|  |  |
| --- | --- |
| УТВЕРЖДАЮ | АО «Комита» |

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

Руководство пользователя

Листов 38

Санкт-Петербург

2021

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc65172036)

[ВВЕДЕНИЕ 3](#_Toc65172037)

[1 ОБЩИЕ СВЕДЕНИЯ 4](#_Toc65172038)

[1.1 Назначение и возможности 4](#_Toc65172039)

[1.2 Описание логической структуры 6](#_Toc65172040)

[1.2.1 Модуль авторизации 6](#_Toc65172041)

[1.2.2 Модуль администратора 7](#_Toc65172042)

[1.2.3 Модуль хранителя ключа: 7](#_Toc65172043)

[1.2.4 Модуль криптографической защиты: 8](#_Toc65172044)

[1.3 Аппаратно-программные требования 8](#_Toc65172045)

[2 ПОДГОТОВКА К РАБОТЕ 9](#_Toc65172046)

[2.1 Установка и обновление 9](#_Toc65172047)

[2.2 Запуск и остановка ПО СКЗД 10](#_Toc65172048)

[2.3 Настройка работы по сети 10](#_Toc65172049)

[2.4 Запуск веб-интерфейса 11](#_Toc65172050)

[2.5 Авторизация в ПО СКЗД 11](#_Toc65172051)

[2.5 Выбор файла лицензии 13](#_Toc65172052)

[2.6 Смена пароля пользователем 15](#_Toc65172053)

[3 МОДУЛЬ АДМИНИСТРАТОРА 17](#_Toc65172054)

[3.1 Вкладка Пользователи 18](#_Toc65172055)

[3.2 Вкладка Ключи 22](#_Toc65172056)

[4 МОДУЛЬ ХРАНИТЕЛЯ КЛЮЧА 27](#_Toc65172057)

[5 ВЗАИМОДЕЙСТВИЕ АРМ 407-П С ПО СКЗД 33](#_Toc65172058)

[5.1 Настройка АРМ для работы с ПО СКЗД 33](#_Toc65172059)

[5.2 Требования к лицензии 33](#_Toc65172060)

[5.3 Авторизация в ПО СКЗД 34](#_Toc65172061)

[5.4 Изменение пароля 35](#_Toc65172062)

[6 ЛОГИРОВАНИЕ СИСТЕМЫ 38](#_Toc65172063)

[7 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 39](#_Toc65172064)

ВВЕДЕНИЕ

Настоящее Руководство пользователя является программным документом по применению Системы криптографической защиты данных (далее – ПО СКЗД).

Настоящее руководство содержит описание ПО СКЗД, включая:

* общие сведения о программном продукте;
* его назначение, возможности;
* установку и настройку;
* пользовательские процедуры, работа в АРМ 407-П с ПО СКЗД.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

© АО «КОМИТА», 2021

# ОБЩИЕ СВЕДЕНИЯ

## Назначение и возможности

ПО СКЗД – программный продукт, обеспечивающий шифрование согласно требованиям стандарта PCI PA-DSS номеров платежных карт (PAN), сохраняемых в базе данных. Для шифрования PAN применяется алгоритм AES с длиной ключа не менее 128 бит в режиме ECB.

ПО СКЗД взаимодействует с АРМ 407-П ипозволяет:

* осуществлять шифрование номеров банковских карт при получении зашифрованных запросов Росфинмониторинга в АРМ,
* сохранять зашифрованные данные PAN в БД;
* осуществлять расшифровку данных PAN по требованию пользователя АРМ.

Система криптографической защиты хранимых данных также обеспечивает возможность защищенного управления ключами шифрования в соответствии с требованиями стандарта PCI DSS.

Общая схема работы с данными при взаимодействии ПО СКЗД с АРМ 407-П изображена на рисунке:

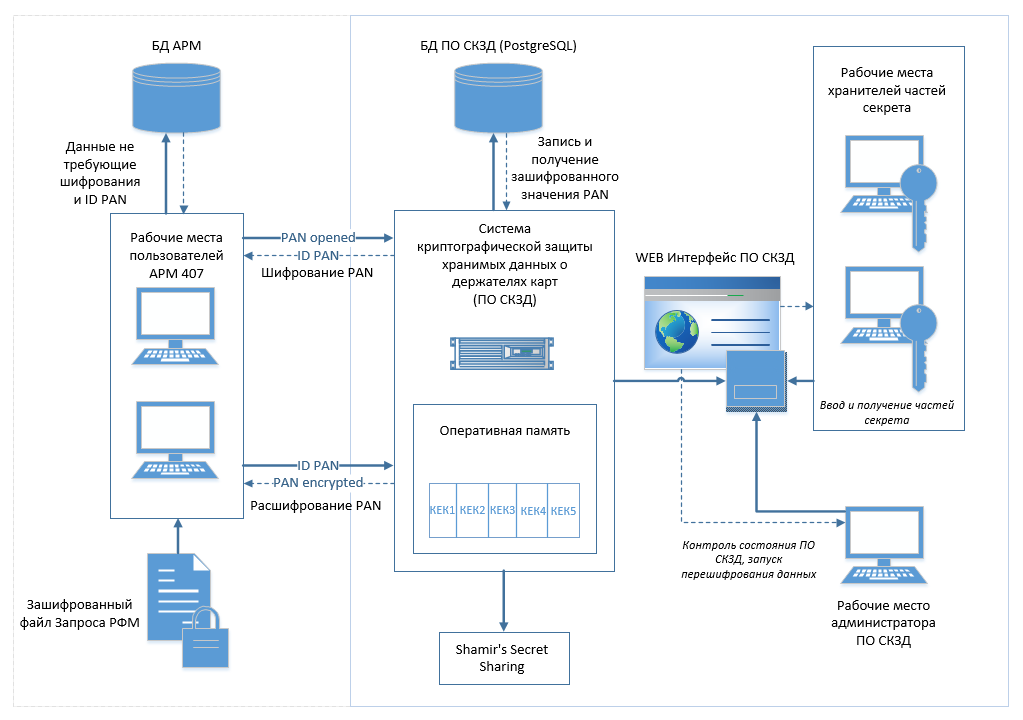


Рис. 1 Общая схема работы ПО СКЗД с АРМ 407

|  |  |
| --- | --- |
| info_button_32 | После первого запуска ПО СКЗД формируется секрет Шамира, который делится на 5 частей и передается хранителям ключа. Программа ожидает подтверждение получения хранителями частей секрета. Из секрета формируется симметричный ключ AES. Данным ключом шифруются случайно сгенерированные тысяча последовательностей (ключи шифрования информации DEK).  При последующих запусках ПО СКЗД, для восстановления секрета и начала работы, достаточно корректно введенных трех частей секрета.  После успешного ввода хранителями своих частей секрета ключ КEK восстанавливается, и программа готова к работе – получению, перешифрованию и сохранению данных.  При неуспешном вводе хранителями частей секрета он не восстанавливается, ПО СКЗД переходит в состояние *«Ошибка»*. При этом требуется остановка и перезапуск ПО СКЗД |

## Описание логической структуры

ПО СКЗД включает в себя следующие модули: модуль авторизации, модуль администратора, модуль хранителя ключа и модуль криптографической защиты.

Возможности и основные функции модулей системы ПО СКЗД перечислены ниже:

### Модуль авторизации

* Аутентификация пользователя;
* Авторизация пользователя.

Система аутентификации позволяет администратору [управлять учетными записями пользователей](#_Вкладка_Пользователи): добавлять пользователя, изменять пароль пользователя, блокировать пользователя, блокировать сеанс работы пользователя при простое свыше 15 минут, а также позволяет пользователям изменять свой пароль.

Аутентификация пользователя в системе представляет собой ввод имени пользователя (логина) и пароля от его учетной записи.

Аутентификация пользователя выполняется с проверками:

* имени пользователя;
* пароля;
* признака блокировки учетной записи;

|  |  |
| --- | --- |
| info_button_32 | Система аутентификации позволяет блокировать пользователя в случае 6 неудачных попыток войти в ЛК, а также блокировать сеанс работы пользователя после 15 минут простоя с необходимостью повторить авторизацию |

* необходимости смены пароля.

|  |  |
| --- | --- |
| info_button_32 | Смена пароля пользователем обязательно проводится:   * после первого входа пользователя в систему; * при наличии временного пароля пользователя; * по истечении срока действия пароля (90 дней) |

Смена пароля пользователя выполняется с проверками:

* корректности ввода старого пароля;
* совпадения нового пароля и его подтверждения;
* соответствия сложности нового пароля заданному формату (пароль может содержать цифры и латинские символы верхнего, нижнего регистра, размер пароля от 8 до 30 символов);
* несовпадения нового пароля и ранее использованных.

Если все проверки при аутентификации выполнены успешно, пользователь авторизуется в системе. При отрицательном результате хотя бы одной из проверок система выдает сообщение об ошибке, а при необходимости смены пароля открывается форма смены пароля.

