ООО Фирма «ИнфоКрипт»

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«VPN-Key-TLS»

вариант исполнения 7

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ИНФК.11485466.4012.021 91 06

2022

Содержание

1 Введение 5

2 Назначение и условия применения 6

2.1 Назначение системы 6
2.2 Условия применения системы 6

3 Подготовка к работе 8

3.1 Инициализация устройства «VPN-Key-TLS» 8
3.2 Подключение устройства «VPN-Key-TLS» 8

4 Описание операций 11

4.1 Начало работы с устройством «VPN-Key-TLS» 11
4.2 Завершение работы с устройством «VPN-Key-TLS» 14
4.3 Разблокирование учетной записи 14
4.4 Подключение к бизнес-системе 16
4.5 Электронная подпись 16
4.5.1 Подписание документов из бизнес-системы 16
4.5.2 Подписание файла 16
4.6 Проверка электронной подписи файла 18
4.7 Шифрование 19
4.8 Расшифрование 20
4.9 Просмотр сертификатов и запросов на сертификаты 22
4.10 Сохранение сертификатов и запросов на сертификаты 24
4.11 Удаление ключевой пары 24
4.12 Удаление личного сертификата 25
4.13 Изменение PIN-кода 26
4.14 Изменение PUK-кода 27
4.15 Изменение значения таймаута 28
4.16 Генерация ключей и запросов на сертификаты 29
4.17 Создание нового транспортного сертификата 31
4.18 Создание нового сертификата первичного подключения 32
4.19 Установка сертификата 33
4.20 Установка конфигурации бизнес-систем 34
4.21 Установка списка отозванных сертификатов 34
4.22 Установка обновления программного обеспечения 35
4.23 Проверка целостности встроенного программного обеспечения 37
4.24 Установка класса СКЗИ 38
4.25 Использование HTTP-прокси для связи по TLS 39
4.26 Просмотр информации об устройстве 40

4.27 Завершение работы HTTP-сервера 41
4.28 Форматирование учётной записи 41

Определения

В настоящем документе использованы следующие термины с соответствующими определениями:

Термин	Определение
Таймаут	Время, по истечении которого неактивная сессия работы с устройством автоматически завершается
PIN-код	Код доступа к устройству
PUK-код	Дополнительный код доступа, предназначенный для разблокирования устройства после троекратного неправильного ввода PIN-кода

Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения:

Обозначение	Описание
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
НЖМД	Накопитель на жёстких магнитных дисках
ОЗУ	Оперативное запоминающее устройство
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись
TLS	Криптографический протокол, обеспечивающий защищённую передачу данных между узлами открытой сети передачи данных

1 Введение

Настоящий документ содержит руководство пользователя СКЗИ «VPN-Key-TLS» в варианте исполнения 7 (далее «VPN-Key-TLS»). Руководство включает в себя справочную информацию о «VPN-Key-TLS» и описывает конкретные действия, которые можно выполнять с помощью «VPN-Key-TLS».

В документе страницы «VPN-Key-TLS» изображены на иллюстрациях так, как они отображаются в веб-обозревателе Microsoft Edge. В других веб-обозревателях вид страниц может незначительно отличаться.

2 Назначение и условия применения

2.1 Назначение системы

СКЗИ «VPN-Key-TLS» предназначено для организации защищённого доступа через открытую сеть передачи данных к ресурсам веб-службы (например, доступа через Интернет к ресурсам интернет-банка).

Конкретный набор ресурсов, к которым можно получить доступ с помощью данного СКЗИ, указывается администратором в процессе инициализации устройства «VPN-Key-TLS».

2.2 Условия применения системы

Устройство «VPN-Key-TLS» устанавливается на компьютер, удовлетворяющий следующим программным и аппаратным требованиям:

- компьютер должен работать под управлением одной из следующих ОС:
  - Windows 7;
  - Windows 8.1;
  - Windows 10;
  - Windows 11;
  - MacOS Catalina 10.15;
  - MacOS BigSur 11;
  - MacOS Monterey 12;
  - MacOS Ventura 13;
  - ubuntu 16.04 LTS x64;
  - ubuntu 18.04 LTS x64;
  - ubuntu 20.04 LTS x64;
  - ubuntu 22.04 LTS x64;
  - Alt workstation 9 x64;
  - Alt workstation 10 x64;
  - CentOS Stream 8 x64;
  - Debian 10 x64;
  - Debian 11 x64;
  - Fedora Linux 36;
  - Mcst Elbrus 6;
  - REDOS 7.3 MUROM x64;
  - Astra Linux C2 x64;

  - Astra Linux SE 1.7.0 x64;
- процессор не ниже Pentium II;
- НЖМД ёмкостью не менее 10 Гб;
- ОЗУ ёмкостью не менее 1 Гб;
- на компьютере должен быть в наличии свободный разъём USB;
- компьютер должен быть подключен к сети передачи данных
- для обеспечения класса СКЗИ КС2 на компьютере должен быть установлен АПМДЗ, сертифицированный в соответствии с требованиями ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ.

СКЗИ «VPN-Key-TLS» может функционировать под управлением одной из следующих виртуальных сред (гипервизоров):

- Microsoft Hyper-V Server 2012/2012R2/2016/2019;
- Citrix XenServer 7.1;
- Citrix Virtual Apps and Desktops 7;
- VMWare WorkStation 16 (x86, x64);
- VMWare WorkStation Player 16 (x86, x64);
- VMWare Fusion 13;
- QEMU 7;
- VMWare vSphere ESXi (6.7, 7.0);
- Oracle VirtualBox (6.1, 7.0);
- Parallels Desktop (Mac OS) 18 (x64).

Для указанных ОС и гипервизоров должно быть обеспечено получение обновлений по безопасности. В случае подключения СКЗИ к каналам связи, выходящим за пределы контролируемой территории, не допускается использование ОС и (или) гипервизоров, производителями которых не выпускаются обновления.

3 Подготовка к работе

3.1 Инициализация устройства «VPN-Key-TLS»

Перед началом использования нового устройства «VPN-Key-TLS», необходимо его инициализировать средствами изделия «АРМ инициализации» из состава СКЗИ «VPN-Key-TLS Администратор». Процедура инициализации выполняется администратором устройства. Если администратором устройства является пользователь, ему необходимо ознакомиться с соответствующими руководствами из состава СКЗИ «VPN-Key-TLS Администратор» и выполнить изложенную там процедуру инициализации.

Инициализированное устройство «VPN-Key-TLS» обеспечивает максимально возможную степень автоматизации процесса установки и подготовки к работе. Вмешательство пользователя может потребоваться лишь в случае отключённой функции автозапуска со съёмных носителей информации, а также при наличии проблем с доступом к узлу Windows Update.

3.2 Подключение устройства «VPN-Key-TLS»

Подключение устройства «VPN-Key-TLS» к компьютеру производится в следующем порядке:

1. Вставьте устройство «VPN-Key-TLS» в разъём USB компьютера.
2. Если в операционной системе отсутствуют необходимые драйверы, при первом подключении будет произведена автоматическая установка драйверов устройства «VPN-Key-TLS». При наличии подключения к Интернету драйверы будут установлены с узла Windows Update, при отсутствии подключения к Интернету драйверы устройства

«VPN-Key-TLS» будут установлены с самого устройства. Устройство идентифицируется в системе как CD-дисковод (см. Рисунок 1).

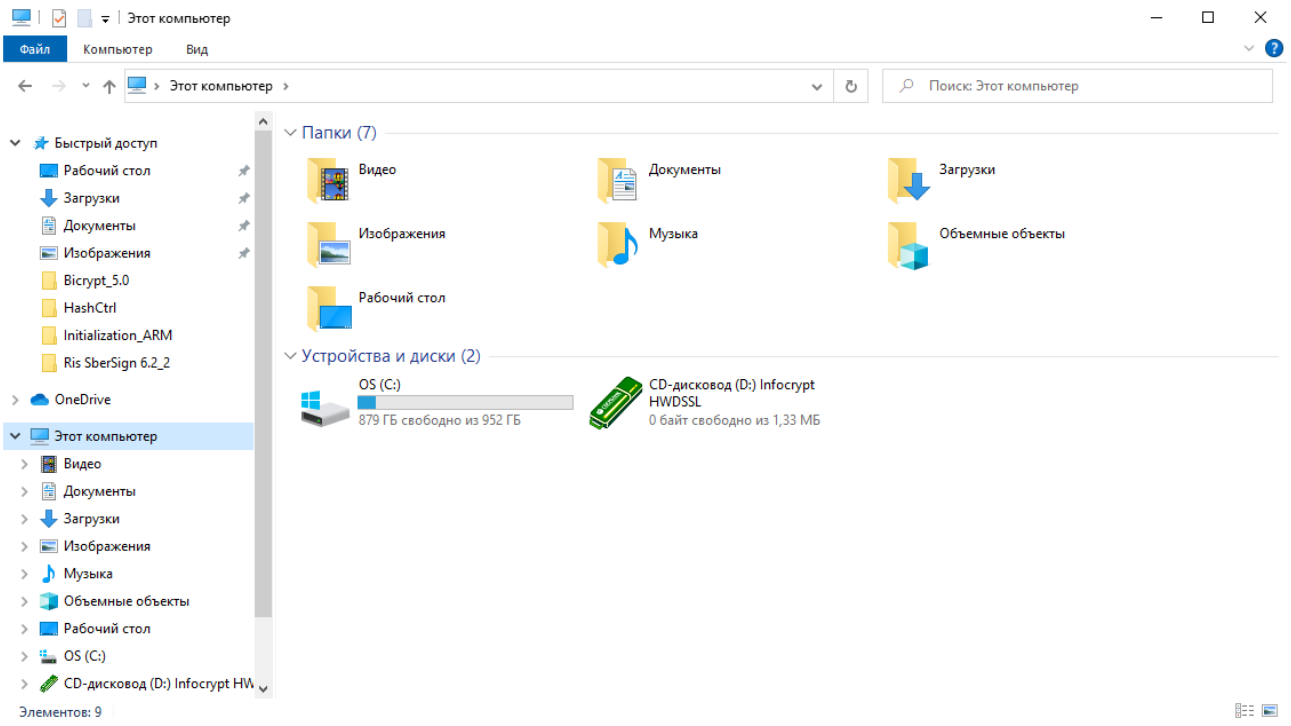


Рисунок 1 – Отображение устройства VPN-Key-TLS в Windows

3. Если в настройках операционной системы разрешён автозапуск со съёмных носителей, будет запущен установленный в операционной системе веб-обозреватель (веб-браузер) по умолчанию с открытой страницей авторизации (см. Рисунок 3). Если в настройках операционной системы запрещён автозапуск со съёмных носителей, следует с CD-дисковода, соответствующего устройству «VPN-Key-TLS» (см. Рисунок 1), вручную запустить приложение START (см. Рисунок 2). После запуска приложения через несколько секунд запустится веб-обозреватель со страницей авторизации для входа в интерфейс устройства «VPN-Key-TLS» (см. Рисунок 3). Это означает, что подключение устройства успешно завершено и можно приступать к работе.

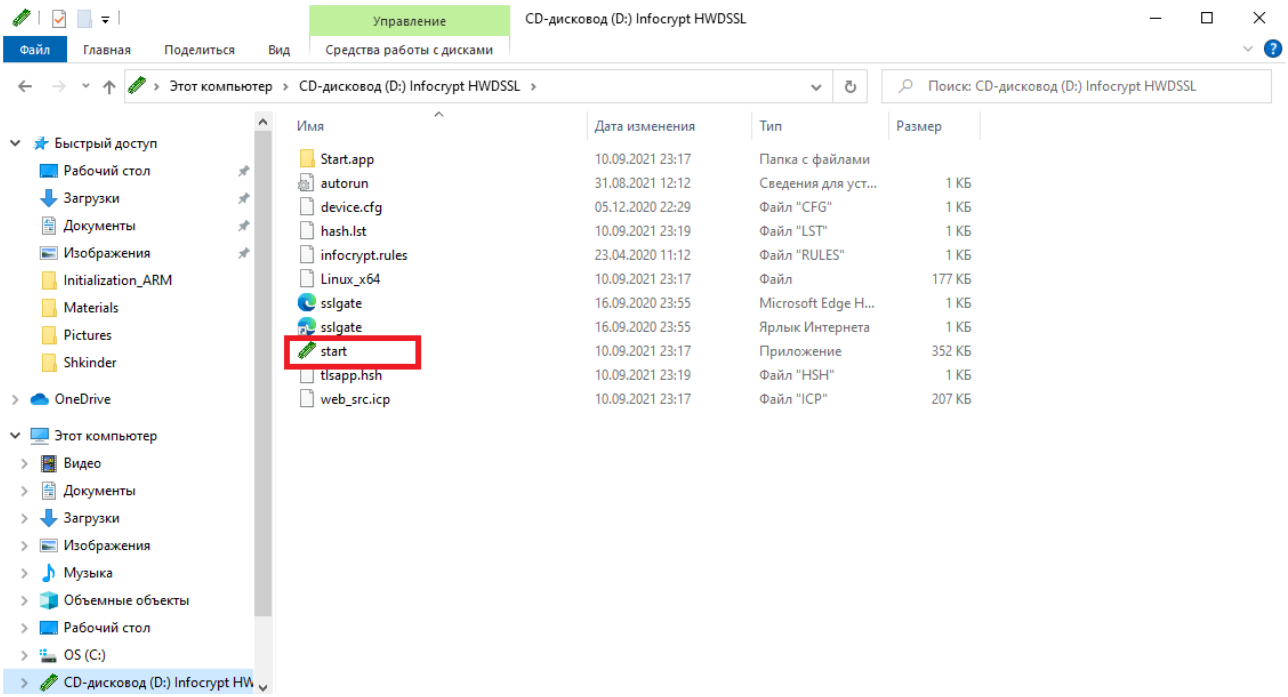


Рисунок 2 – Содержание устройства «VPN-Key-TLS»

4 Описание операций

4.1 Начало работы с устройством «VPN-Key-TLS»

Для начала работы следует подключить устройство «VPN-Key-TLS» в соответствии с процедурой подключения, описанной в разделе 3.2. В результате подключения запустится веб-обозреватель со страницей авторизации для входа в интерфейс устройства «VPN-Key-TLS» (см. Рисунок 3).

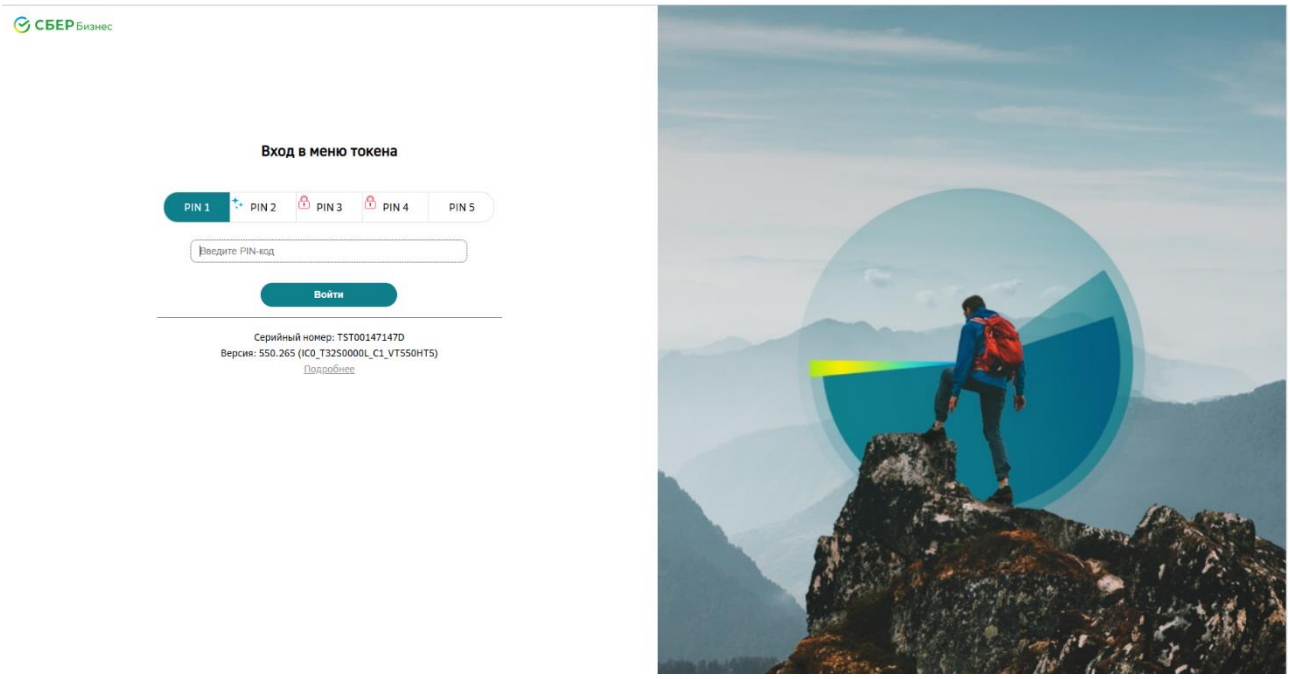


Рисунок 3 – Страница авторизации для входа в интерфейс устройства «VPN-Key-TLS»

На странице авторизации отображается серийный номер и версия встроенного ПО устройства. Для просмотра дополнительной информации об устройстве следует перейти по ссылке Подробнее.

При первом подключении устройства необходимо сверить серийный номер с указанным в формуляре и проверить целостность встроенного ПО (см. раздел 4.23).

Для входа и дальнейшего взаимодействия с устройством VPN-Key-TLS необходимо выбрать учётную запись пользователя, ввести код доступа (PIN-код), соответствующий выбранной учётной записи, и нажать кнопку **Войти**.

Если код доступа к учётной записи введён верно, на экране монитора будет отображена внутренняя страница устройства VPN-Key-TLS (см. Рисунок 4).

