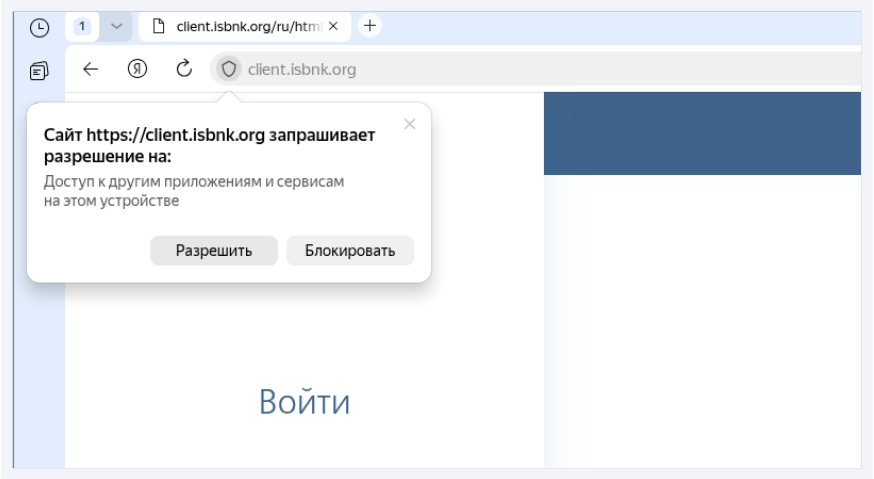

Рисунок 22. Запрос доступа к приложениям

14 Разрешите браузеру доступ к криптоплагину и добавьте страницу в список доверенных.

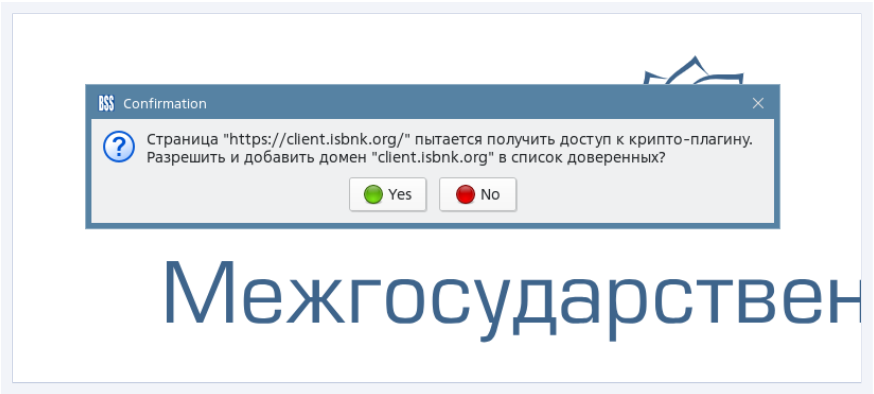

Рисунок 23. Добавление страницы в список доверенных

15 Если всё сделано правильно, появится окно ввода PIN-кода токена.

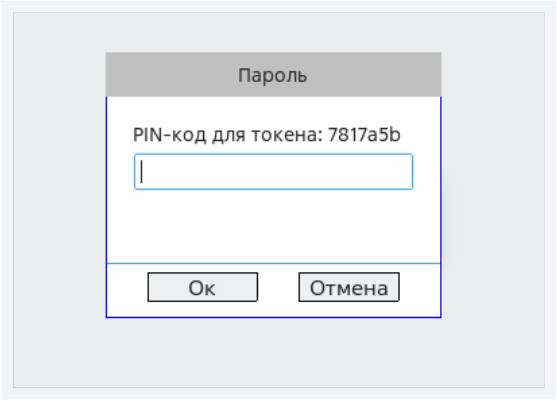

Рисунок 24. Окно ввода PIN-кода токена

РЕЗУЛЬТАТ

Настройка, специфичная для ОС Astra Linux, завершена. Дальнейшая генерация ключевых пар выполняется так же, как в ОС Windows, — см. Часть II настоящей инструкции.

Контакты службы поддержки

При возникновении вопросов обращайтесь по телефонам:

+7 (495) 958-55-22	Техническая поддержка
+7 (495) 745-23-36	Департамент расчётно-кассового обслуживания