Авторизация пользователя выполняется в случае успешной аутентификации. В зависимости от группы пользователя открывается ЛК соответствующего пользователя, которому предоставляется доступ к следующей функциональности:

* группа администраторов (admin) – доступ к [модулю администратора](#_МОДУЛЬ_АДМИНИСТРАТОРА) ПО СКЗД;
* группа хранителей ключа – доступ к [модулю хранителя ключа](#_МОДУЛЬ_ХРАНИТЕЛЯ_КЛЮЧА);
* группа пользователей – доступ к модулю криптографической защиты (шифрование и расшифрованные данных).

|  |  |
| --- | --- |
| info_button_32 | Для группы пользователей ЛК отсутствует, при авторизации в АРМ им становятся доступны только функции криптографической защиты данных |

### Модуль администратора

* Управление пользователями;
* Инициация и контроль процедуры формирования ключей шифрования;
* Контроль процесса ввода частей секрета ответственными сотрудниками;
* Инициация и контроль процесса перешифрования PAN на новом ключе.

### Модуль хранителя ключа:

* Получение и подтверждение части секрета;
* Ввод части секрета для функционирования ПО СКЗД.

### Модуль криптографической защиты:

* Шифрование PAN;
* Расшифрование PAN.

## Аппаратно-программные требования

Для работы ПО СКЗД требуются:

1. **Компьютер со следующими характеристиками:**

* центральный процессор – intel i3 (рекомендуется i5);
* объем свободной оперативной памяти – не менее 4 Гбайт;
* жесткий диск со свободным пространством не менее 60 Гбайт.

1. Операционная система:

* SUSE Linux Enterprise Server;
* Red Hat Enterprise Linux;
* Microsoft Windows 7 (64- разрядная) или выше.

1. База данных:

* PostgreSQL версии не ниже 10.

1. Прикладное программное обеспечение:

* Wildfly версии не ниже 13.

# ПОДГОТОВКА К РАБОТЕ

## Установка и обновление

Установку и обновление ПО СКЗД проводит администратор системы:

Перед установкой необходимо создать чистую базу данных в СУБД PostgreSQL.

Чтобы установить ПО СКЗД:

***Шаг 1.*** В файловой системе ОС создайте папку **WildFly**, например: **с:\WildFly**.

***Шаг 2.***Распакуйте в ней архив **CS\_Comita.zip.**

***Шаг 3.***В папке **\standalone\configuration** откройте файл **standalone-full.xml** на редактирование и скорректируйте строки в блоке <datasource>:

**Подключение к БД PostgreSQL:**

<connection-url>jdbc:postgresql://адрес:порт/имяБД</connection-url>

<driver-class>org.postgresql.Driver</driver-class>

<driver>postgresql-XX.X.XX.jar</driver>

Параметры **адрес, порт** и **имя БД** замените соответствующими значениями!

**Имя пользователя и пароль доступа к БД:**

<security>

<user-name>имя пользователя</user-name>

<password>пароль</password>

</security>

Пользователь должен обладать правами на создание таблиц и объектов в БД.

***Шаг 4.*** Запустите сервер **WildFly** (см. п. 2.2).

Чтобы обновить ПО СКЗД:

***Шаг 1.*** Остановите сервер **WildFly**, если он запущен (закройте окно терминала).

***Шаг 2.*** Откройте папку **Sql** обновления и выполните SQL-скрипты при их наличии в обновлении.

***Шаг 3.*** Откройте папку **standalone** и очистите папки **tmp** и **data**.

***Шаг 4.***Откройте папку **deployments** и удалите файлы с расширением **deployed**.

***Шаг 5.*** Скопируйте новый **ear**-файл программы в папку **deployments**.

***Шаг 6.*** Запустите сервер **WildFly** (см. п. 2.2).

***Шаг 7.***Очистите кэш (журнал) и куки (cookies) браузера.

## Запуск и остановка ПО СКЗД

ПО СКЗД запускается администратором системы.

Например, для ОС Microsoft Windows: чтобы запустить ПО СКЗД, вызовите из папки /**bin** исполняемый файл **standalone.bat** с ключом **-c standalone-full.xml**. Запуск необходимо осуществлять через командную строку.

Чтобы остановить ПО СКЗД, закройте окно терминала.

## Настройка работы по сети

По умолчанию сервер настроен на работу по адресу 127.0.0.1 (localhost), по порту 8080.

Для работы по локальной сети:

***Шаг 1.*** Остановите сервер, если он запущен.

***Шаг 2.*** В папке **\standalone\configuration** откройте файл **standalone-full.xml**, секцию **<interfaces>:**.

<interfaces>

<interface name="management">

<inet-address value="${jboss.bind.address.management:127.0.0.1}"/>

</interface>

<interface name="public">

<inet-address value="${jboss.bind.address:127.0.0.1}"/>

</interface>

</interfaces>

и измените ее на:

<interfaces>

<interface name="management">

<inet-address value="${jboss.bind.address.management:127.0.0.1}"/>

</interface>

<interface name="public">

**<any-address/>**

</interface>

</interfaces>

***Шаг 3.*** Сохраните и закройте измененный файл

***Шаг 4.*** Запустите сервис, проверьте вход по ссылке, используя в адресе не **localhost**, а IP адрес или доменное имя запущенного сервера.

Для работы по порту отличному от 8080:

***Шаг 1.*** Остановите сервер, если он запущен.

***Шаг 2.*** В папке **\standalone\configuration** откройте файл **standalone-full.xml**, секцию **<** **socket-binding-group >:**.

<socket-binding name="http" port="${jboss.http.port:8080}"/>

измените ее на, требуемый порт, ниже приведен пример:

<socket-binding name="http" port="${jboss.http.port:8585}"/>

***Шаг 3.*** Сохраните и закройте измененный файл

***Шаг 4.*** Запустите сервис, проверьте вход по ссылке, используя в адресе порт запущенного сервера.

## Запуск веб-интерфейса

Откройте браузер и введите адрес <адрес сервера>:<порт>/secure-store/.

<адрес сервера> – IP адрес или доменное имя компьютера, на котором установлен wildfly

<порт> - порт указанный ранее в секции **<** **socket-binding-group >,** для <socket-binding name="http" port=

Откроется главная страница веб-интерфейса.

## Авторизация в ПО СКЗД

Откройте веб-интерфейс. Откроется страница авторизации.



Рис. 2. Страница авторизации на ПО СКЗД

Для авторизации пользователя с ролью администратора

Введите логин и пароль администратора и нажмите на кнопку Подтвердить. Откроется страница модуля администрирования (ЛК администратора).

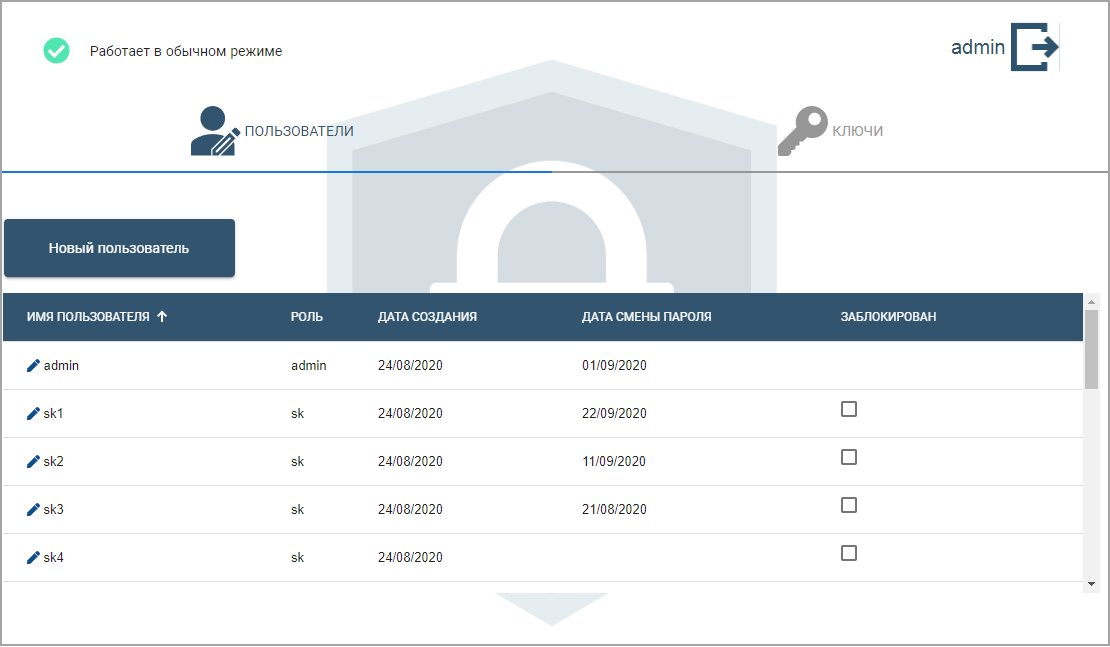


Рис. 3 Страница личного кабинета администратора

Для авторизации пользователя с ролью хранителя ключа.