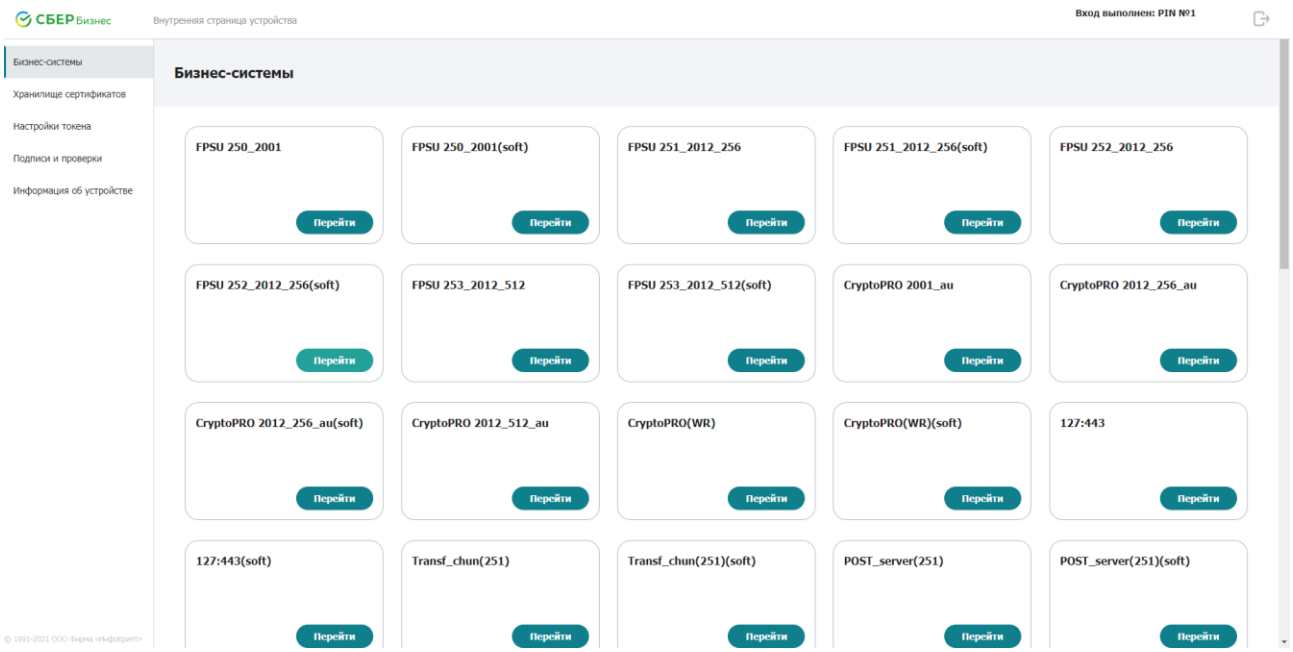


Рисунок 4 – Основная страница устройства VPN-Key-TLS

В центральной части внутренней страницы устройства VPN-Key-TLS расположены кнопки с названиями бизнес-систем, подключение к которым возможно с помощью данного устройства VPN-Key-TLS.

В левой части страницы расположено главное меню. Пункты меню **Хранилище сертификатов** и **Настройки токена**, предназначены для изменения конфигурации устройства. Пункт меню **Подписи и проверки** предназначен для подписания и проверки подписи документов, а также для шифрования файлов. Пункт меню **Информация об устройстве** предназначен для проверки целостности внутреннего ПО, завершения работы HTTP-сервера и просмотра информации об устройстве.

Если введён неверный PIN-код, на экране монитора появится сообщение об ошибке (см. Рисунок 5).

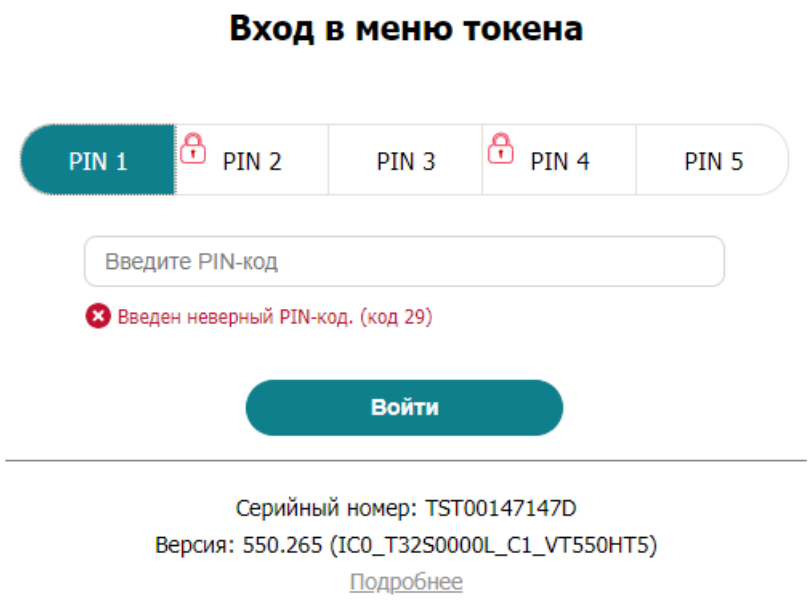


Рисунок 5 – Сообщение о неверном вводе PIN-кода

Если PIN-код введен неверно 3 раза подряд, соответствующая учётная запись блокируется, а на экране монитора появится сообщение о том, что все попытки ввода PIN-кода израсходованы (см. Рисунок 6).

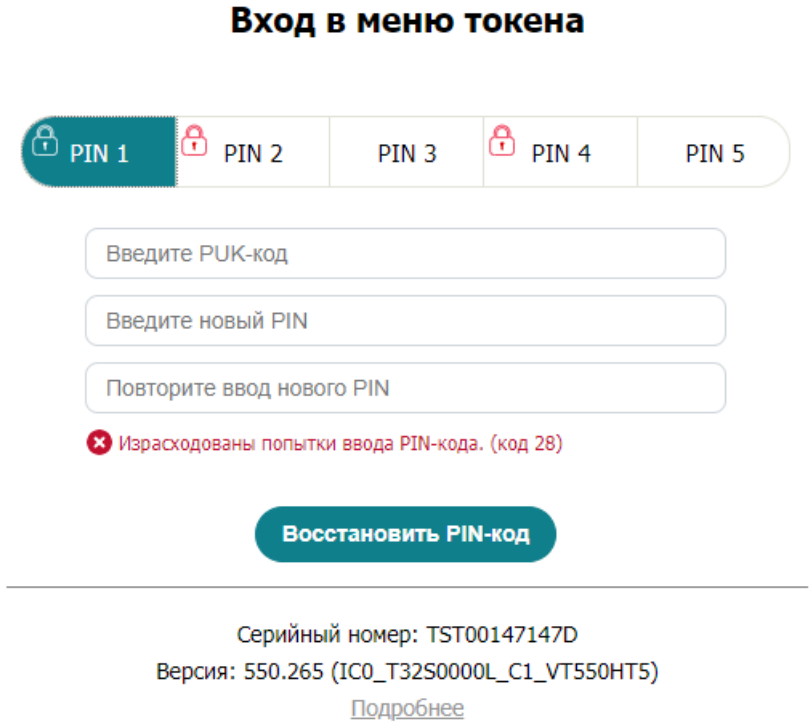


Рисунок 6 – Сообщение о том, что попытки ввода PIN-кода израсходованы

Процедура разблокирования учетной записи изложена в разделе 4.3.

При первом подключении устройства необходимо сверить серийный номер и контрольную сумму встроенного ПО, находящиеся в файле device.cfg на CD-дисководе, соответствующем устройству, а также контрольную сумму «Start.exe», находящуюся в файле tlsapp.hsh, с серийным номером и эталонными контрольными суммами, указанными в формуляре, и сменить PIN-код и PUK-код. Затем следует создать ключи ЭП, шифрования и TLS и соответствующие запросы на сертификаты, отправить созданные запросы в УЦ и по получении сертификатов установить их.

4.2 Завершение работы с устройством «VPN-Key-TLS»

Для корректного завершения работы с устройством «VPN-Key-TLS» следует выполнить следующие действия:

– завершить сеанс работы с бизнес-системой;

– вернуться на внутреннюю страницу устройства «VPN-Key-TLS»;

– щёлкнуть значок в правом верхнем углу внутренней страницы устройства «VPN-Key-TLS»;

– извлечь устройство «VPN-Key-TLS» из USB-разъёма компьютера.

4.3 Разблокирование учетной записи

Если пользователь три раза подряд ввёл неверный PIN-код, соответствующая учётная запись блокируется, а в поле «Выберите из списка свою учётную запись» перед названием заблокированной учётной записи появляется символ (см. Рисунок 7).



Рисунок 7 – Учётная запись пользователя блокирована

Для того чтобы разблокировать учётную запись, необходимо выбрать её. На открывшейся странице ввода PUK-кода (см. Рисунок 8) необходимо выполнить следующие действия:

– В поле «Введите PUK-код» ввести PUK-код, содержащийся в выданном вместе с устройством PIN-конверте.

– Ввести новый PIN-код в поле «Введите новый PIN». Длина PIN-кода должна быть равна 6 символам. Допустимыми символами являются английские буквы, цифры и спецсимволы.

– Повторно ввести новый PIN-код в поле «Повторите ввод нового PIN».

– Подтвердить изменение PIN-кода, нажав кнопку **Восстановить PIN-код**.

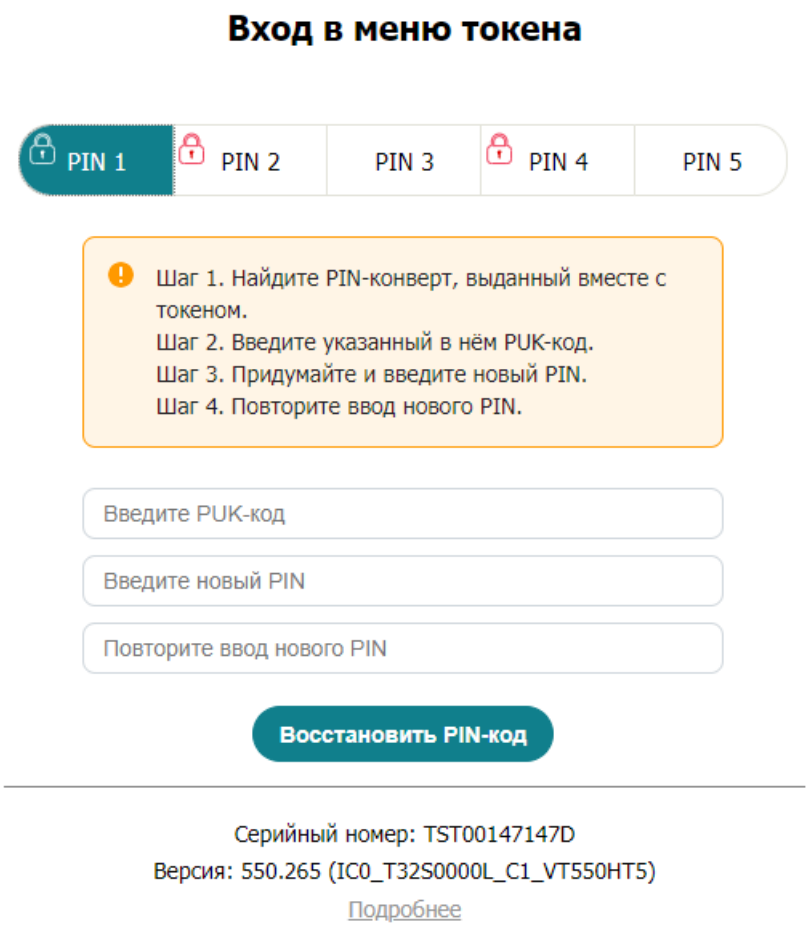


Рисунок 8 – Страница ввода PUK-кода

В случае трёх и более попыток ввода неверного PUK-кода подряд начинается период принудительной задержки, зависящий от количества предыдущих попыток ввода неверного PUK-кода подряд (Таблица 1). Введённые в течение этого периода PUK-коды не будут приняты к рассмотрению, а на экране монитора появится сообщение об ошибке.

Таблица 1 – Периоды принудительной задержки

Предыдущее число неверных попыток ввода кода подряд	0	1	2	3	4	5	6	7	8	9
Принудительная задержка до следующей попытки (в минутах)	0	0	0	15	30	60	120	180	1440	1440

Если количество принятых к рассмотрению попыток ввода неверного PUK-кода подряд достигнет 10, данная учётная запись будет заблокирована окончательно, и её дальнейшее восстановление будет невозможно.

При вводе корректного PUK-кода, принятого к рассмотрению, счётчик предыдущего количества неверных попыток ввода PUK-кода подряд обнуляется.

Если количество принятых к рассмотрению попыток ввода неверного PUK-кода достигнет 300 без смены PUK-кода, то данная учётная запись также будет заблокирована окончательно, и её дальнейшее восстановление будет невозможно.

4.4 Подключение к бизнес-системе

Для того чтобы начать работу с бизнес-системой, необходимо нажать кнопку с соответствующим названием в центральной части внутренней страницы устройства «VPN-Key-TLS» (см. Рисунок 4).

После этого откроется страница выбранной бизнес-системы.

4.5 Электронная подпись

Устройство «VPN-Key-TLS» предоставляет возможность подписания электронной подписью как документов, с которыми ведется работа в бизнес-системе, так и произвольных файлов.

4.5.1 Подписание документов из бизнес-системы

Устройство «VPN-Key-TLS» предоставляет возможность подписания электронной подписью документов, когда во время работы с бизнес-системой возникает такая необходимость. Для подписания документа никаких дополнительных действий с устройством не требуется.

4.5.2 Подписание файла

Устройство «VPN-Key-TLS» предоставляет возможность подписания электронной подписью произвольных файлов.

Для того чтобы подписать файл, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Подписи и проверки**.

На открывшейся странице (см. Рисунок 9) следует перейти по ссылке «Подписание документа» в центральной части страницы или нажать кнопку **Подписать** в правой части страницы.

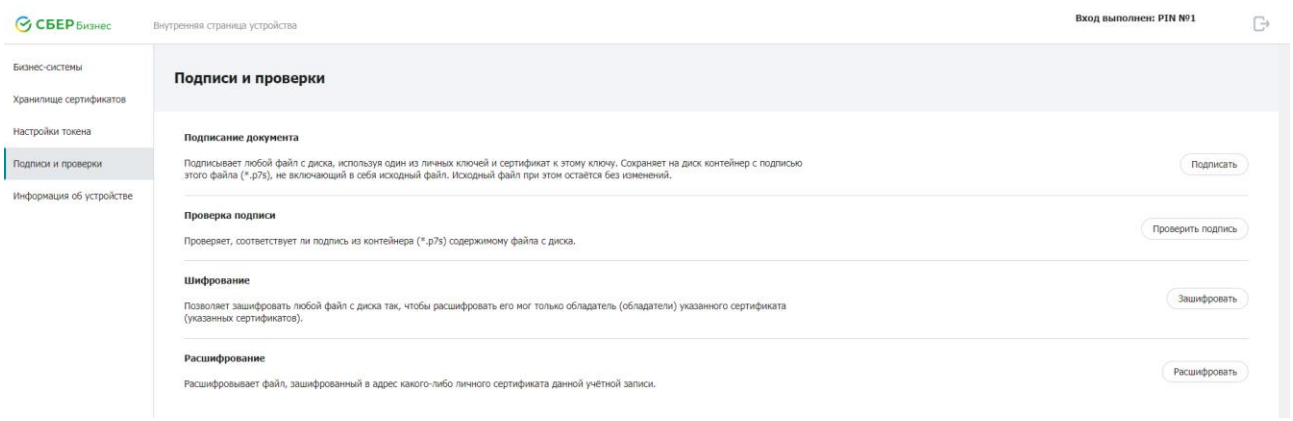


Рисунок 9 – Страница криптографических операций

На открывшейся странице подписания документов (см. Рисунок 10) будет отображена закрашенная жёлтым цветом область «Укажите файл для подписания» и список личных сертификатов, которые могут быть использованы для подписания файлов.

Для того чтобы подписать файл, необходимо выполнить следующие действия:

– Нажать кнопку **Выберите** и выбрать файл, который необходимо подписать. (Можно также с помощью мыши перетащить файл, который необходимо подписать, в область, закрашенную жёлтым цветом.)

– Установить флажок слева от сертификата, который будет использован при подписании файла.

– Нажать кнопку **Подписать** в правом нижнем углу страницы.

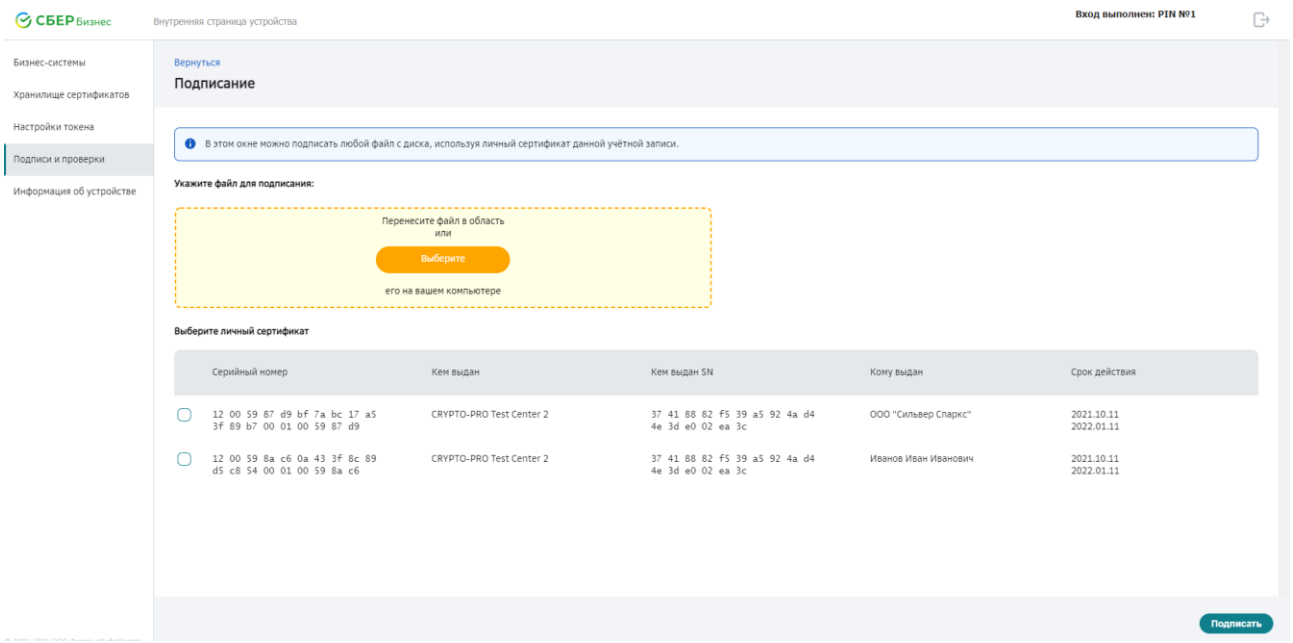


Рисунок 10 – Страница подписания документов

На экране появится сообщение об успешном завершении операции (см. Рисунок 11).

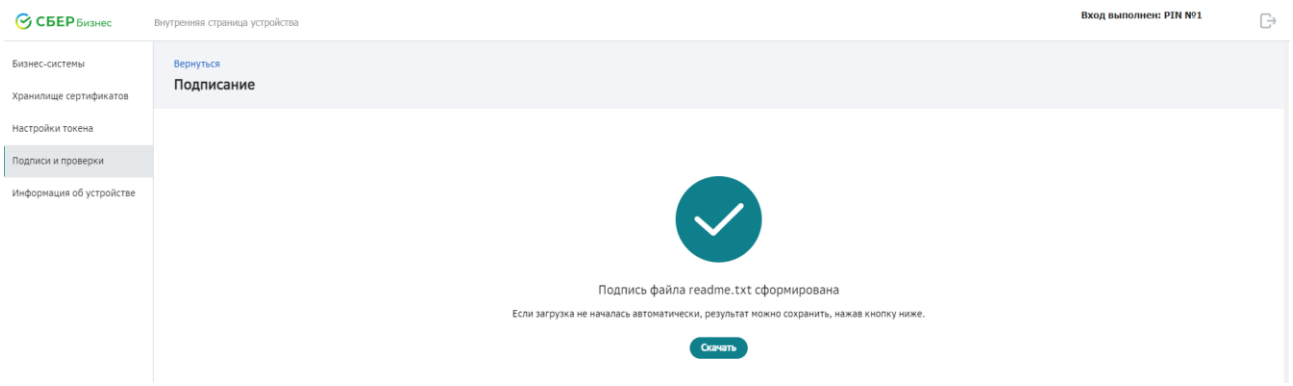


Рисунок 11 – Сохранение электронной подписи

Если в папке «Загрузки» не появился файл с именем подписанного файла и расширением .cms, электронную подпись файла можно сохранить принудительно, нажав кнопку **Скачать**.

4.6 Проверка электронной подписи файла

Для того чтобы проверить электронную подпись файла, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Подписи и проверки**.

На открывшейся странице (см. Рисунок 9) следует перейти по ссылке «Проверка подписи» в центральной части страницы или нажать кнопку **Проверить подпись** справа от неё.

На открывшейся странице проверки подписи (см. Рисунок 12) необходимо выполнить следующие действия:

- В закрашенной жёлтым цветом области «Укажите исходный файл на диске» нажать кнопку **Выберите** и выбрать файл, для которого требуется проверить подпись. (Можно также с помощью мыши перетащить файл в область «Укажите исходный файл на диске».)
- В закрашенной жёлтым цветом области «Укажите контейнер с подписью» нажать кнопку **Выберите** и выбрать файл, содержащий подпись. (Можно также с помощью мыши перетащить файл с подписью в область «Укажите контейнер с подписью».).
- Нажать кнопку **Проверить подпись** в правом нижнем углу страницы.

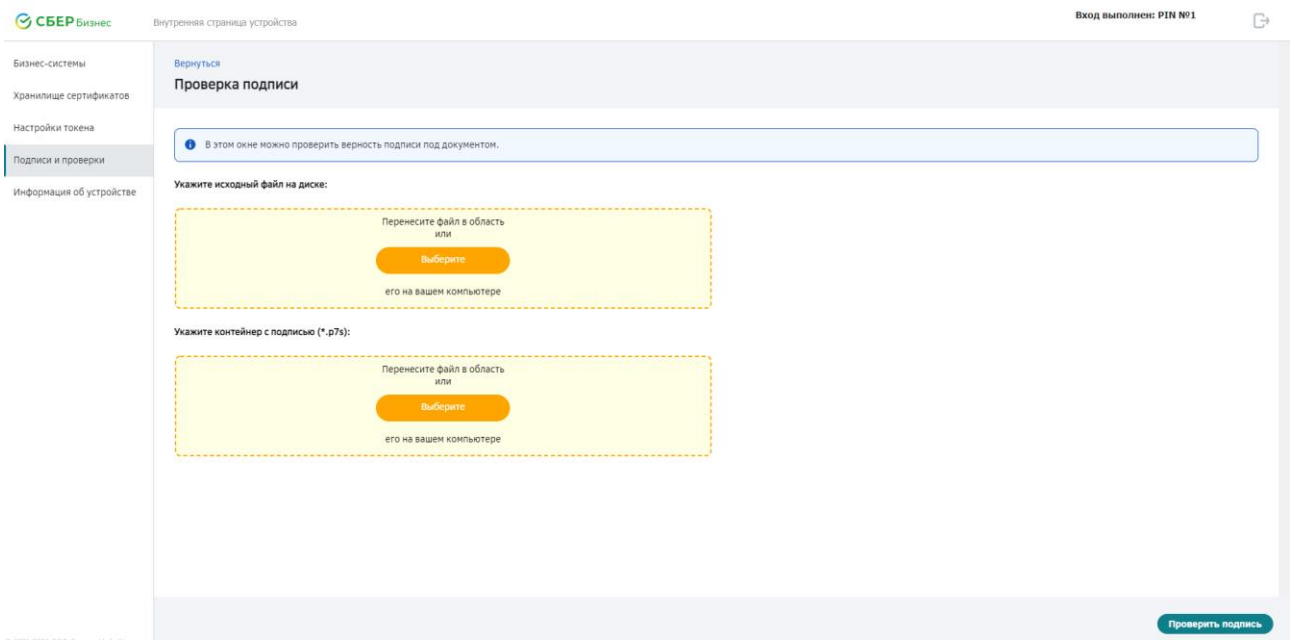


Рисунок 12 – Страница проверки подписи

На экране монитора появится сообщение о результате операции.

4.7 Шифрование

Для того чтобы зашифровать файл, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Подписи и проверки**.

На открывшейся странице (см. Рисунок 9) следует перейти по ссылке «Шифрование» в центральной части страницы или нажать кнопку **Зашифровать** справа от неё.

На открывшейся странице шифрования (см. Рисунок 13) необходимо выполнить следующие действия:

1. В закрашенной жёлтым цветом области «Выберите на диске файл для шифрования» нажать кнопку **Выберите** и выбрать файл, который требуется зашифровать. (Можно также с помощью мыши перетащить файл в область «Выберите на диске файл для шифрования».)
2. Если файл предназначен для другого адресата, указать сертификат, принадлежащий этому адресату. Для этого в закрашенной жёлтым цветом области «Выберите на диске файл личного сертификата ЭП адресата (не обязательно)» нажать кнопку **Выберите** и выбрать сертификат. (Можно также с помощью мыши перетащить сертификат в область «Выберите на диске файл личного сертификата ЭП адресата (не обязательно)».)

3. Если предполагается, что зашифрованный файл потребуется расшифровать для того же пользователя, который его зашифровал, необходимо установить флажок слева от сертификата, который будет использован при расшифровании файла.
4. Нажать кнопку **Зашифровать** в правом нижнем углу страницы.

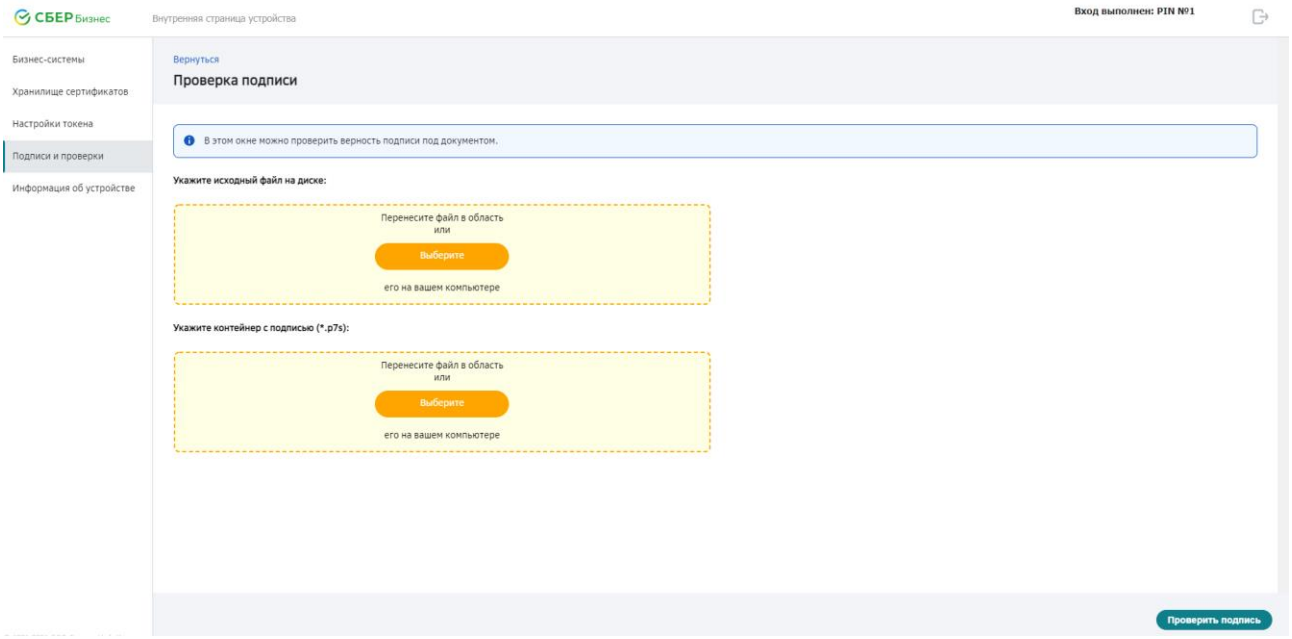


Рисунок 13 – Страница шифрования файла

На экране монитора появится сообщение об успешном завершении операции (см. Рисунок 14).

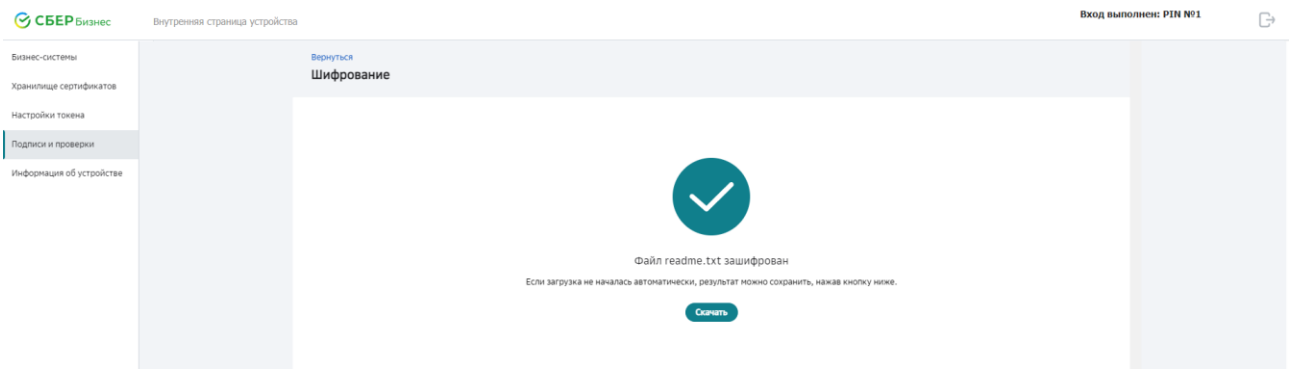


Рисунок 14 – Сохранение зашифрованного файла

Если в папке «Загрузки» не появился зашифрованный файл с именем исходного файла и расширением .p7e, его можно сохранить принудительно, нажав кнопку **Скачать**.

4.8 Расшифрование

Для того чтобы расшифровать файл, зашифрованный для данной учётной записи пользователя, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Подписи и проверки**.

На открывшейся странице (см. Рисунок 9) следует перейти по ссылке «Расшифрование» в центральной части страницы или нажать кнопку **Расшифровать** справа от неё.

На открывшейся странице расшифрования (см. Рисунок 15) необходимо выполнить следующие действия:

1. В закрашенной жёлтым цветом области «Выберите на диске файл для расшифрования» нажать кнопку **Выберите** и выбрать файл, который требуется расшифровать. (Можно также с помощью мыши перетащить файл в область «Выберите на диске файл для расшифрования».)
2. Нажать кнопку **Расшифровать** в правом нижнем углу страницы.

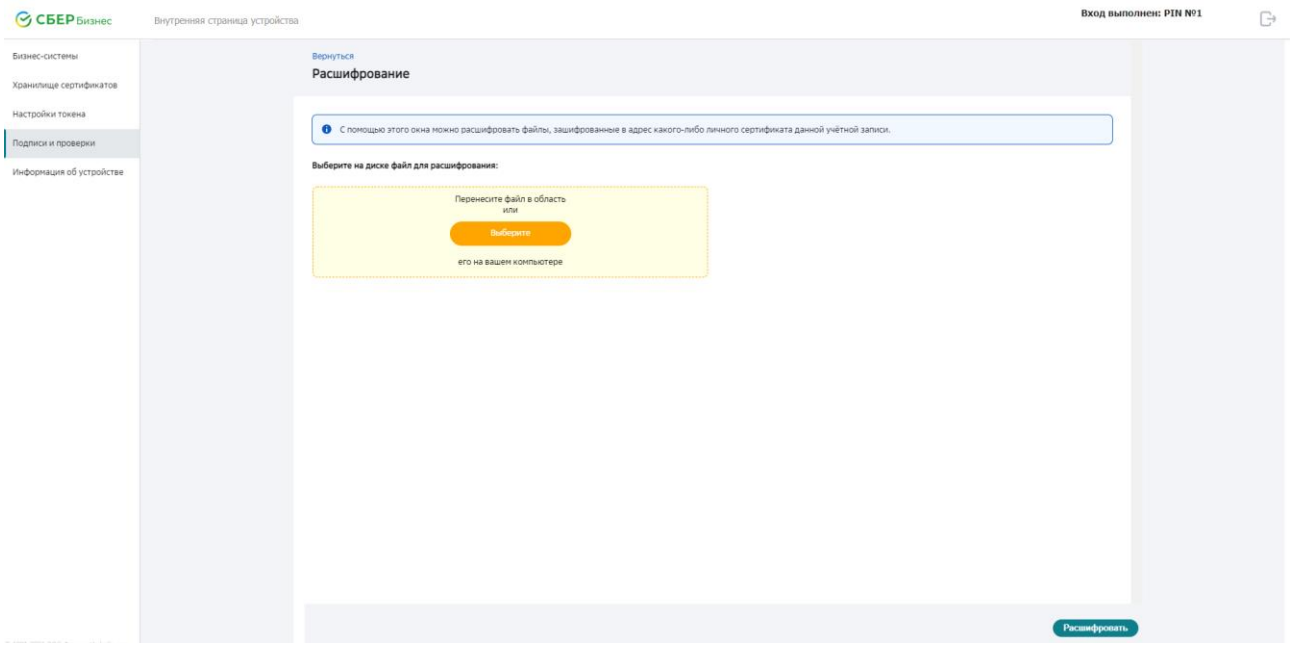


Рисунок 15 – Страница расшифрования файла

На экране монитора появится сообщение о результате операции.(см. Рисунок 16).

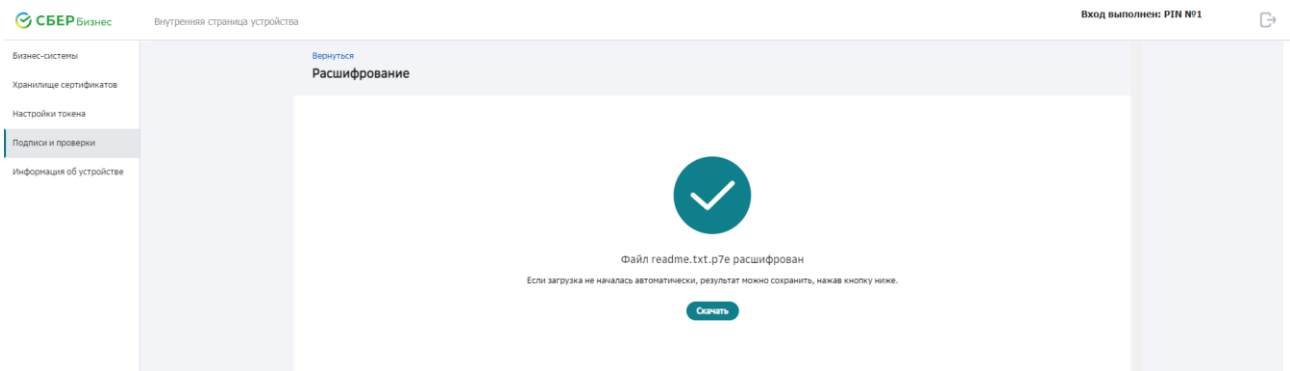


Рисунок 16 – Сохранение расшифрованного файла

Если в папке «Загрузки» не появился расшифрованный файл, его можно сохранить принудительно, нажав кнопку **Скачать**.