При вводе учетных данных пользователя – хранителя ключа откроется страница модуля хранителя ключа (ЛК хранителя ключа).

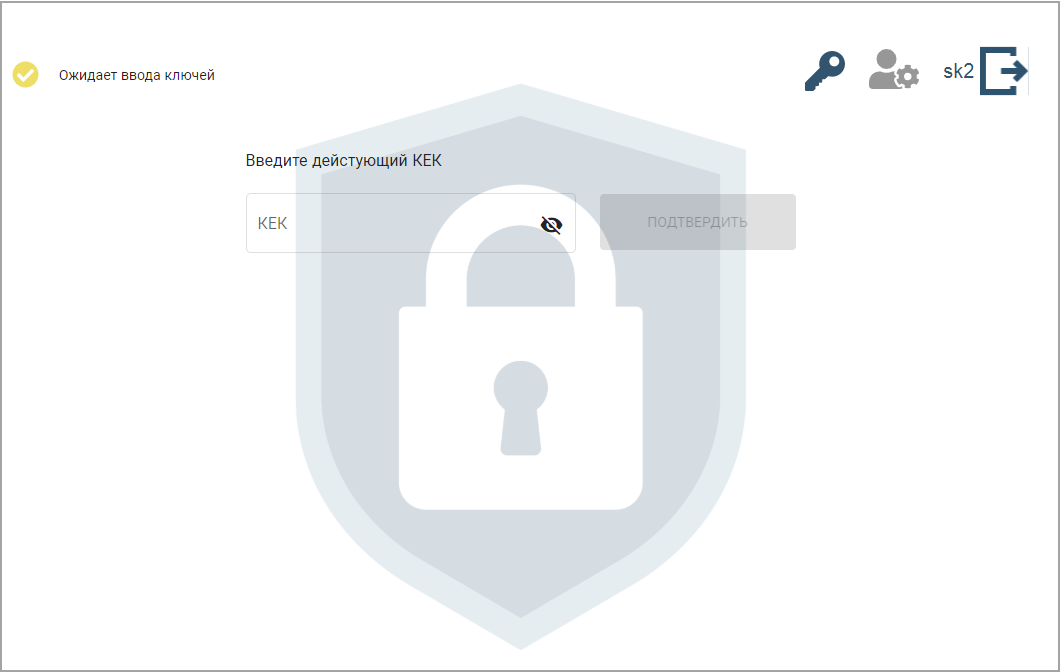


Рис. 4 Страница личного кабинета пользователя (хранителя ключа)

|  |  |
| --- | --- |
| info_button_32 | 1. После первой авторизации в ПО СКЗД необходимо [изменить свой пароль](#_Смена_пароля_пользователем), заданный по умолчанию.   Администратора: логин – admin. Пароль - admin Пользователи – хранители ключа. Логины: sk1, sk2, sk3, sk4 и sk5. Пароли соответственно: sk1, sk2, sk3, sk4 и sk5.   1. По истечении срока действия пароля (90 дней) пользователю необходимо [изменить свой пароль](#_Смена_пароля_пользователем). Перед открытием модуля пользователя откроется окно смены пароля |

## Выбор файла лицензии

Для использования ПО СКЗД в полном объеме необходимо указать файл лицензии. Полученный файл лицензии необходимо распаковать из архива, выбирать необходимо файл, с расширением \*.xml

***Для выбора файла лицензии***

***Шаг 1.*** Зайдите в модуль Администратора (см п.3)

******

***Шаг 2.*** Перейдите в раздел настройки

***Шаг 3.*** В окне выбора лицензии укажитесоответствующий файл лицензии.

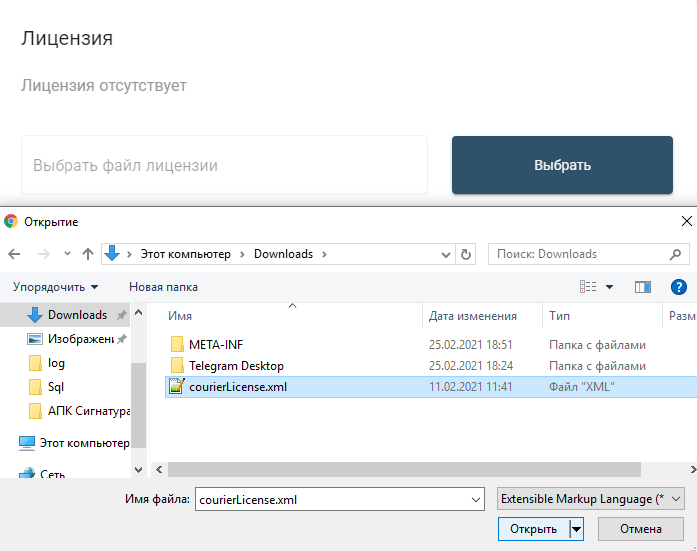
******

Рис. 5 Выбор файла лицензии

***Шаг 4.*** Убедитесь в корректности выбранной лицензии и подтвердите выбор кнопкой **Подтвердить**

Без лицензии ПО СКЗД будет работать только для расшифровки имеющихся данных в БД ПО СКЗД.

|  |  |
| --- | --- |
| info2.png | По вопросам приобретения лицензии к ПО СКЗД обращайтесь в службу технической поддержки **АО «Комита»**:   * по телефону 8 (812) 578–01–96; * по адресу электронной почты [5780196@comita.ru](mailto:5780196@comita.ru) |

## Смена пароля пользователем

Смена пароля выполняется пользователем из личного кабинета.

Для смены своего пароля нажмите на кнопку 

Будет отображена страница смены пароля.

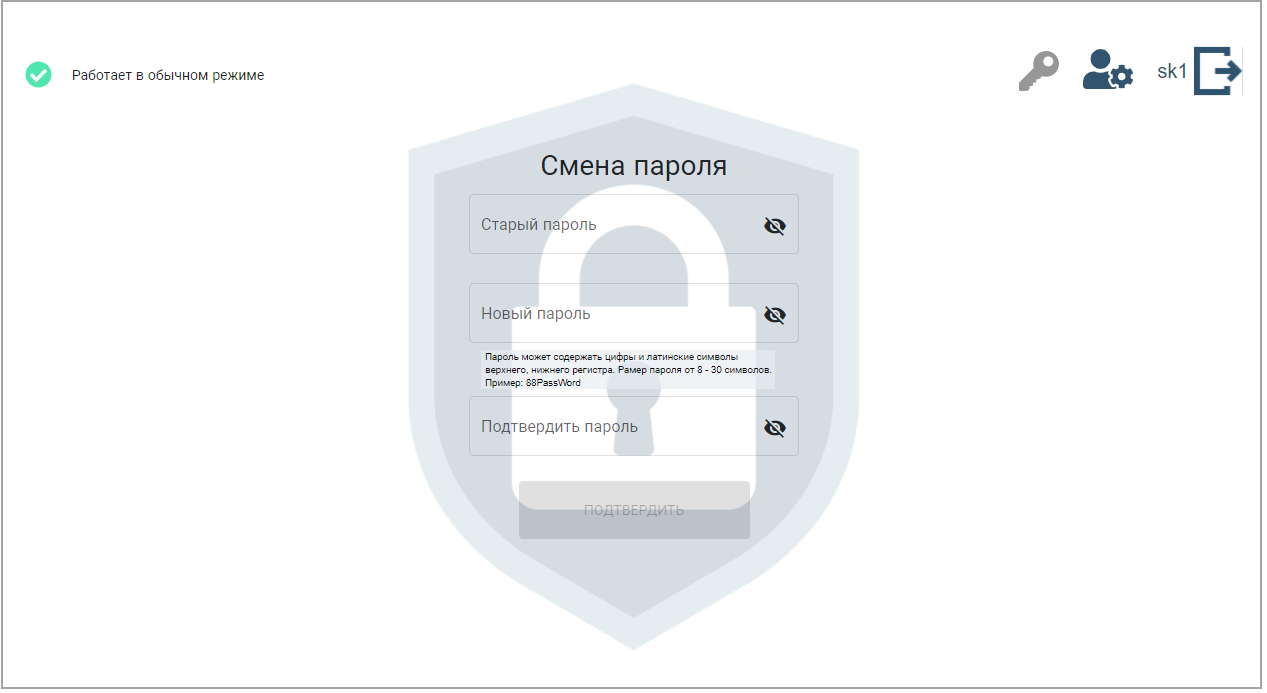


Рис. 6 Страница смены пароля

Введите свой старый пароль, новый пароль, соответствующий указанным требованиям, и подтверждение нового пароля.