4.9 Просмотр сертификатов и запросов на сертификаты

Для того чтобы просмотреть список сертификатов и запросов на сертификаты, установленных в устройство «VPN-Key-TLS», следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Хранилище сертификатов**.

Чтобы просмотреть имеющиеся на устройстве сертификаты, общие для всех пользователей, следует в открывшейся странице просмотра хранилища сертификатов (см. Рисунок 17) нажать кнопку **Общие** в верхней части страницы. Если требуется просмотреть личные сертификаты пользователей, следует нажать кнопку **Персональные**.

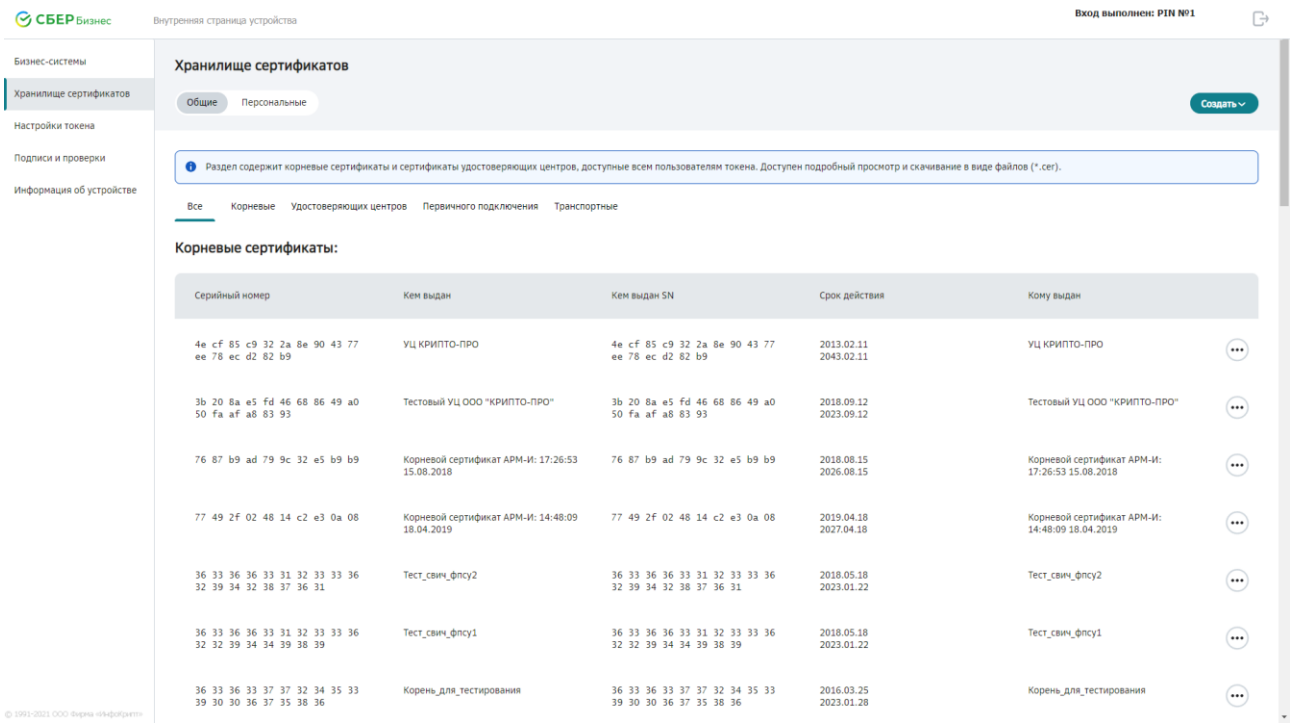


Рисунок 17 – Страница просмотра хранилища сертификатов

В результате появится страница со списком сертификатов того типа, который был выбран пользователем. Для каждого сертификата указывается его серийный номер, кем и кому был выдан данный сертификат и срок действия сертификата.

Список общих сертификатов разделён на следующие разделы:

- Корневые сертификаты (вкладка «Корневые»);
- Сертификаты УЦ (вкладка «Удостоверяющих центров»);
- Сертификаты первичного подключения TLS (вкладка «Первичного подключения»);
- Транспортные сертификаты.

Список личных сертификатов и запросов на сертификаты (см. Рисунок 18) разделён на следующие разделы:

– Сертификаты и запросы на сертификаты ЭП и (или) шифрования (вкладка «ЭП»);
– Сертификаты и запросы на сертификаты TLS (вкладка «TLS»).

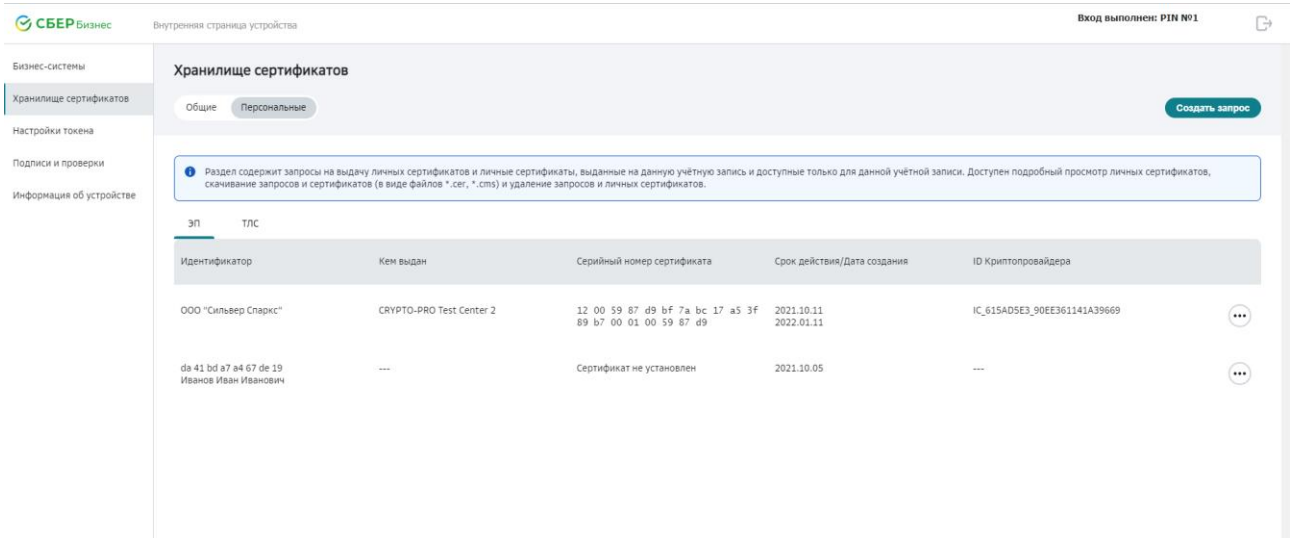


Рисунок 18 – Список личных сертификатов и запросов на сертификаты

Для просмотра детальной информации по сертификату следует выбрать его в списке.

На открывшейся странице (см. Рисунок 19) будет отображена подробная информация по выбранному сертификату:

– серийный номер сертификата;
– криптографический алгоритм подписи сертификата;
– срок действия сертификата;
– данные о поставщике сертификата;
– данные о субъекте, которому выдан сертификат;
– открытый ключ субъекта.

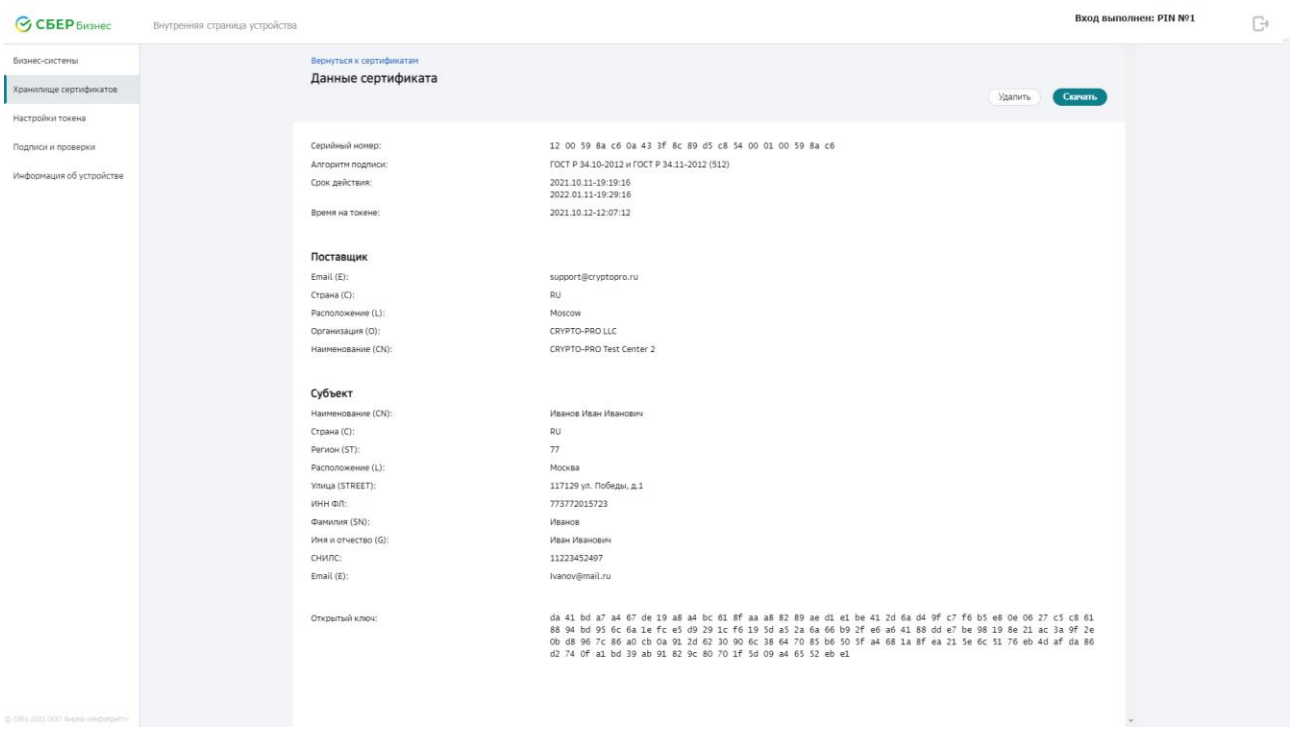


Рисунок 19 – Подробная информация по сертификату

4.10 Сохранение сертификатов и запросов на сертификаты

Для того чтобы записать сертификат в файл, следует нажать кнопку **Скачать** на странице подробной информации по сертификату (см. Рисунок 19).

Аналогично, для того чтобы записать запрос на сертификат в файл формата cms, следует в списке личных сертификатов и запросов на сертификаты (см. Рисунок 18) щёлкнуть значок , расположенный в строке соответствующего сертификата или запроса на сертификат, и в открывшемся меню выбрать пункт **Сохранить запрос**.

4.11 Удаление ключевой пары

Для того чтобы удалить ключевую пару, следует в списке личных сертификатов и запросов на сертификаты (см. Рисунок 18) щёлкнуть значок , расположенный в строке соответствующего сертификата. В открывшемся меню следует выбрать пункт **Удалить ключевую пару**.

Следует иметь в виду, что при удалении ключевой пары сертификат и соответствующий запрос на сертификат также будут удалены. Восстановление секретного ключа и дальнейшее использование сертификата будет невозможно.

На открывшейся странице с предупреждением о последствиях удаления (см. Рисунок 20) следует нажать кнопку **Удалить** для подтверждения удаления или кнопку **Отказаться** для отказа от удаления.

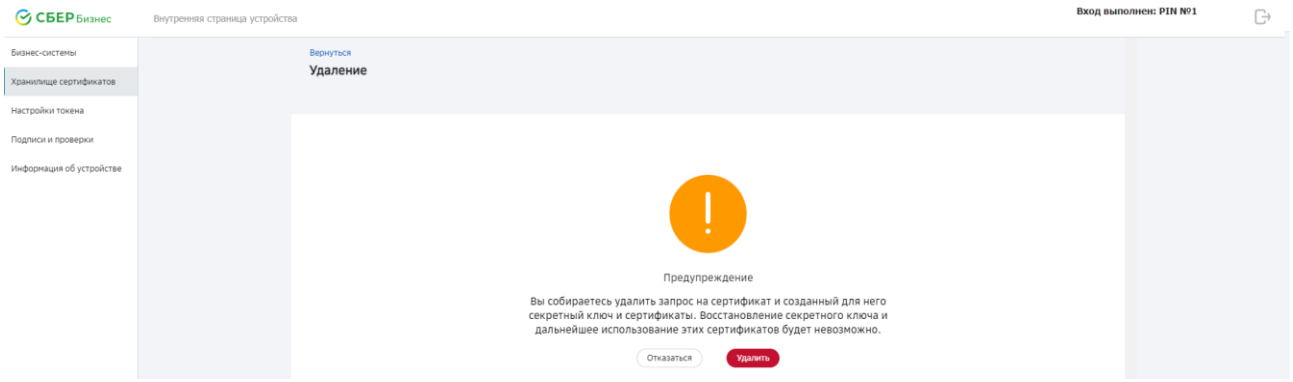


Рисунок 20 – Предупреждение о последствиях удаления ключевой пары

Если для ключевой пары ещё не получен сертификат, то щёлкнув значок , расположенный в строке запроса на сертификат и выбрав пункт **Удалить ключевую пару**, можно удалить запрос на сертификат и соответствующую ключевую пару.

4.12 Удаление личного сертификата

Для того чтобы удалить личный сертификат, следует нажать кнопку **Удалить** на странице подробной информации по сертификату (см. Рисунок 19).

Следует иметь в виду, что дальнейшее использование сертификата будет невозможно.

На открывшейся странице с предупреждением о последствиях удаления (см. Рисунок 21) следует нажать кнопку **Удалить** для подтверждения удаления или кнопку **Отказаться** для отказа от удаления.

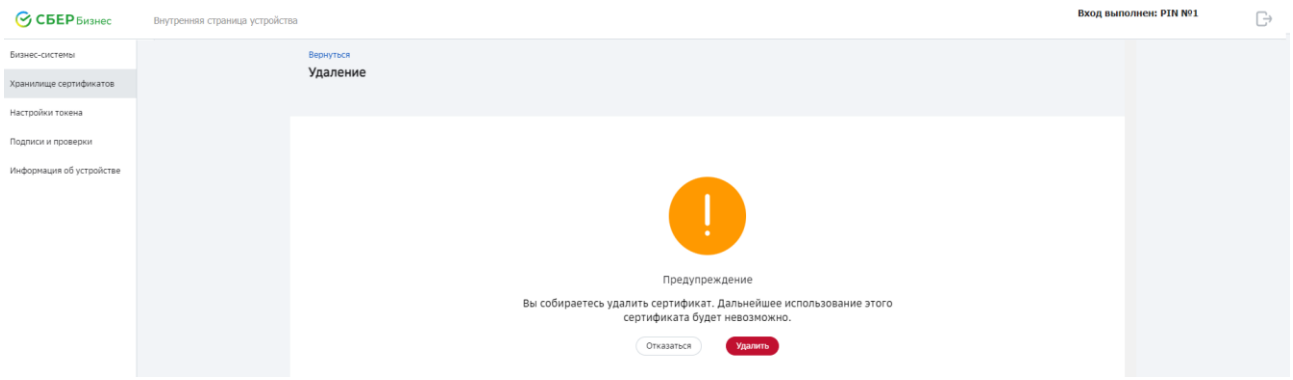


Рисунок 21 – Предупреждение о последствиях удаления сертификата

На экране появится сообщение о результате операции.

4.13 Изменение PIN-кода

Смену PIN-кода следует выполнять каждые 6 месяцев. Для того чтобы изменить PIN-код своей учётной записи, следует на внутренней странице (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует нажать кнопку **Изменить** в правой части страницы или перейти по ссылке «Изменение PIN-кода» в центральной части страницы.

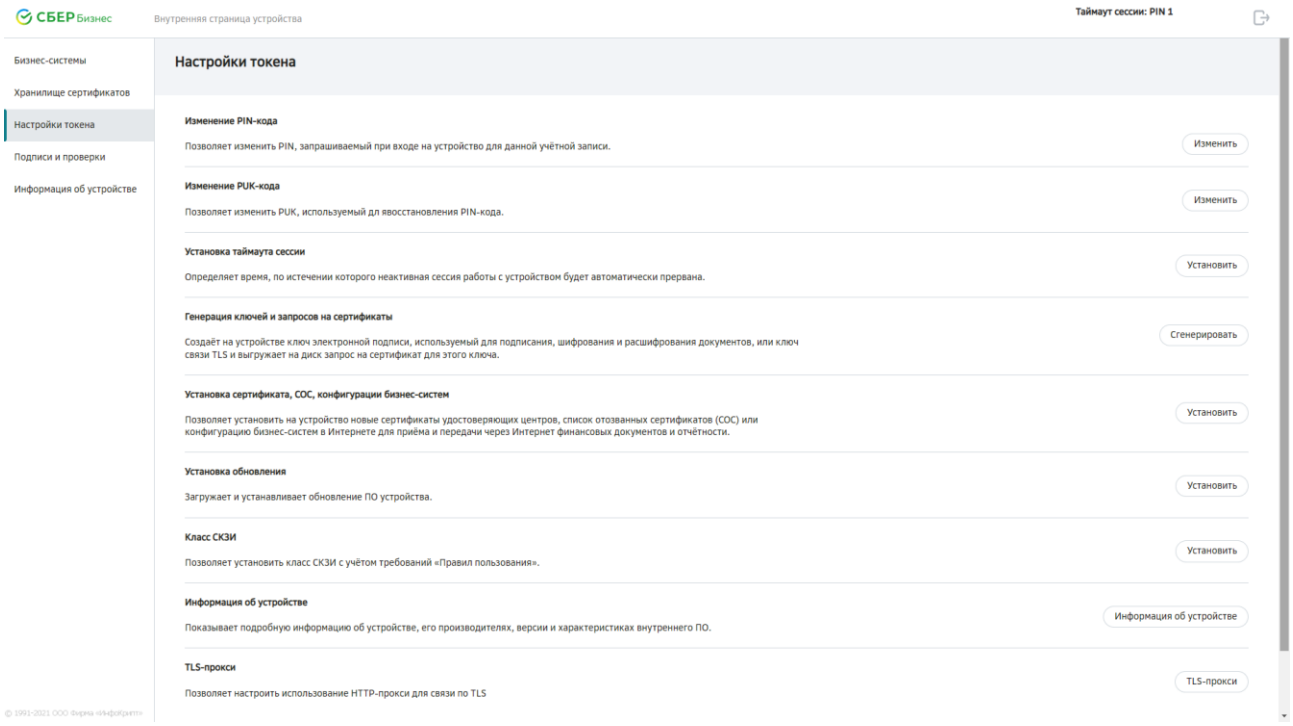


Рисунок 22 – Страница настройки устройства

На открывшейся странице изменения PIN-кода (см. Рисунок 23) необходимо выполнить следующие действия:

- Ввести действующий PIN-код в поле «Текущий PIN». Если PIN-код введен неверно 3 раза подряд, соответствующая учётная запись блокируется.
- Ввести новый PIN-код в поле «Новый PIN». Длина PIN-кода должна быть равна 6 символам. Допустимыми символами являются английские буквы, цифры и спецсимволы.
- Повторно ввести новый PIN-код в поле «Повторите новый PIN».
- Подтвердить изменение PIN-кода, нажав кнопку **Изменить PIN** в правом нижнем углу страницы.

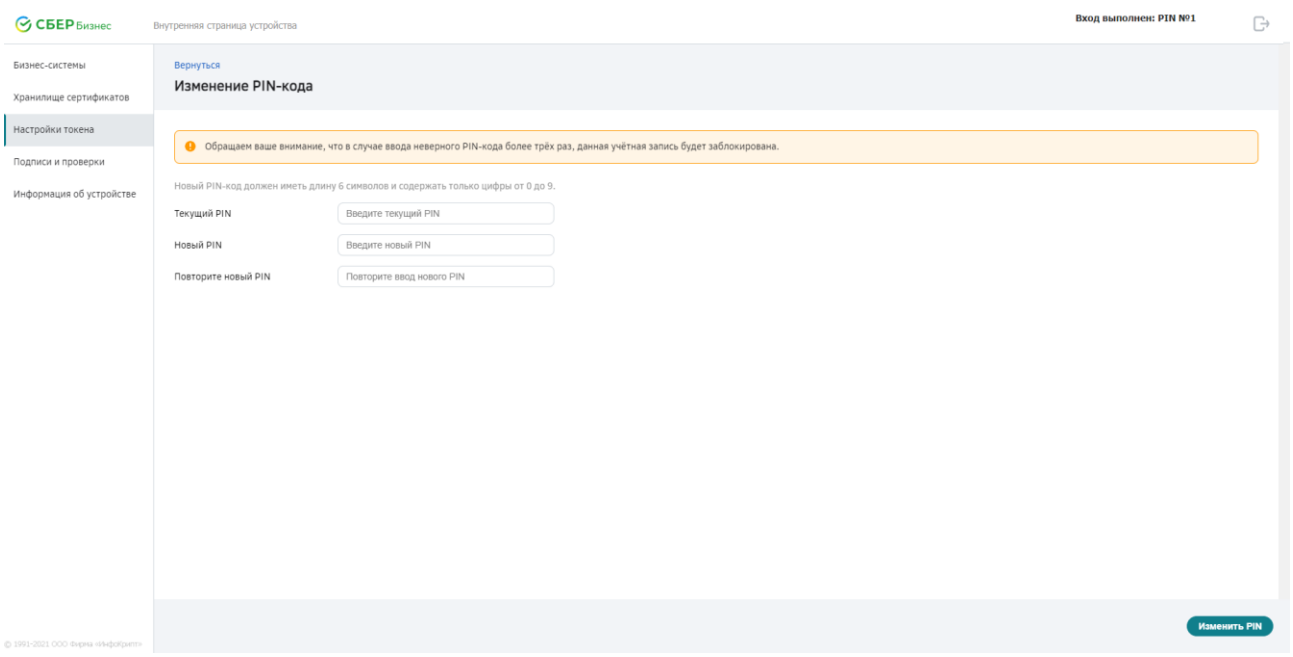


Рисунок 23 – Страница изменения PIN-кода

В результате этих действий PIN-код будет изменён и откроется страница с сообщением об успешном изменении PIN-кода.

Если новый PIN-код введен неверно, откроется страница с сообщением об ошибке.

4.14 Изменение PUK-кода

Смену PUK-кода следует выполнять каждые 6 месяцев. Для того чтобы изменить PUK-код своей учётной записи, следует на внутренней странице (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует нажать кнопку **Изменить** в правой части страницы или перейти по ссылке «Изменение PUK-кода» в центральной части страницы.

На открывшейся странице изменения PUK-кода (см. Рисунок 24) необходимо выполнить следующие действия:

Ввести действующий PUK-код в поле «Текущий PUK». В случае трёх и более попыток ввода неверного PUK-кода подряд начинается период принудительной задержки, зависящий от количества предыдущих попыток ввода неверного PUK-кода подряд (Таблица 1). Введённый течение этого периода PUK-код будет принят к рассмотрению только после его окончания. Если количество принятых к рассмотрению попыток ввода неверного PUK-кода подряд достигнет 10, данная учётная запись будет заблокирована окончательно, и её дальнейшее восстановление будет невозможно.

– Ввести новый PUK-код в поле «Новый PUK». Длина PUK-кода должна быть равна 12 символам. Допустимыми символами являются английские буквы, цифры и спецсимволы.
– Повторно ввести новый PUK-код в поле «Повторите новый PUK».
– Подтвердить изменение PUK-кода, нажав кнопку **Изменить PUK** в правом нижнем углу страницы.

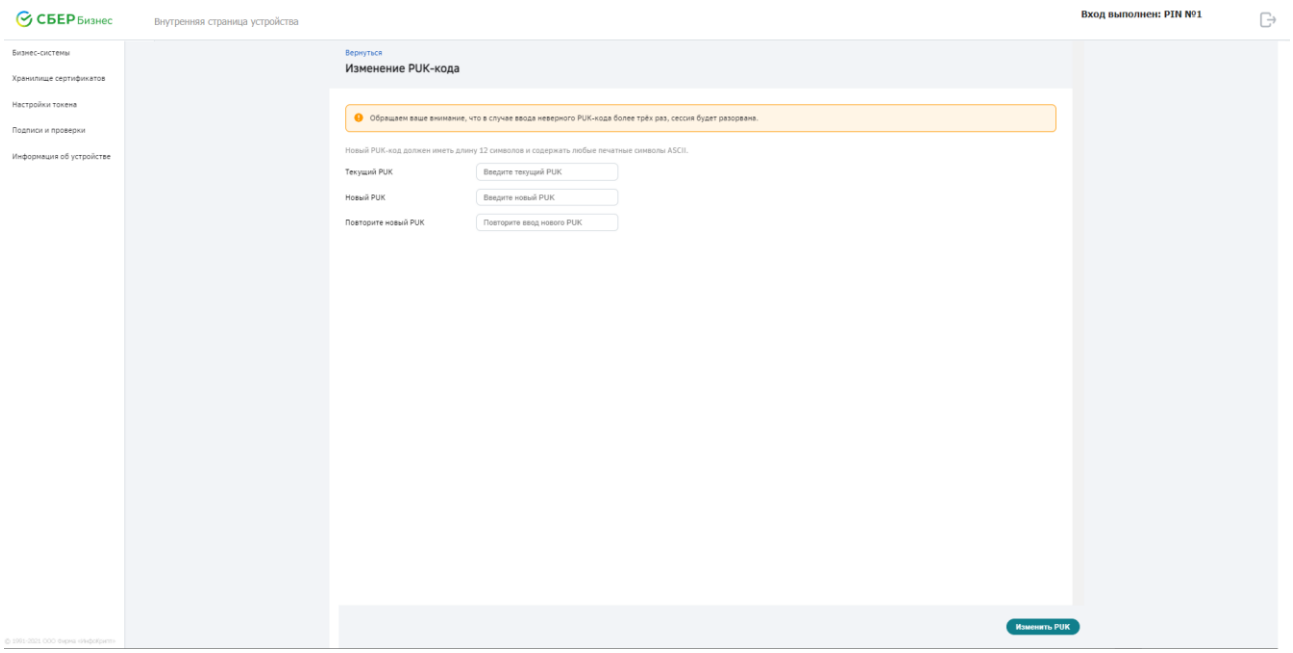


Рисунок 24 – Страница изменения PUK-кода

В результате этих действий PUK-код будет изменён и откроется страница с сообщением об успешном изменении PUK-кода.

Если новый PUK-код введен неверно, откроется страница с сообщением об ошибке.

4.15 Изменение значения таймаута

Таймаут представляет собой время простоя в работе с устройством «VPN-Key-TLS», по истечении которого соединение будет автоматически завершено, и для дальнейшей работы пользователю будет необходимо повторить процедуру авторизации (см. раздел 4.1).

Для того чтобы изменить значение таймаута, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует перейти по ссылке «Установка таймаута сессии» в центральной части страницы или нажать кнопку **Установить** справа от неё.

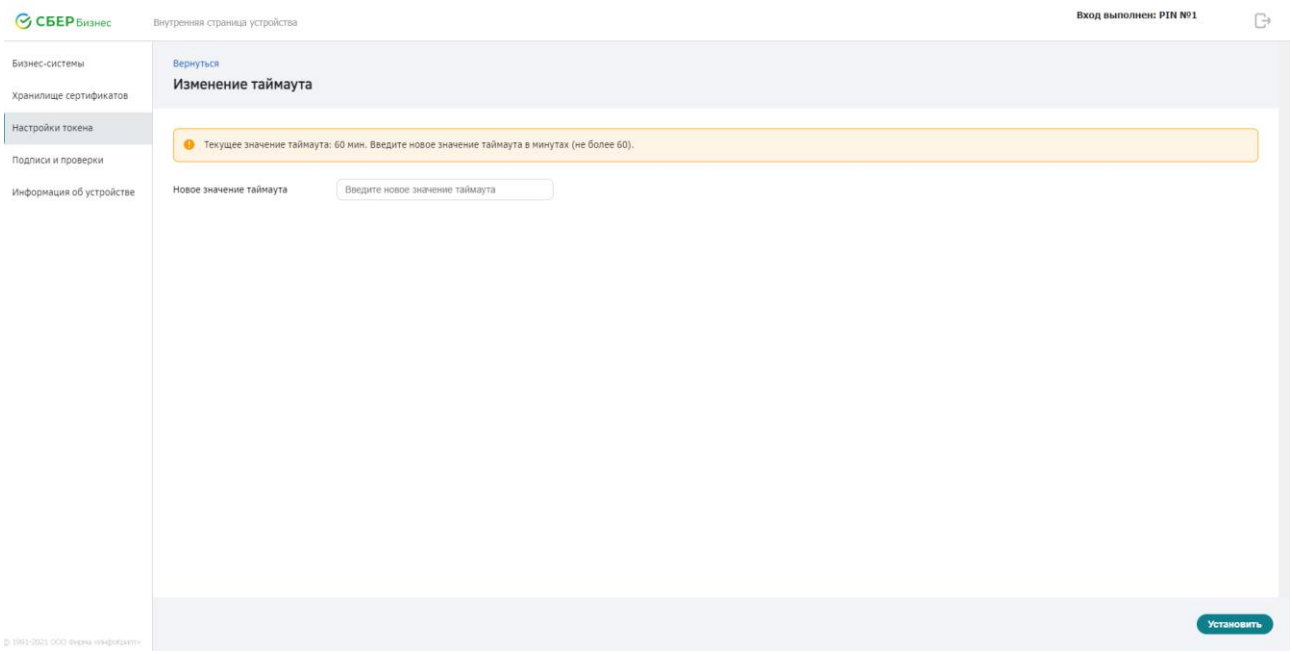


Рисунок 25 – Страница изменения значения таймаута

На открывшейся странице изменения значения таймаута (см. Рисунок 25) необходимо выполнить следующие действия:

- Ввести новое значение таймаута в минутах в поле «Новое значение таймаута». Значение таймаута может быть установлено в пределах от 1 до 60 минут.
- Подтвердить изменение значения таймаута, нажав кнопку **Установить** в правом нижнем углу страницы.

В результате этих действий значение таймаута будет изменено, и откроется страница с сообщением об успешном завершении операции.

4.16 Генерация ключей и запросов на сертификаты

СКЗИ «VPN-Key-TLS» позволяет создавать ключи электронной подписи и ключи TLS, а также запросы на сертификаты для них. На устройстве может находиться одновременно не более 16 запросов на сертификаты для ключей электронной подписи и не более 16 запросов на сертификаты для ключей TLS.

Для создания ключей электронной подписи следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) перейти по ссылке «Генерация ключей и запросов на сертификаты» в центральной части страницы или нажать кнопку **Сгенерировать** справа от неё.

Можно также выбрать пункт меню **Хранилище сертификатов**, нажать кнопку **Персональные** (см. Рисунок 17) и затем нажать кнопку **Создать**.

На открывшейся странице генерации ключей электронной подписи и запросов на сертификаты (см. Рисунок 26) следует выбрать тип владельца сертификата: юридическое лицо, уполномоченное лицо юридического лица, физическое лицо или индивидуальный предприниматель.

Далее необходимо ввести в соответствующие поля данные организации и (или) данные пользователя, выбрать тип запрашиваемого сертификата (ЭП, шифрования или TLS) и алгоритм электронной подписи.

Затем следует подтвердить данные, нажав кнопку **Сгенерировать** в правом нижнем углу страницы.

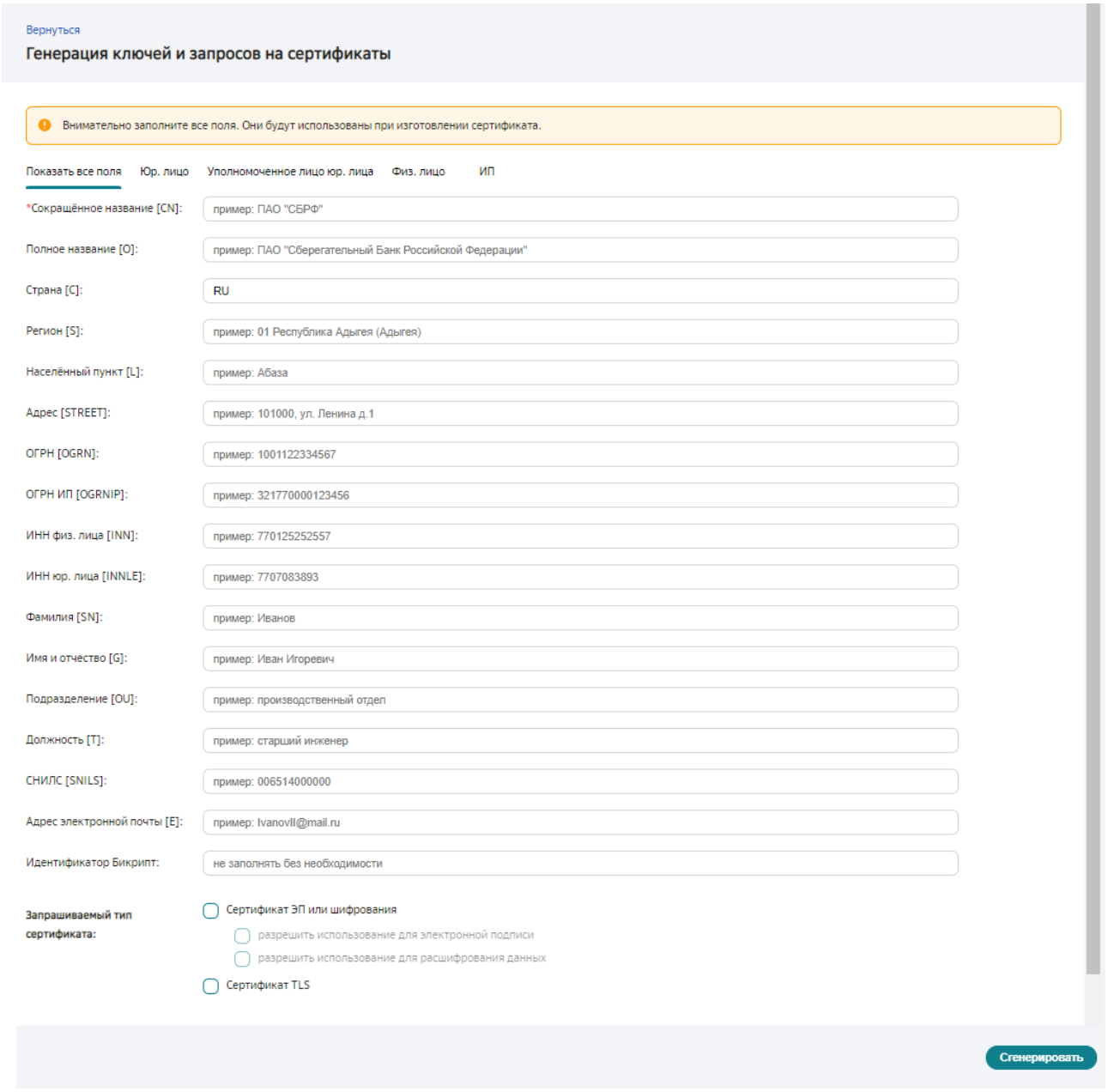


Рисунок 26 – Генерация ключей и запросов на сертификаты

Если на устройстве уже имеется 16 запросов на сертификаты выбранного типа (ЭП или TLS), на экране монитора появится сообщение о невозможности создания нового запроса на сертификат. Необходимо предварительно удалить один из уже имеющихся запросов на сертификаты (см. раздел 4.11).