|  |  |
| --- | --- |
| info_button_32 | Пароль должен содержать цифры от 0 до 9 и латинские символы верхнего регистра от А до Z и нижнего регистра от a до z. Размер пароля должен составлять от 8 до 30 символов |

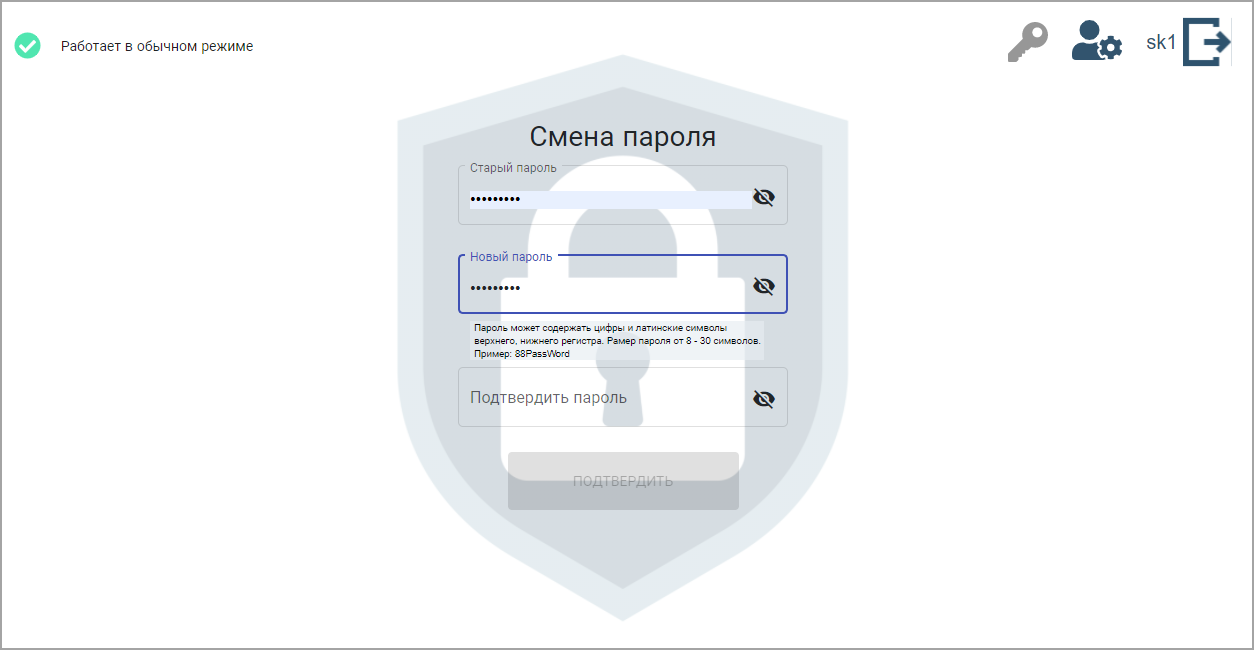


Рис. 7 Изменение пароля

Нажмите на кнопку **Подтвердить**.

Откроется диалоговое окно.

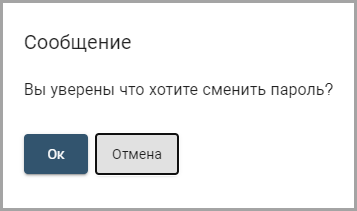


Рис. 8 Диалоговое окно

Нажмите на кнопку **ОК**.

Если все данные были введены верно, пароль пользователя будет изменен c сообщением об успешном его обновлении.



Рис. 9 Сообщение об успешном изменении пароля

Иначе будет выведено сообщение об ошибке.



Рис. 10 Сообщение об ошибке изменения пароля

# МОДУЛЬ АДМИНИСТРАТОРА

|  |  |
| --- | --- |
| info_button_32 | Все операции в модуле [протоколируются](#_ЛОГИРОВАНИЕ_СИСТЕМЫ) |

Для работы в модуле откройте страницу администратора**.**

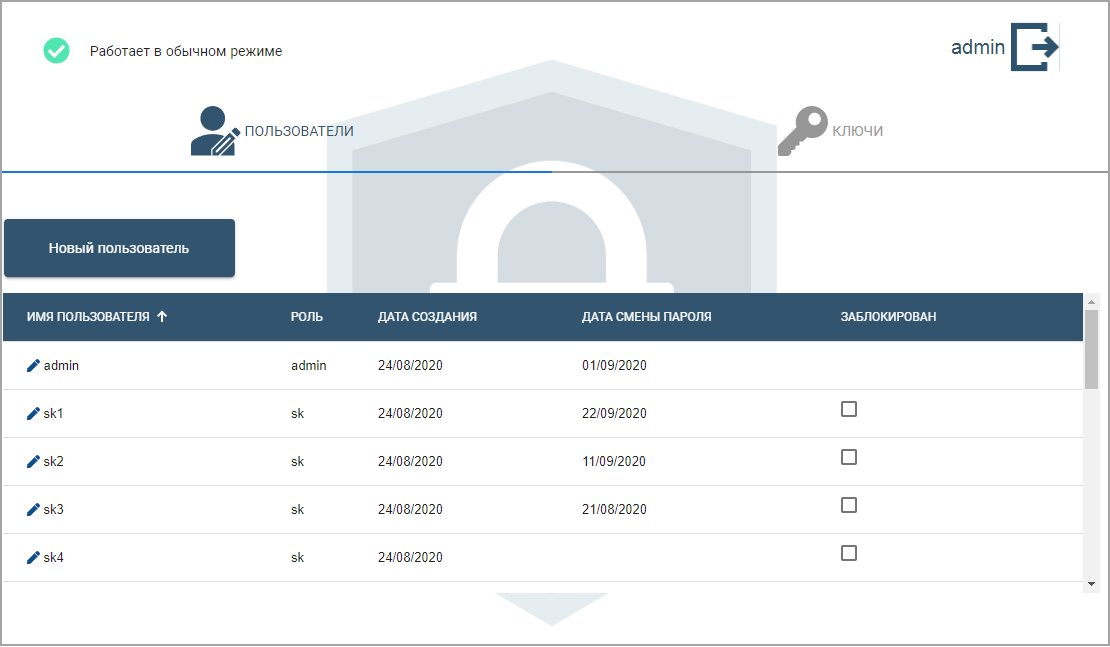


Рис. 11 Страница администратора, вкладка Пользователи

Отобразятся вкладки [**Пользователи**](#_Вкладка_Пользователи) и [**Ключи**](#_Вкладка_Ключи), кнопки управления.

|  |  |
| --- | --- |
| info_button_32 | После 15-минутного простоя сеанс работы пользователя с ПО СКЗД прерывается с требованием повторного ввода пароля для разблокировки |

Для обозначения режимов работы ПО СКЗД используются следующие значки:

 – обычный режим работы;

*  – режим формирования ключей, режим перешифрования данных, режим ожидания ввода частей секрета хранителями.

Для выхода из модуля администратора нажмите на кнопку 

## Вкладка Пользователи

Для управления учетными записями пользователей откройте вкладку **Пользователи.**

В таблице указаны пользователи системы. Пользователь-администратор (admin) и 5 пользователей-хранителей ключа (sk1...sk5) внесены в систему по умолчанию, их учетные записи (пароли) доступны для редактирования.

Других пользователей, которым доступен модуль криптозащиты, администратор может добавлять в систему, устанавливать им пароли, блокировать и т.д.

Для добавления пользователя

Нажмите на кнопку **Новый пользователь.**

Откроется форма создания пользователя.

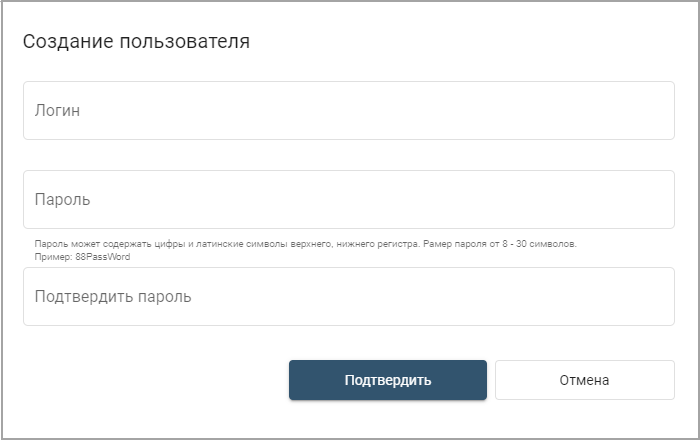


Рис. 12. Форма добавления пользователя

Логин пользователя – его уникальное имя в системе. Максимальная длина логина 100 символов.

Пароль пользователя устанавливается администратором и может быть изменен администратором или самим пользователем. Подсказка к полю **Пароль** содержит описание [требований](#треб) к символам в пароле и к их количеству.

Заполните поля формы и нажмите на кнопку Подтвердить.

При правильном заполнении полей новый пользователь будет добавлен в систему.

***Для редактирования учетных данных пользователя***

Нажмите на значок  в строке выбранного пользователя (изменять можно только пароль пользователя).

Откроется форма редактирования.

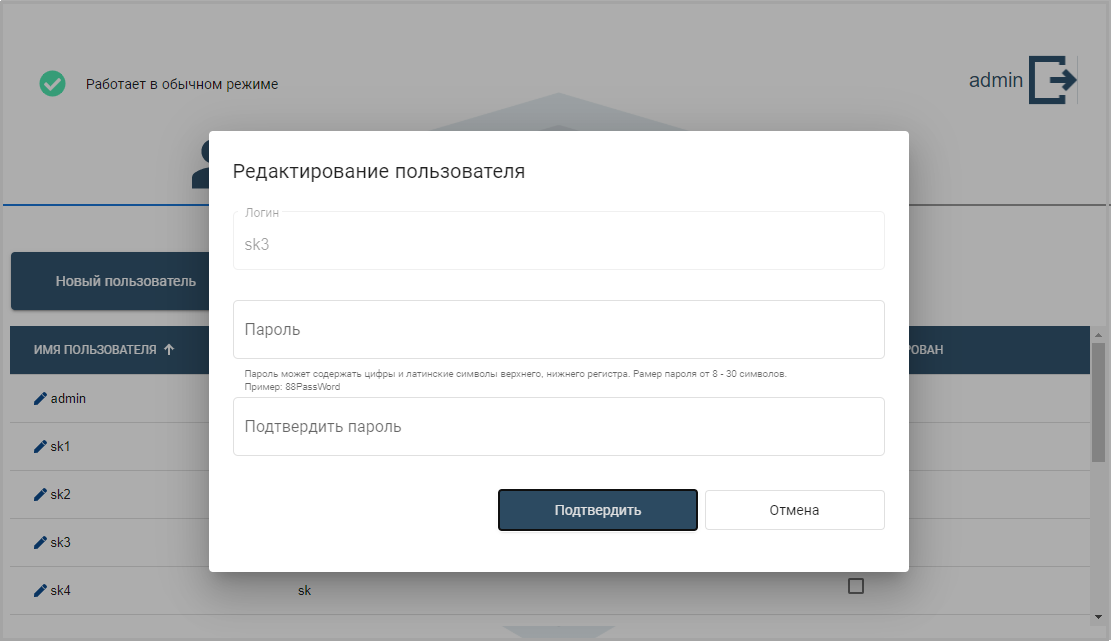


Рис. 13 Форма редактирования учетных данных пользователя

Введите новый пароль пользователя, введите его подтверждение и нажмите на кнопку Подтвердить.

При редактировании учетных данных администратора введите старый пароль пользователя–администратора, введите новый пароль администратора и его подтверждение, нажмите на кнопку Подтвердить.

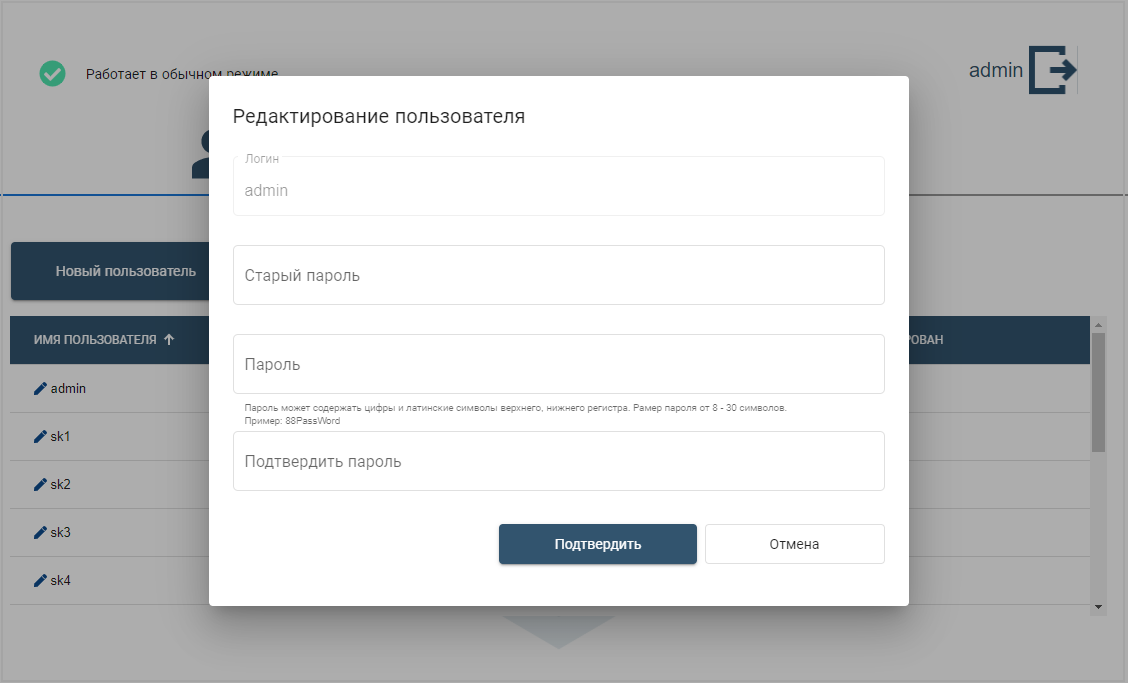


Рис. 14 Форма редактирования учетных данных администратора

При правильном заполнении полей будут внесены изменения в учетные данные существующего пользователя.

|  |  |
| --- | --- |
| info_button_32 | Пароль пользователя, установленный администратором, является временным. После первого входа в программу пользователю необходимо [изменить свой пароль](#_Смена_пароля_пользователем) |

***Для блокирования пользователя***

Установите флажок в столбце **Заблокирован** напротив выбранного пользователя.