В результате этих действий будут созданы ключи и соответствующий запрос на сертификат, который будет помещён в виде файла с расширением .cms в папку «Загрузки», и откроется страница с сообщением об успешном завершении операции (см. Рисунок 27).

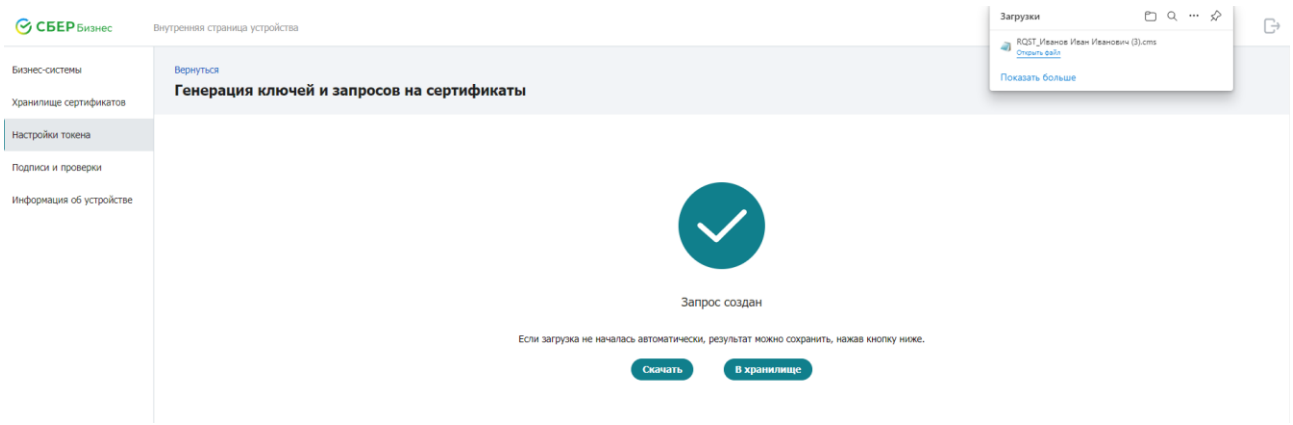


Рисунок 27 – Сохранение запроса на сертификат ЭП в виде файла

Если в папке «Загрузки» не появился файл с расширением .cms, запрос на сертификат можно сохранить принудительно, нажав кнопку **Скачать**. Этот файл следует передать в удостоверяющий центр.

Для работы с запросами на сертификаты можно перейти на соответствующую страницу, нажав кнопку **В хранилище**.

4.17 Создание нового транспортного сертификата

Для создания нового транспортного сертификата следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Хранилище сертификатов**.

В открывшейся странице просмотра хранилища сертификатов (см. Рисунок 17) следует нажать кнопку **Создать** в правом верхнем углу страницы и в открывшемся меню выбрать пункт **Новый транспортный сертификат**.

Следует иметь в виду, что в случае создания нового транспортного сертификата станет невозможной установка сертификатов для выгруженных ранее запросов.

На открывшейся странице с предупреждением о последствиях создания нового транспортного сертификата (см. Рисунок 28) следует нажать кнопку **Сгенерировать** для подтверждения создания нового транспортного сертификата или кнопку **Отказаться** для отказа.

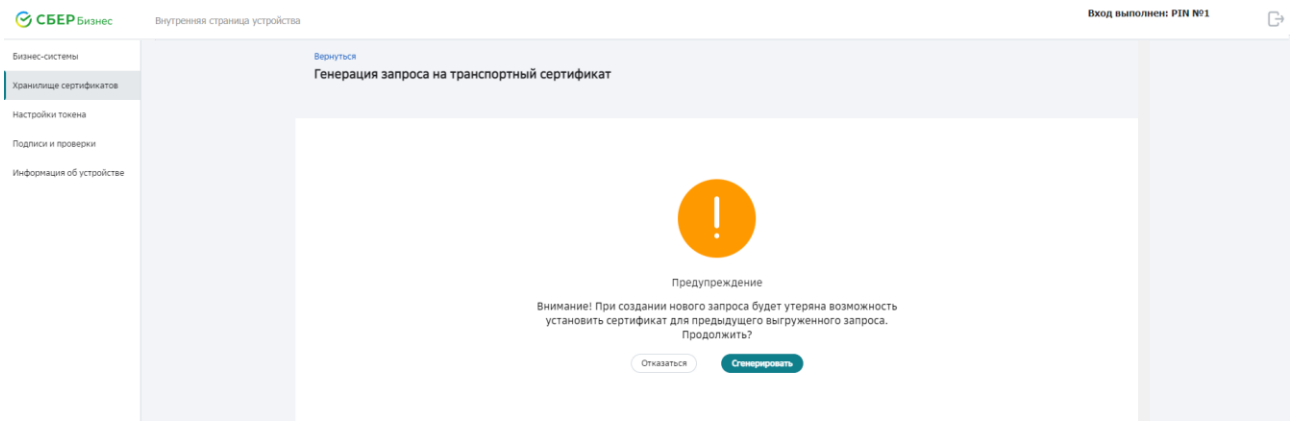


Рисунок 28 – Предупреждение о последствиях создания нового транспортного сертификата

4.18 Создание нового сертификата первичного подключения

Для создания нового сертификата первичного подключения следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Хранилище сертификатов**.

В открывшейся странице просмотра хранилища сертификатов (см. Рисунок 17) следует нажать кнопку **Создать** в правом верхнем углу страницы и в открывшемся меню выбрать пункт **Новый сертификат первичного подключения TLS**.

Следует иметь в виду, что в случае создания нового транспортного сертификата станет невозможной установка сертификатов для выгруженных ранее запросов.

На открывшейся странице с предупреждением о последствиях создания нового транспортного сертификата (см. Рисунок 29) следует нажать кнопку **Сгенерировать** для подтверждения создания нового транспортного сертификата или кнопку **Отказаться** для отказа.

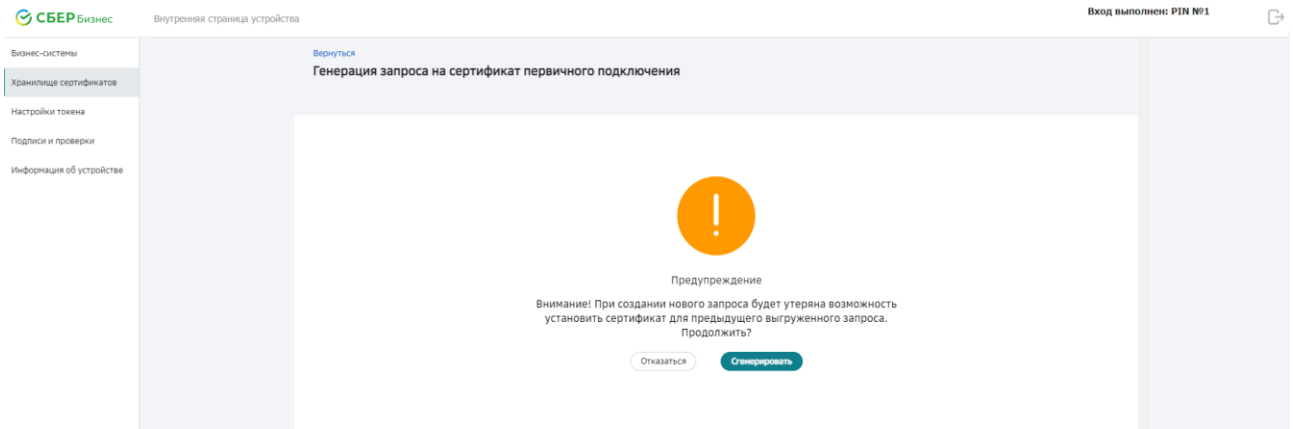


Рисунок 29 – Предупреждение о последствиях создания нового сертификата первичного подключения TLS

4.19 Установка сертификата

СКЗИ «VPN-Key-TLS» позволяет установить сертификаты, выданные удостоверяющим центром по ранее созданным данным устройством запросам на сертификаты, а также новые сертификаты удостоверяющих центров.

Для установки сертификата следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует перейти по ссылке «Установка сертификата, СОС, конфигурации бизнес-систем» в центральной части страницы или нажать кнопку **Установить** справа от неё.

На открывшейся странице установки сертификатов, СОС, конфигурации бизнес-систем (см. Рисунок 30) следует выполнить следующие действия:

– Нажать кнопку **Выберите** и выбрать файл с сертификатом, который необходимо установить. (Можно также с помощью мыши перетащить файл с сертификатом, который необходимо установить, в область, закрашенную жёлтым цветом.)

– Подтвердить выбор, нажав кнопку **Установить** в правом нижнем углу страницы.

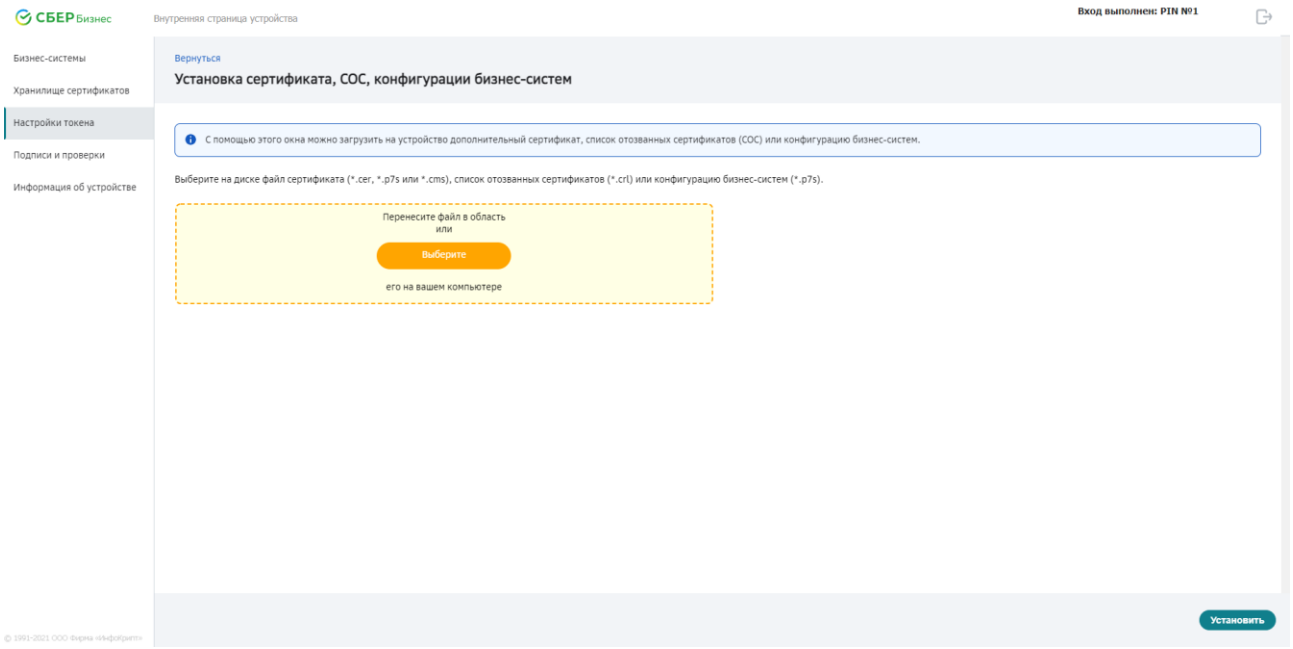


Рисунок 30 – Установка сертификата, СОС, конфигурации бизнес-систем

В результате этих действий выбранный сертификат будет установлен и может быть в дальнейшем использован при выработке электронной подписи или организации защищённого TLS-соединения в зависимости от ограничений, установленных удостоверяющим центром.

4.20 Установка конфигурации бизнес-систем

СКЗИ «VPN-Key-TLS» позволяет установить новый список бизнес-систем, которые будут доступны пользователю.

Для установки конфигурации бизнес-систем следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует перейти по ссылке «Установка сертификата, СОС, конфигурации бизнес-систем» в центральной части страницы или нажать кнопку **Установить** справа от неё.

На открывшейся странице установки сертификатов, СОС, конфигурации бизнес-систем (см. Рисунок 30) необходимо выполнить следующие действия:

- Нажать кнопку **Выберите** и выбрать файл с конфигурацией бизнес-систем, которую необходимо установить. (Можно также с помощью мыши перетащить файл с конфигурацией бизнес-систем, которую необходимо установить, в область, закрашенную жёлтым цветом.)
- Подтвердить выбор, нажав кнопку **Установить** в правом нижнем углу страницы.

В результате этих действий выбранная конфигурация бизнес-систем будет установлена и при следующем подключении к устройству «VPN-Key-TLS» в центральной части внутренней страницы устройства (см. Рисунок 4) будет отображен новый список бизнес-систем.

4.21 Установка списка отозванных сертификатов

СКЗИ «VPN-Key-TLS» позволяет установить выданный удостоверяющим центром список отозванных сертификатов.

Для установки списка отозванных сертификатов следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует перейти по ссылке «Установка сертификата, СОС, конфигурации бизнес-систем» в центральной части страницы или нажать кнопку **Установить** справа от неё.

На открывшейся странице установки сертификатов, СОС, конфигурации бизнес-систем (см. Рисунок 30) необходимо выполнить следующие действия:

- Нажать кнопку **Выберите**;
- Выбрать файл с расширением .crl, который необходимо установить;
- Подтвердить выбор, нажав кнопку **Установить** в правом нижнем углу страницы.

Можно также с помощью мыши перетащить файл с расширением .crl, который необходимо установить, в область, закрашенную жёлтым цветом.

В результате этих действий выбранный список отозванных сертификатов будет установлен и в дальнейшем использован при выработке электронной подписи или организации защищённого TLS-соединения.

4.22 Установка обновления программного обеспечения

Встроенное программное обеспечение устройства «VPN-Key-TLS» может быть обновлено. Для этого необходимо получить файл с обновлением ПО.

Для установки обновления ПО следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице настройки устройства (см. Рисунок 22) следует перейти по ссылке «Установка обновления» в центральной части страницы или нажать кнопку **Установить** справа от неё.

На открывшейся странице установки обновления (см. Рисунок 31) необходимо выполнить следующие действия:

- Нажать кнопку **Выберите** и выбрать файл с обновлением (*.fw), который необходимо установить. (Можно также с помощью мыши перетащить файл с расширением .fw, который необходимо установить, в область, закрашенную жёлтым цветом.)
- Подтвердить выбор, нажав кнопку **Установить** в правом нижнем углу страницы.

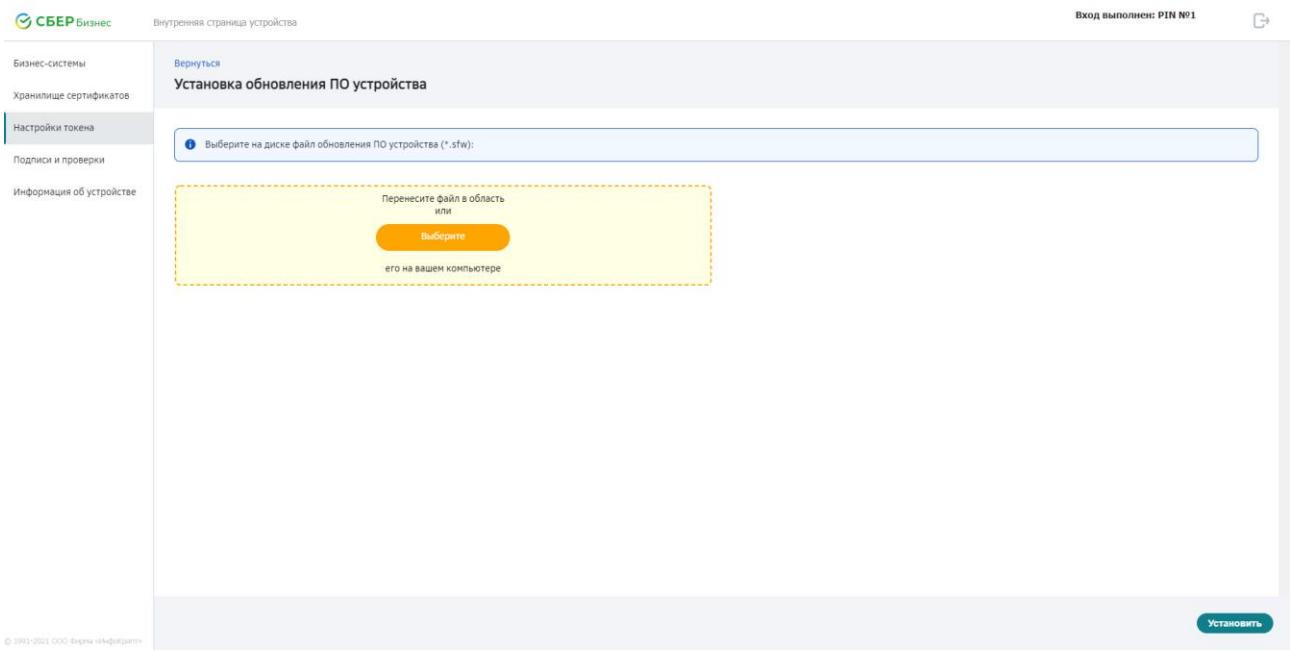


Рисунок 31 – Установка обновления

В результате этих действий выбранный файл копируется в устройство и проверяется на подлинность. В процессе обновления ПО на устройстве горят зелёный и красный светодиоды. Необходимо дождаться окончания процесса копирования файла с обновлением (см. Рисунок 32).

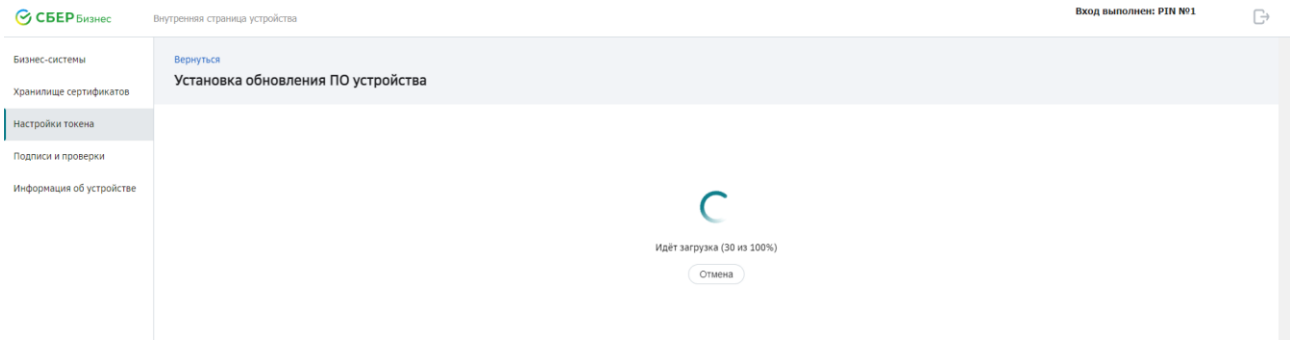


Рисунок 32 – Процесс копирования обновления

В случае успешного прохождения проверок обновление встроенного программного обеспечения будет установлено. По окончании процесса обновления светодиоды на устройстве погаснут, на странице установки обновления появится сообщение о том, что обновление установлено (см. Рисунок 33). Устройство «VPN-Key-TLS» становится недоступным.

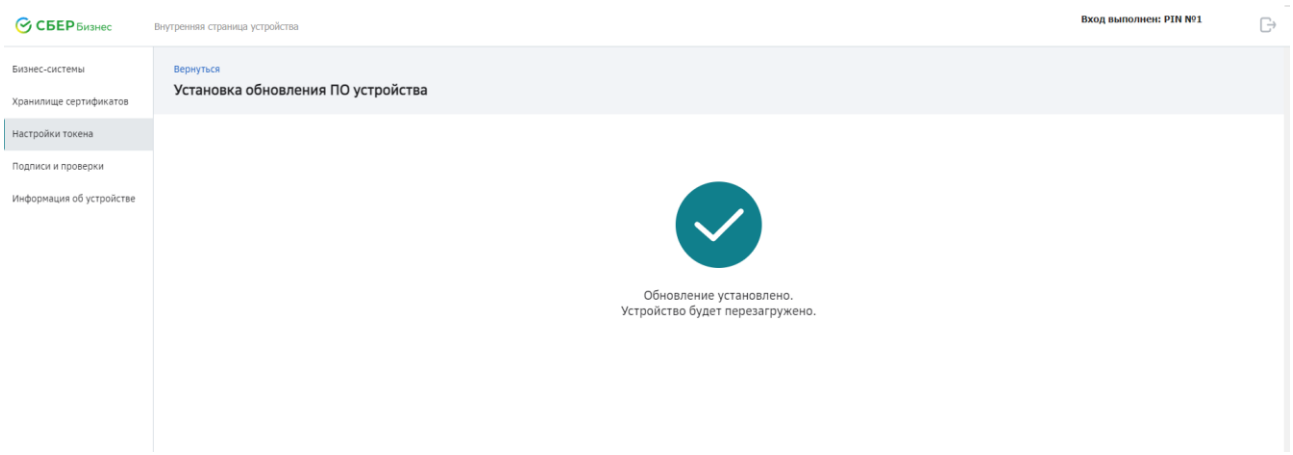


Рисунок 33 – Сообщение о процессе обновления ПО

Для продолжения работы с устройством необходимо повторить процедуру его подключения (см. раздел 3.2).

Если получен отрицательный результат проверки ЭП обновления ПО, появится сообщение об ошибке. В этом случае необходимо обратиться в службу поддержки для получения корректного обновления ПО.

Если в процессе обновления ПО произошёл сбой, на устройстве будет гореть красный светодиод. В этом случае также необходимо обратиться в службу поддержки.

4.23 Проверка целостности встроенного программного обеспечения

СКЗИ «VPN-Key-TLS» позволяет убедиться в том, что встроенное программное обеспечение не подверглось несанкционированному изменению.

Для установки обновления ПО следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Информация об устройстве** или на странице настройки устройства (см. Рисунок 22) перейти по ссылке «Информация об устройстве» в центральной части страницы или нажать кнопку **Информация об устройстве** справа от неё.

Затем на открывшейся странице информации об устройстве (см. Рисунок 34) следует перейти по ссылке «Рассчитать» в строке «Рассчитанная контрольная сумма встроенного ПО» или в строке «Рассчитанная контрольная сумма «Start.exe».

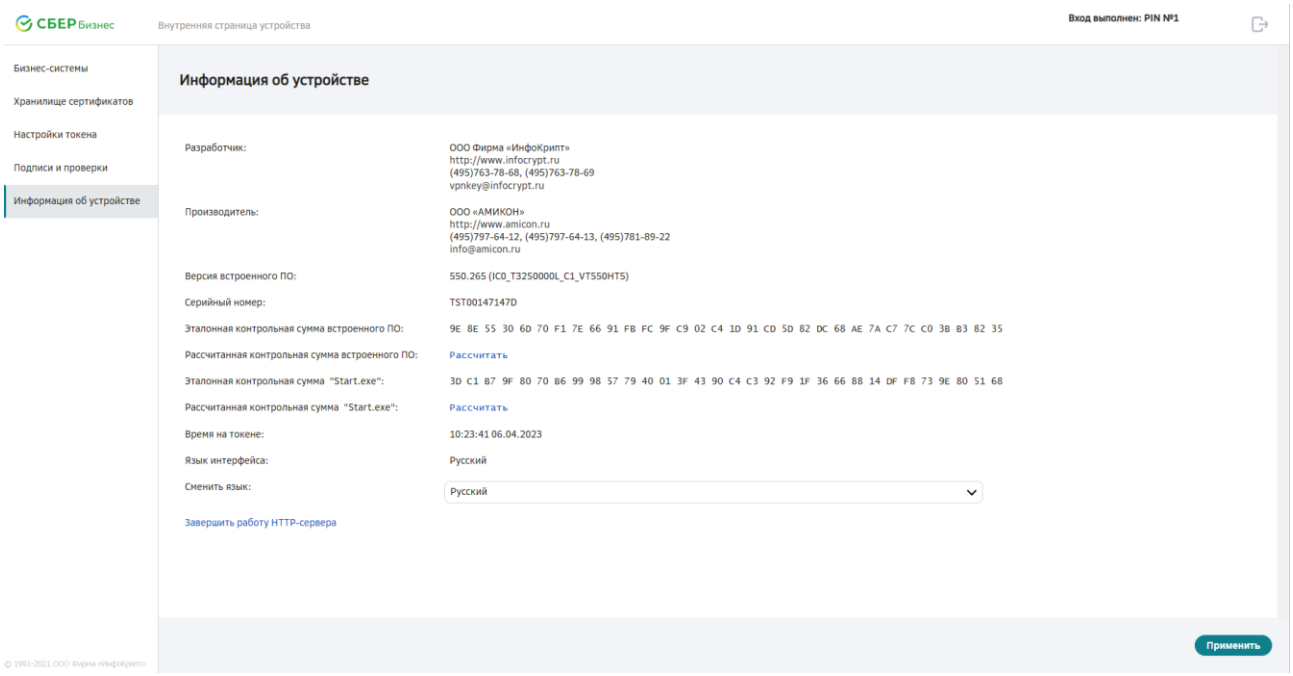


Рисунок 34 – Информация об устройстве

В результате в строке таблицы «Рассчитанная контрольная сумма встроенного ПО» появится значение контрольной суммы встроенного программного обеспечения, а в строке «Рассчитанная контрольная сумма «Start.exe» появится значение контрольной суммы приложения Start.exe, рассчитанные в данный момент времени (см. Рисунок 35).

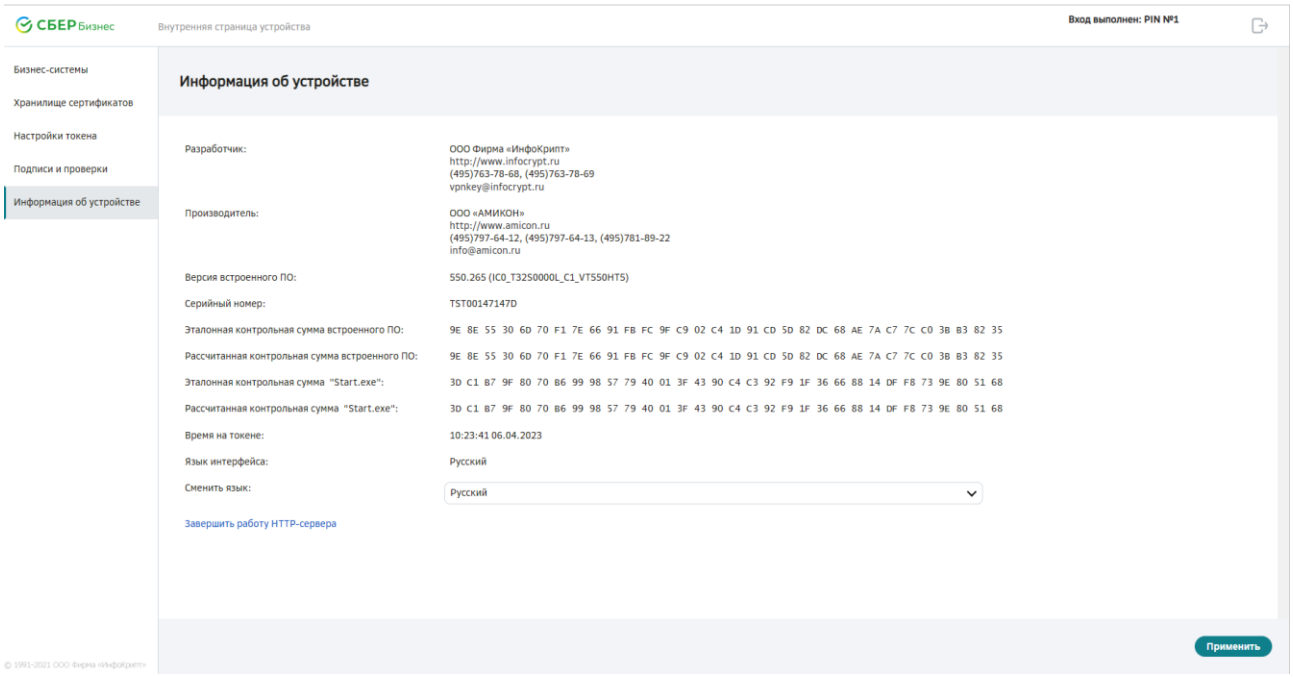


Рисунок 35 – Рассчитанные контрольные суммы

Если значение в строке «Рассчитанная контрольная сумма встроенного ПО» совпадает со значением в строке «Эталонная контрольная сумма встроенного ПО», то встроенное программное обеспечение не подвергалось несанкционированному изменению. Аналогично, если значение в строке «Рассчитанная контрольная сумма «Start.exe» совпадает со значением в строке «Эталонная контрольная сумма «Start.exe», то приложение Start.exe не подвергалось несанкционированному изменению.

4.24 Установка класса СКЗИ

Для того чтобы установить класс СКЗИ, следует на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице (см. Рисунок 22) следует перейти по ссылке «Класс СКЗИ» в центральной части страницы или нажать кнопку **Установить** справа от неё.

На открывшейся странице установки класса СКЗИ (см. Рисунок 36) необходимо выполнить следующие действия:

– Выбрать класс СКЗИ.

– Нажать кнопку **Установить** в правом нижнем углу страницы.

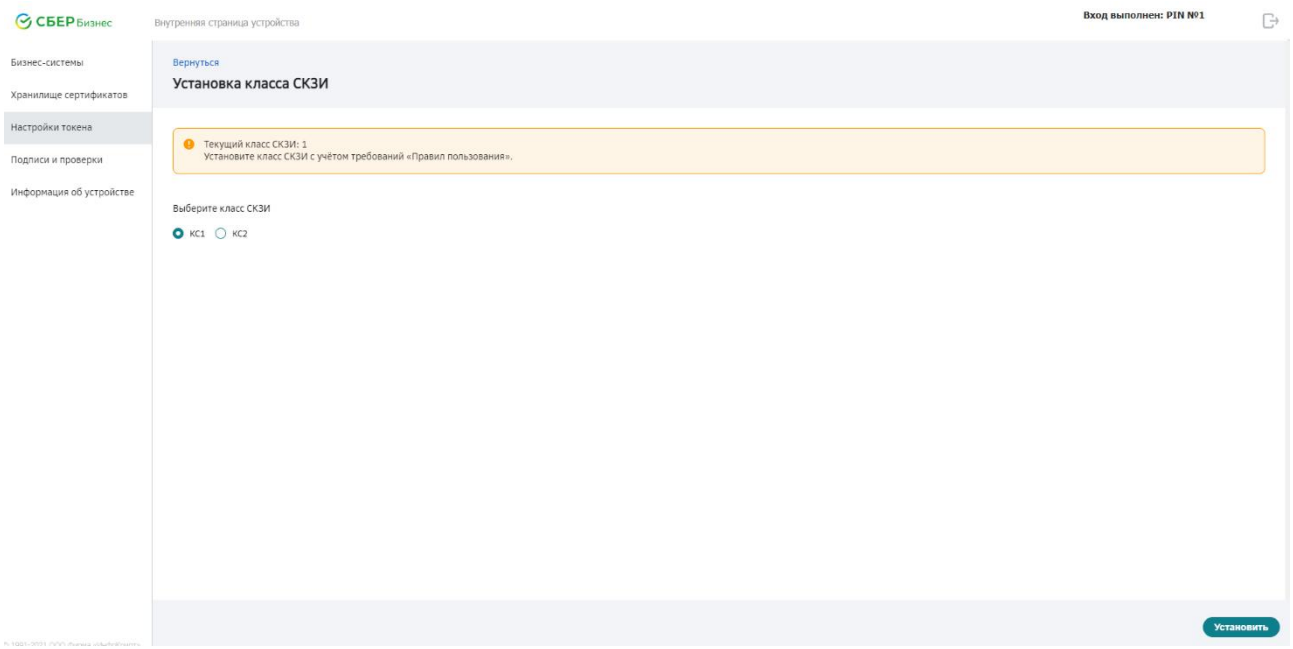


Рисунок 36 - Страница установки класса СКЗИ

4.25 Использование HTTP-прокси для связи по TLS

Для того чтобы настроить использование HTTP-прокси сервера для связи по TLS, необходимо на внутренней странице устройства (см. Рисунок 4) выбрать пункт меню **Настройки токена**.

На открывшейся странице (см. Рисунок 22) следует перейти по ссылке «TLS-прокси» в центральной части страницы или нажать кнопку **TLS-прокси** справа от неё.

На открывшейся странице настройки использования HTTP-прокси (см. Рисунок 37) для использования HTTP-прокси необходимо выполнить следующие действия:

- Установить флажок «Использовать HTTP прокси».
- В поле «Адрес» указать адрес HTTP-прокси сервера
- В поле «Порт» указать номер порта HTTP-прокси сервера.
- Если на прокси сервере необходимо аутентифицироваться, установить флажок «Аутентифицироваться на прокси» и вести в соответствующие поля логин и пароль, для аутентификации на прокси сервере.
- Нажать кнопку **Сохранить настройки** в правом нижнем углу страницы.

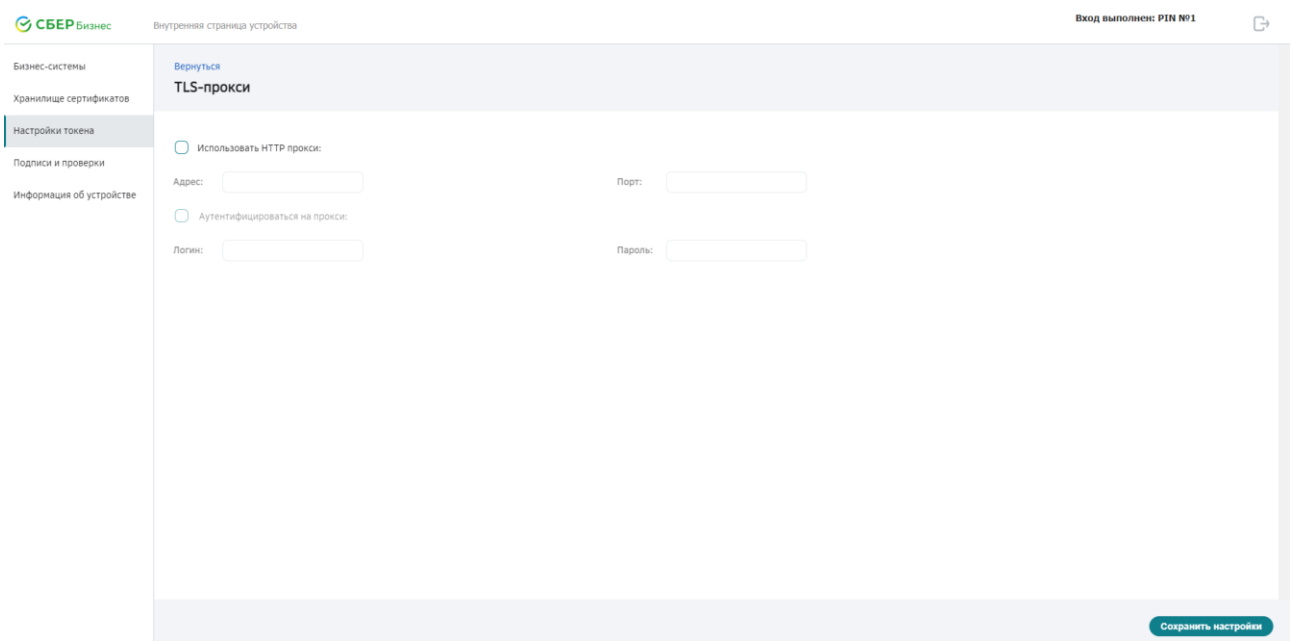


Рисунок 37 – Страница настройки использования HTTP-прокси

Для того чтобы отключить использование HTTP-прокси, необходимо выполнить следующие действия:

– Снять флажок «Использовать HTTP прокси».