Откроется окно подтверждения

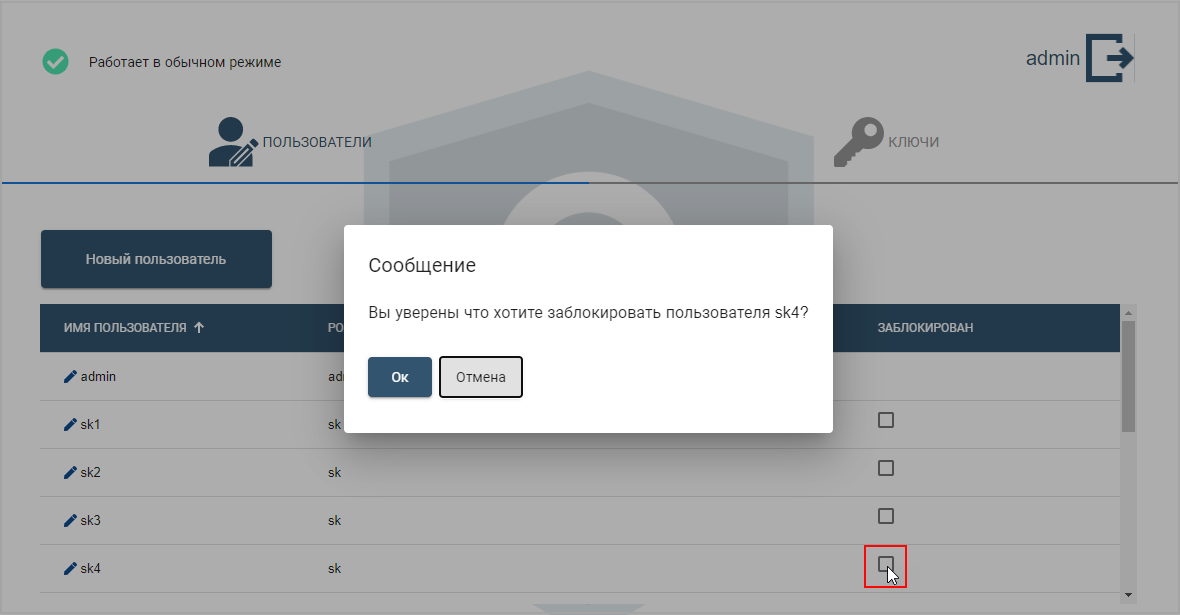


Рис. 15 Окно подтверждения блокировки пользователя

Нажмите на кнопку **ОК**. Выбранный пользователь будет заблокирован

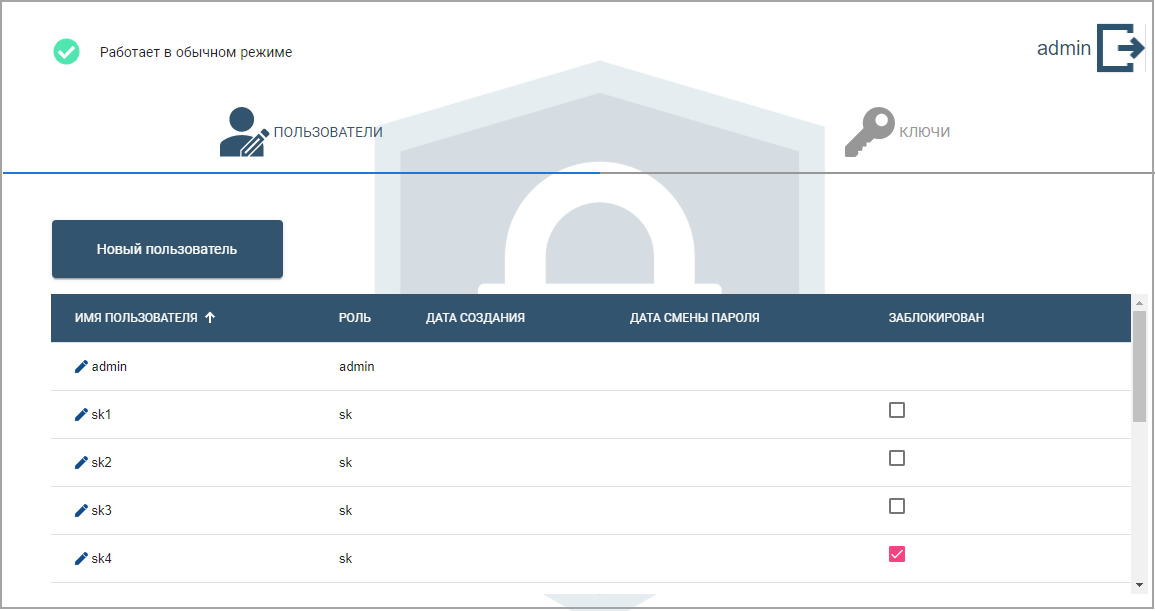


Рис. 16 Пользователь заблокирован

При попытке входа заблокированного пользователя в личный кабинет будет выведено сообщение об ошибке.



Рис. 17 Сообщение о блокировке пользователя

## Вкладка Ключи

Для управления ключами откройте вкладку **Ключи.**

На вкладке отображается перечень хранителей ключа и статус ключа (KEK) для каждого из пяти хранителей.

В рабочем режиме ПО СКЗД все ключи хранителей подтверждены, секрет сформирован. ПО СКЗД находится в состоянии «Работает в обычном режиме» и может получать, перешифровывать и сохранять данные.

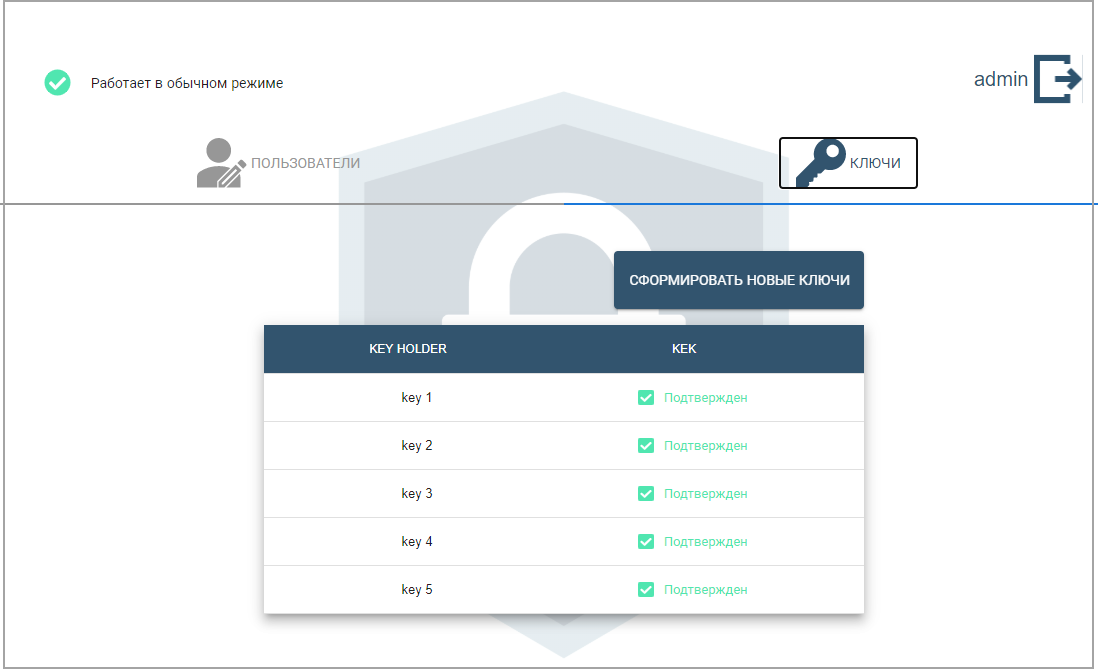


Рис. 18 Страница администратора, вкладка Ключи

|  |  |
| --- | --- |
| info_button_32 | Секрет формируется после первого запуска ПО СКЗД. Процедура изменения секрета (формирования новых ключей) может быть инициирована администратором системы |

Для смены секрета и формирования новых ключей

***Шаг 1.*** Нажмите на кнопку Сформировать новые ключи.

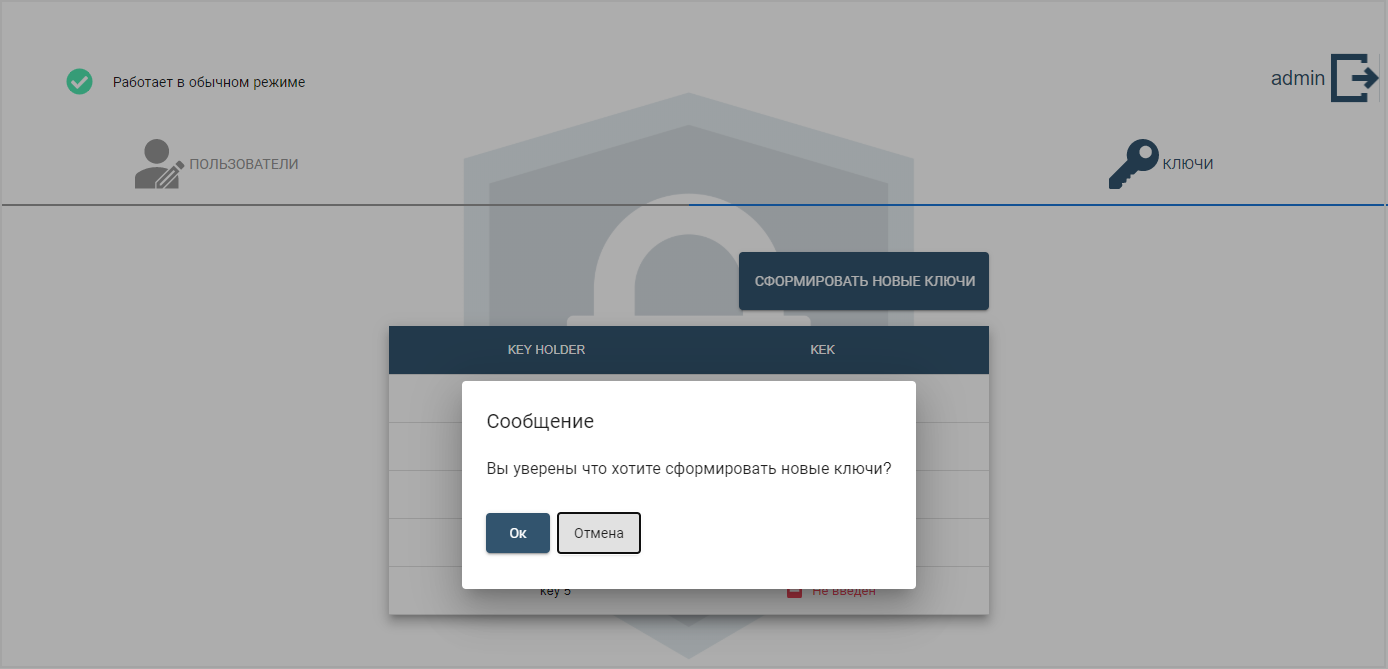


Рис. 19 Страница администратора, переход в режим смены ключей

***Шаг 2.*** Нажмите на кнопку Ок. Будет запущен процесс формирования новых ключей шифрования. Состояние ПО СКЗД изменится на «Раздает новые ключи».

Части секрета получат статус «Не подтвержден» в столбце КЕК*.* Сервер будет ожидать подтверждения хранителями своих новых частей секрета.

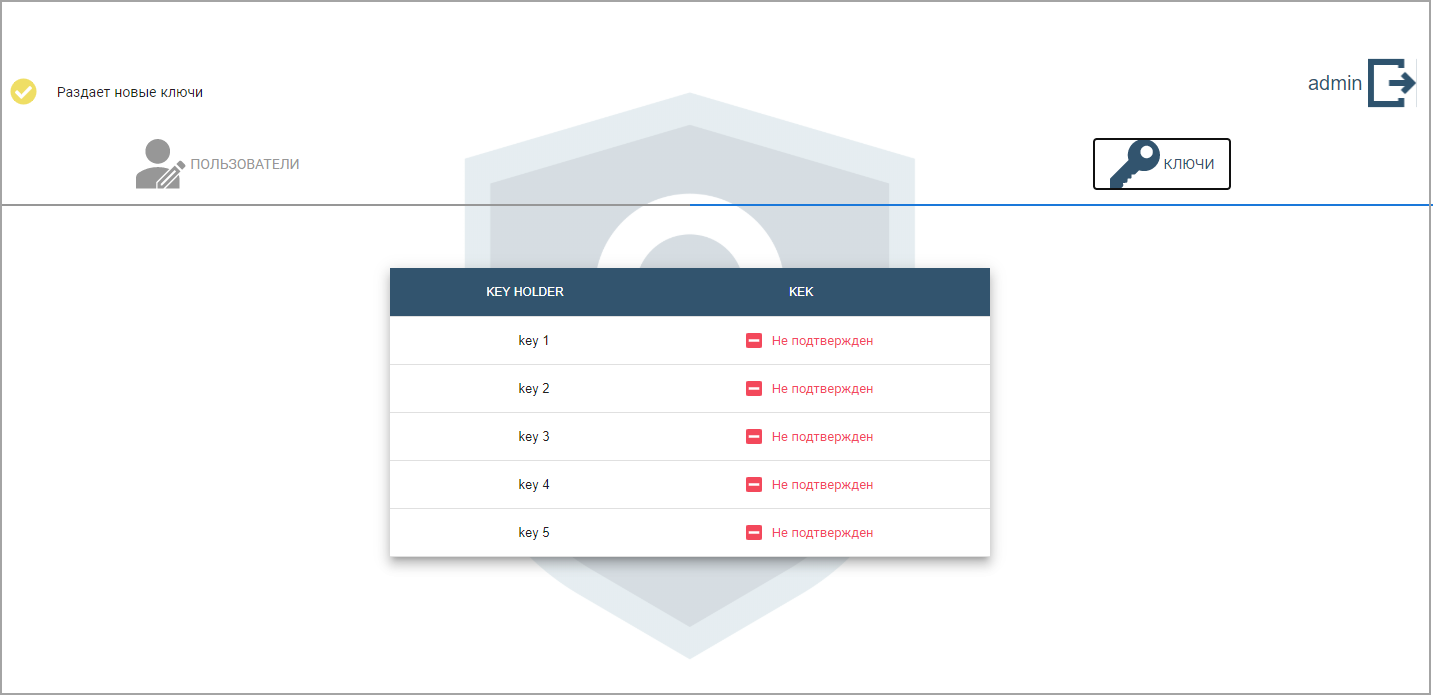


Рис. 20 Страница администратора, ПО СКЗД раздает хранителям новые ключи

***Шаг 3.*** В таблице на вкладке **Ключи** отображаются текущие статусы частей секрета.

После подтверждения хранителями частей секрета, изменяется статус в колонке КЕК на *«Подтвержден»*.

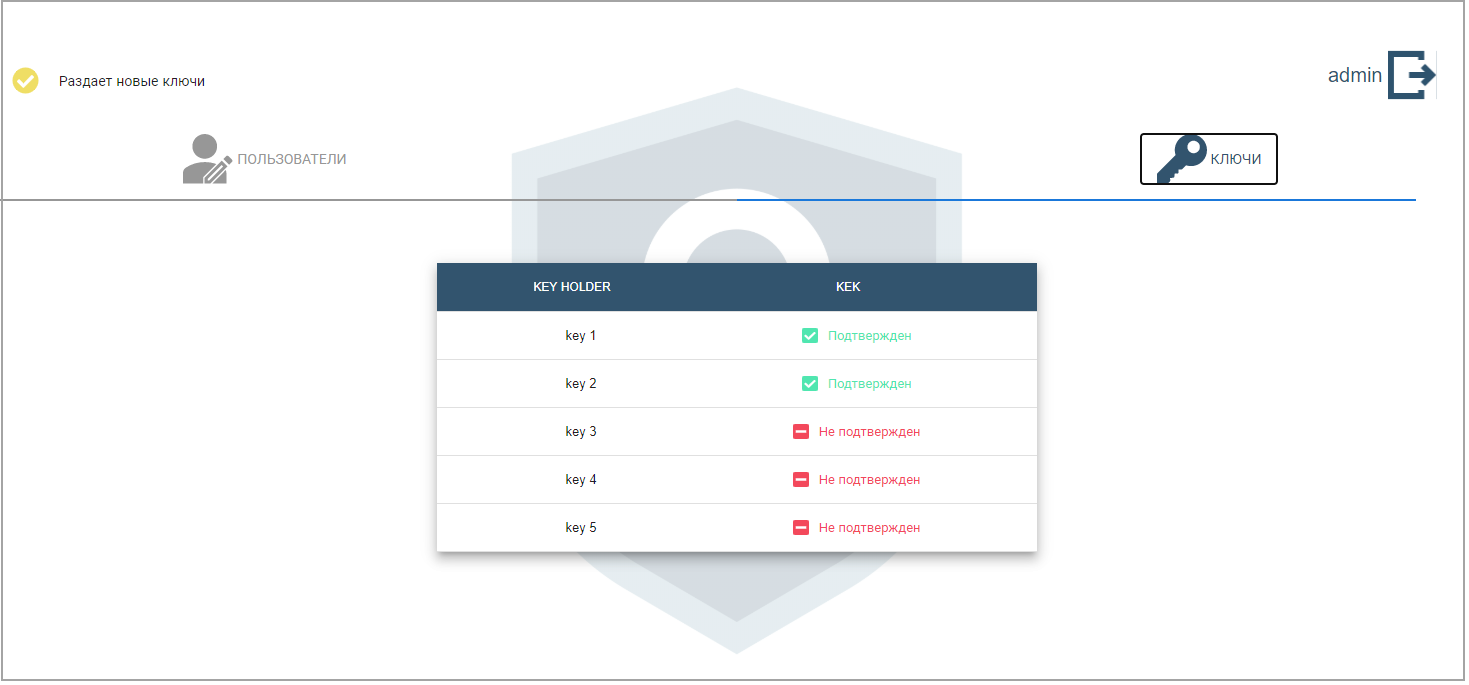


Рис. 21 Страница администратора, изменение статуса ключей

***Шаг 4.*** После подтверждения **всех** пяти частей секрета их хранителями ПО СКЗД запускает процесс перешифрования данных PAN на новых ключах.

Состояние ПО СКЗД изменится на «Работает перешифрование данных на новых ключах».