– Нажать кнопку **Сохранить настройки** в правом нижнем углу страницы.

4.26 Просмотр информации об устройстве

Для получения информации об устройстве следует выбрать пункт меню **Информация об устройстве** или на странице настройки устройства (см. Рисунок 22) перейти по ссылке «Информация об устройстве» в центральной части страницы или нажать кнопку **Информация об устройстве** справа от неё.

На открывшейся странице информации об устройстве (см. Рисунок 34) будет отображена следующая информация:

– Информация о разработчике устройства.

– Информация о производителе устройства.

– Версия установленного на устройстве программного обеспечения.

– Серийный номер устройства.

– Время на устройстве.

– Язык интерфейса устройства.

4.27 Завершение работы HTTP-сервера

В СКЗИ «VPN-Key-TLS» предусмотрена возможность завершения работы HTTP-сервера. При этом HTTP-интерфейс становится недоступным, но СКЗИ «VPN-Key-TLS» остаётся доступным для работы через csp-интерфейс.

Для завершения работы HTTP-сервера следует выбрать пункт меню **Информация об устройстве** или на странице настройки устройства (см. Рисунок 22) перейти по ссылке «Информация об устройстве» в центральной части страницы или нажать кнопку **Информация об устройстве** справа от неё.

На открывшейся странице информации об устройстве (см. Рисунок 34) необходимо перейти по ссылке Завершить работу HTTP-сервера.

При появлении сообщения с предложением подтвердить завершение работы HTTP-сервера (см. Рисунок 43) следует нажать кнопку **ОК** для подтверждения или кнопку **Отмена** для отказа.

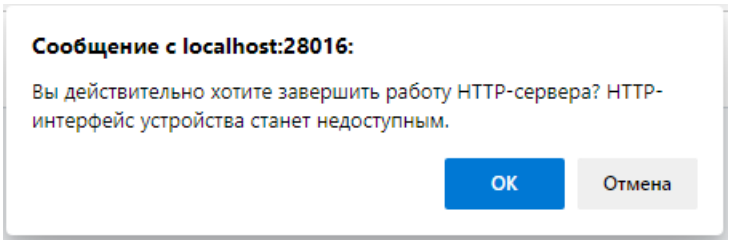


Рисунок 38 – Сообщение с предложением подтвердить завершение работы HTTP-сервера

Для того чтобы включить HTTP-интерфейс СКЗИ «VPN-Key-TLS», следует заново запустить приложение START (см. раздел 3.2).

4.28 Форматирование учётной записи

Учётная запись пользователя может быть отформатирована. При форматировании из памяти устройства удаляются все ключевые пары и запросы, созданные данной учётной записью, и все выданные для неё сертификаты. Кроме того, для данной учётной записи очищаются PIN- и PUK-коды. В результате открытие внутренней страницы устройства VPN-Key-TLS для данной учётной записи становится возможным без ввода PIN-кода, но до задания пользователем PIN- и PUK-кодов запрещается создание ключевых пар и открытие TLS-тоннелей к бизнес-системам.

Для того чтобы отформатировать учётную запись, необходимо на странице авторизации (см. Рисунок 3) перейти по ссылке Подробнее. На появившейся странице с информацией об устройстве необходимо перейти по ссылке Разрешить расширенное управление учётными записями в нижней части страницы.

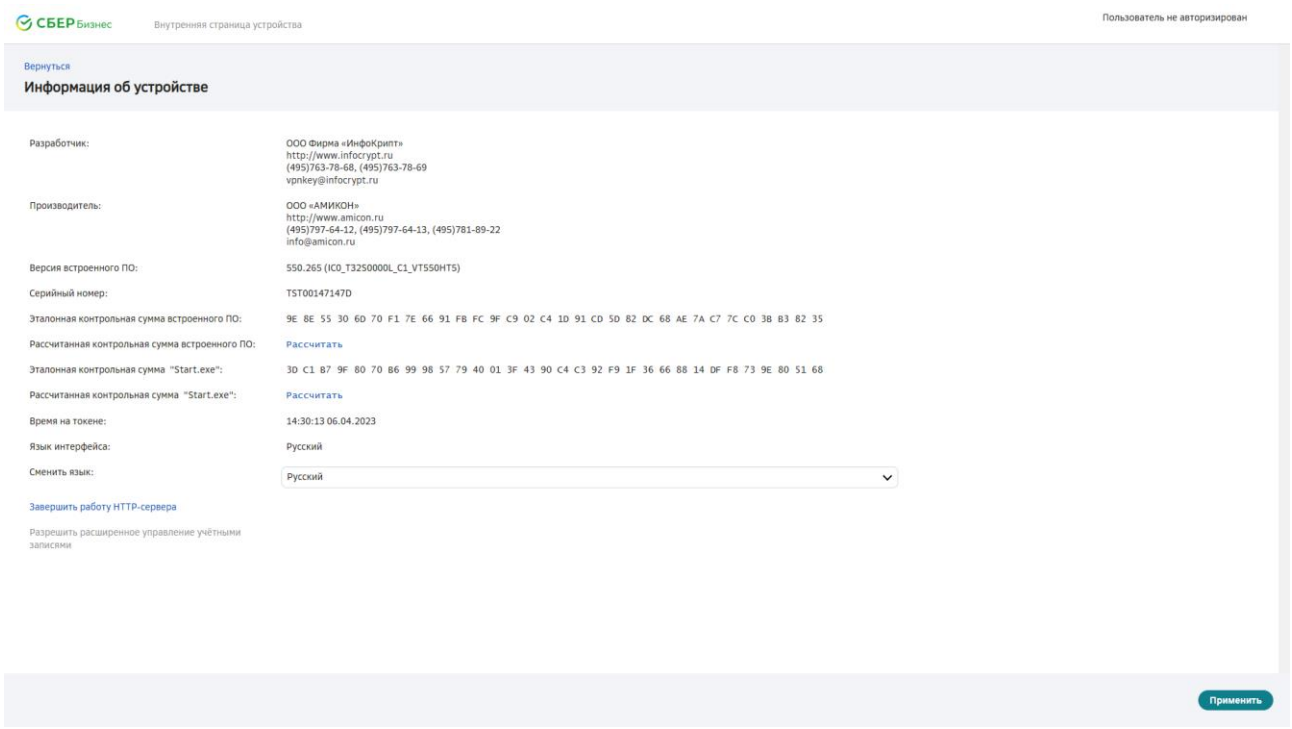


Рисунок 39 – Информация об устройстве

При появлении сообщения с предупреждением о возможных критических последствиях форматирования, таких как удаление всех ключевые пар, запросов и личных сертификатов, (см. Рисунок 40) следует нажать кнопку **ОК** для продолжения или кнопку **Отмена** для отказа от форматирования.

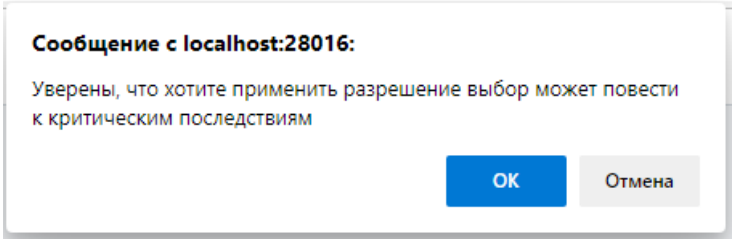


Рисунок 40 – Предупреждение о возможных последствиях форматирования

Для продолжения следует перейти по появившейся ссылке Перейти к расширенному управлению учётными записями в нижней части страницы с информацией об устройстве (см. Рисунок 41).

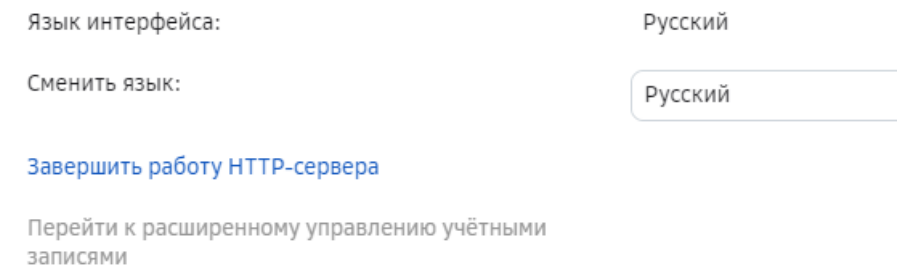


Рисунок 41 – Ссылка для перехода к расширенному управлению учётными записями

На открывшейся странице форматирования учётных записей (см. Рисунок 42) необходимо выбрать учётную запись, которую требуется отформатировать, и нажать кнопку **Форматировать**.

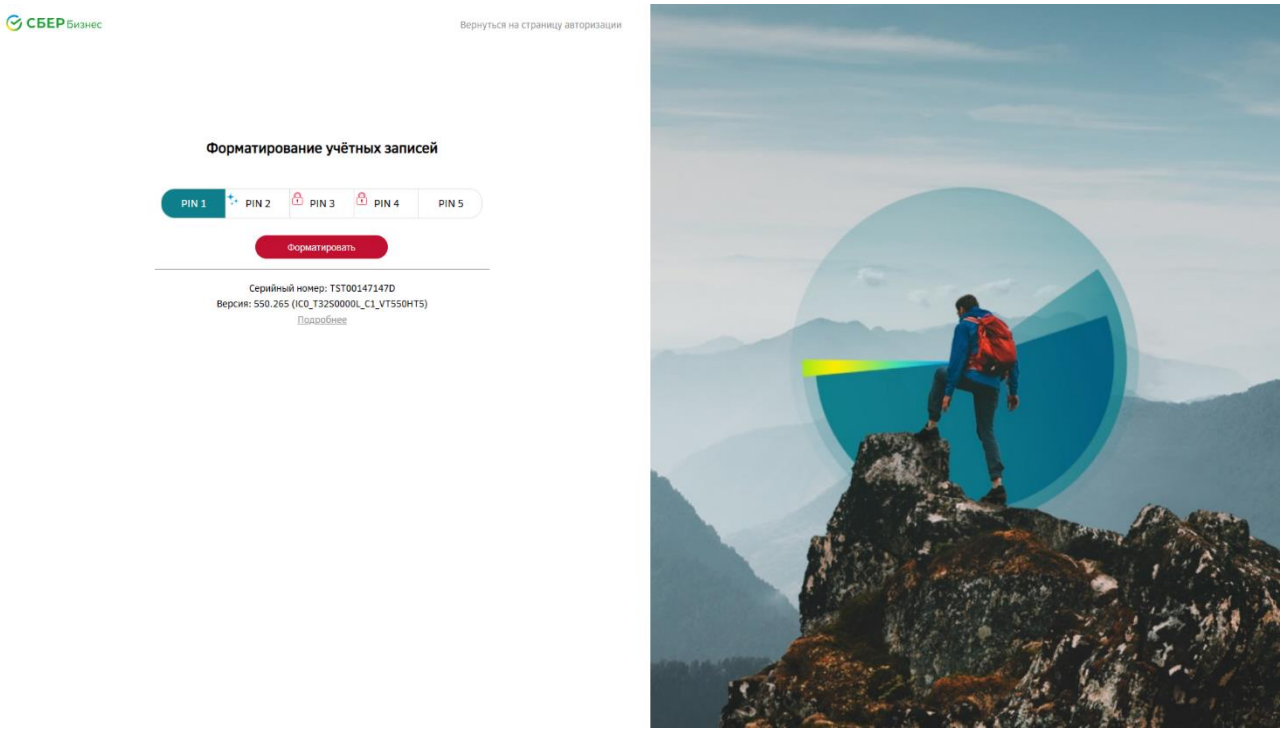


Рисунок 42 – Страница форматирования учётных записей

При появлении сообщения с предложением подтвердить форматирование выбранной учётной записи (см. Рисунок 43) следует нажать кнопку **ОК** для подтверждения форматирования или кнопку **Отмена** для отказа от форматирования.

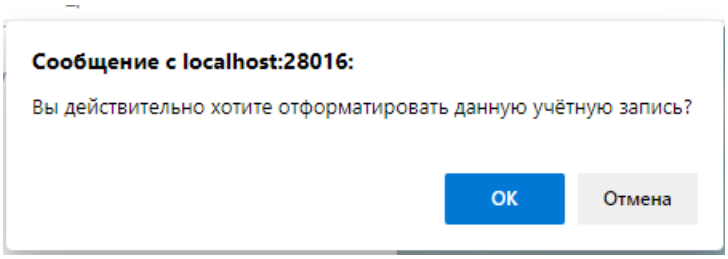


Рисунок 43 – Сообщение с предложением подтвердить форматирование

В результате форматирование будет выполнено, и на странице авторизации отформатированная учётная запись будет помечена «звёздами» (см. Рисунок 44).

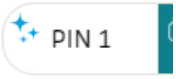


Рисунок 44 – Отформатированная учётная запись

Для такой учётной записи открытие внутренней страницы устройства VPN-Key-TLS становится возможным без ввода PIN-кода.

Для создания ключевых пар и работы с бизнес-системами необходимо перейти по ссылке Необходимо сменить PIN-код (см. Рисунок 45), появившейся в правом верхнем углу страницы.

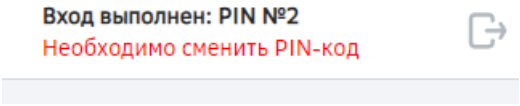


Рисунок 45 – Ссылка для перехода на страницу смены PIN-кода

На открывшейся странице изменения PIN-кода (см. Рисунок 46) необходимо выполнить следующие действия:

- Не заполнять поле «Текущий PIN».
- Ввести новый PIN-код в поле «Новый PIN». Длина PIN-кода должна быть равна 6 символам. Допустимыми символами являются английские буквы, цифры и спецсимволы.
- Повторно ввести новый PIN-код в поле «Повторите новый PIN».
- Ввести новый PUK-код в поле «Задайте в этой строке PUK-код». Устройство предложит случайный PUK-код и запишет его в поле «Задайте PUK-код». Далее его можно отредактировать по желанию пользователя. Длина нового PUK-кода должна быть равна 12 символам. Допустимыми символами являются английские буквы, цифры и спецсимволы.
- Подтвердить изменение PIN-кода, нажав кнопку **Изменить PIN** в правом нижнем углу страницы.

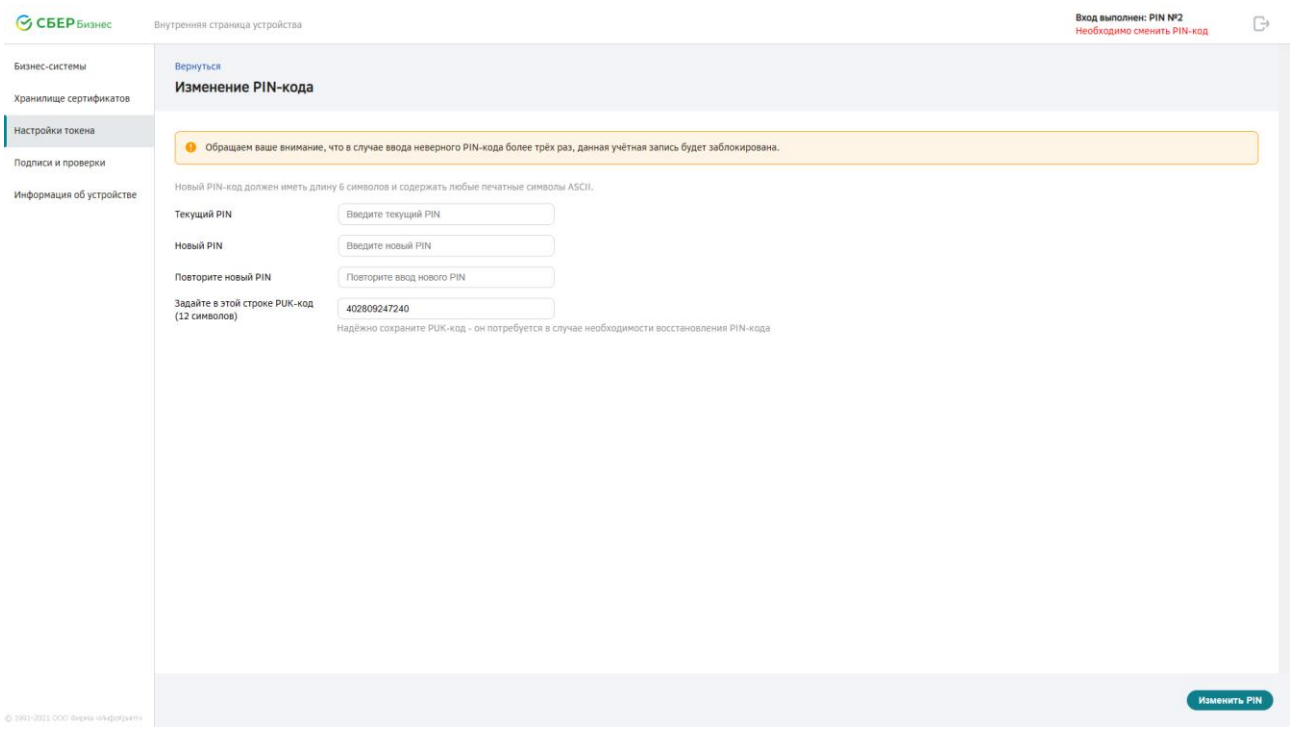


Рисунок 46 – Страница изменения PIN-кода

В результате этих действий PIN-код будет изменён и откроется страница с сообщением об успешном изменении PIN-кода.

Если новый PIN-код введен неверно, откроется страница с сообщением об ошибке.

Лист регистрации изменений

п/п	Дата	Описание изменения, основание для внесения изменения	Автор
1			
2			
3			