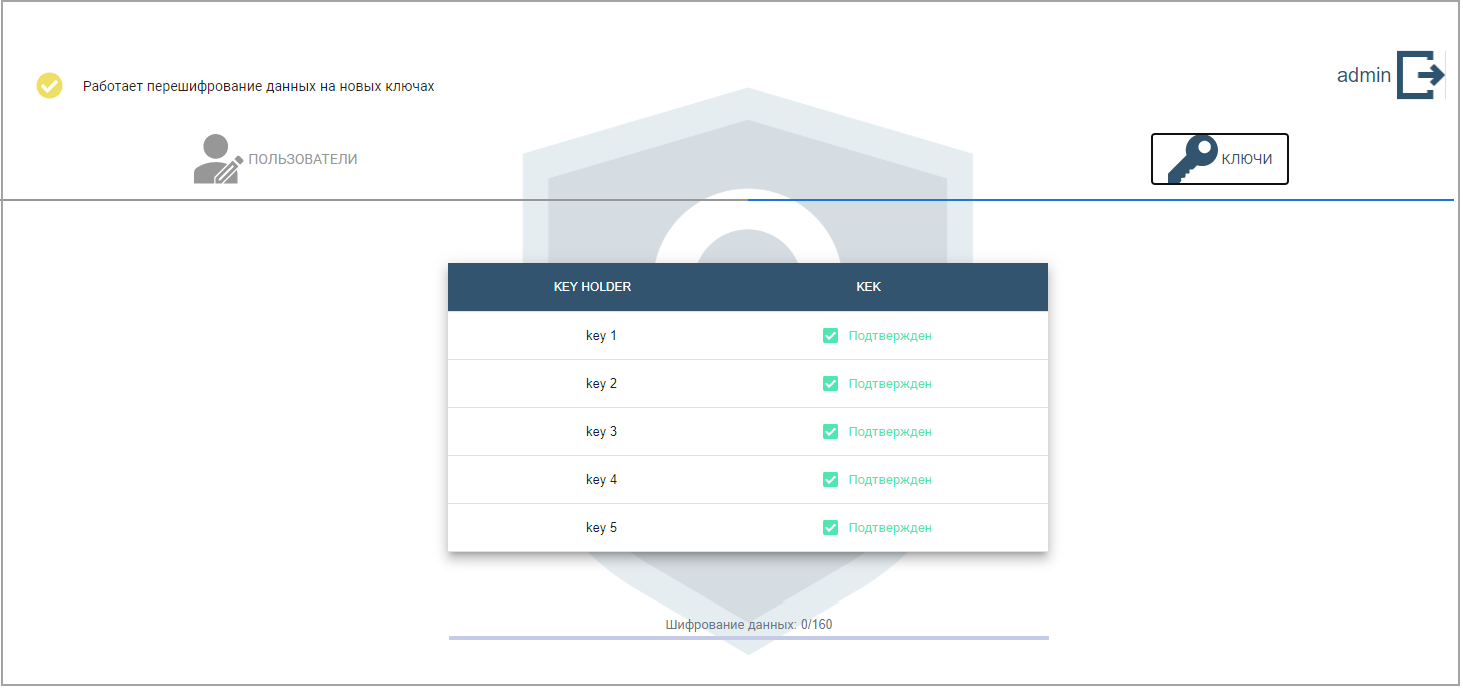


Рис. 22 Страница администратора, все ключи подтверждены. Процесс перешифрования

***Шаг 5.*** По окончании процесса перешифрования ПО СКЗД переходит в состояние «Работает в обычном режиме».

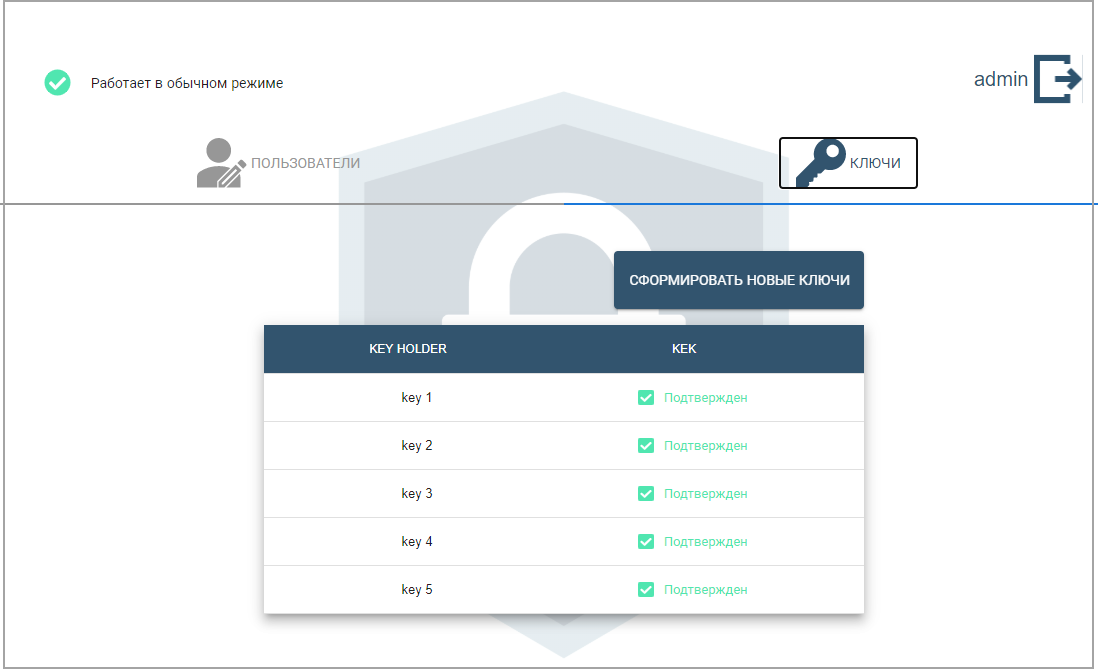


Рис. 23 Страница администратора, все ключи подтверждены. Процесс перешифрования завершен

Для контроля введенных ключей

Администратор проводит контроль введенных частей секрета пользователей-хранителей ключа. Работа АРМ с ПО СКЗД возможна, если ключи правильно введены хотя бы тремя из пяти хранителей.

Если ключ не введен хранителем, это отображается в ЛК администратора статусом ключа *«Не введен».*

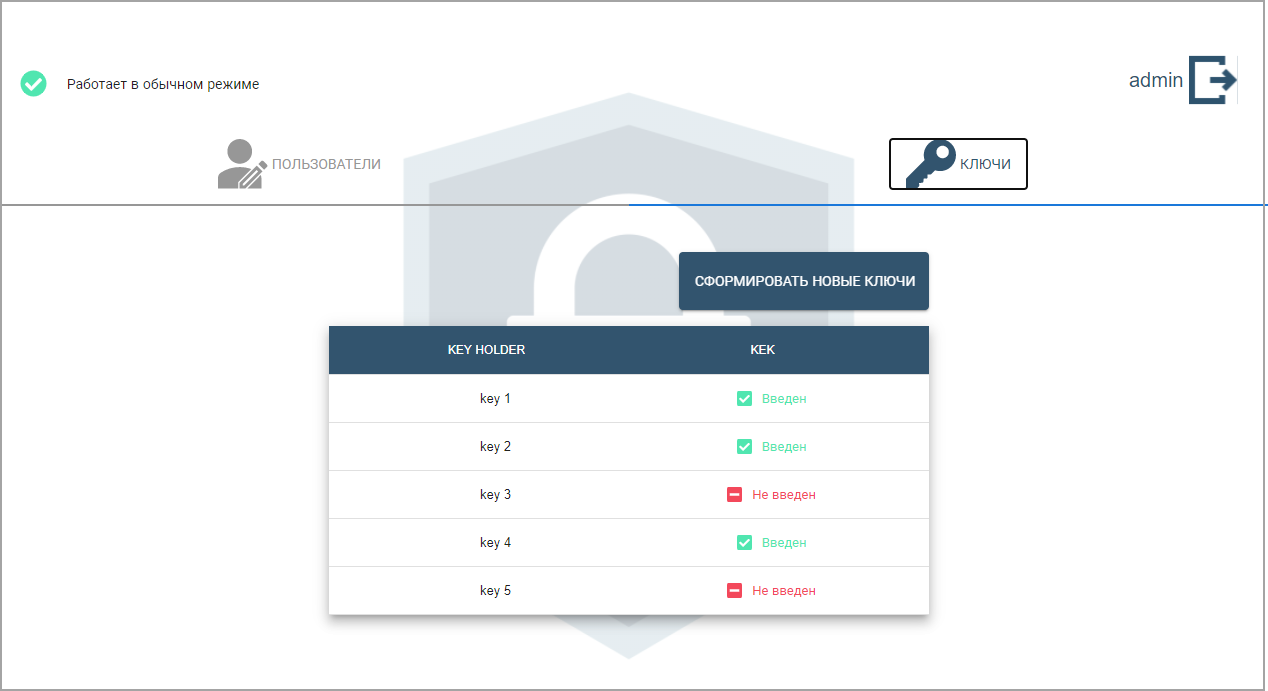


Рис. 24 Страница администратора. Контроль ввода частей секрета

Если хотя бы один из трех ключей введен с ошибкой, это отображается статусом *«Введен с ошибкой»* длявсех введенных ключей.

Если после ввода частей секрета нет возможности восстановить секрет (не было введено минимум трех корректных частей секрета), то ПО СКЗД переходит в состояние *«Ошибка»*, после чего требуется перезапуск ПО СКЗД.

# МОДУЛЬ ХРАНИТЕЛЯ КЛЮЧА

Модуль хранителя ключа позволяет:

* Получить новую часть секрета;
* Ввести часть секрета.

Для работы в модуле пройдите авторизацию с учетными данными хранителя ключа. Откроется страница пользователя – хранителя ключа.

|  |  |
| --- | --- |
| info_button_32 | После 15-минутного простоя сеанс работы пользователя с ПО СКЗД прерывается с требованием повторного ввода пароля для разблокировки |

На странице пользователя отображаются кнопки управления, а также значок текущего состояния ([режима работы](#режим_работы)) ПО СКЗД.



Рис. 25 Страница пользователя – хранителя ключа

|  |  |
| --- | --- |
| info_button_32 | При первичном формировании или изменении секрета ПО СКЗД разделяет секрет на части, раздает их хранителям и ожидает от них подтверждения получения своих частей секрета.  Хранитель ключа должен сохранять/запомнить значение той части секрета, которой владеет, и вводить его по запросу системы |

Для выхода из модуля хранителя ключа нажмите на кнопку .

Получение хранителем части секрета.

***Шаг 1.*** При получении нового ключа КЕК на странице хранителя отобразится сообщение «Ваш новый КЕК…».

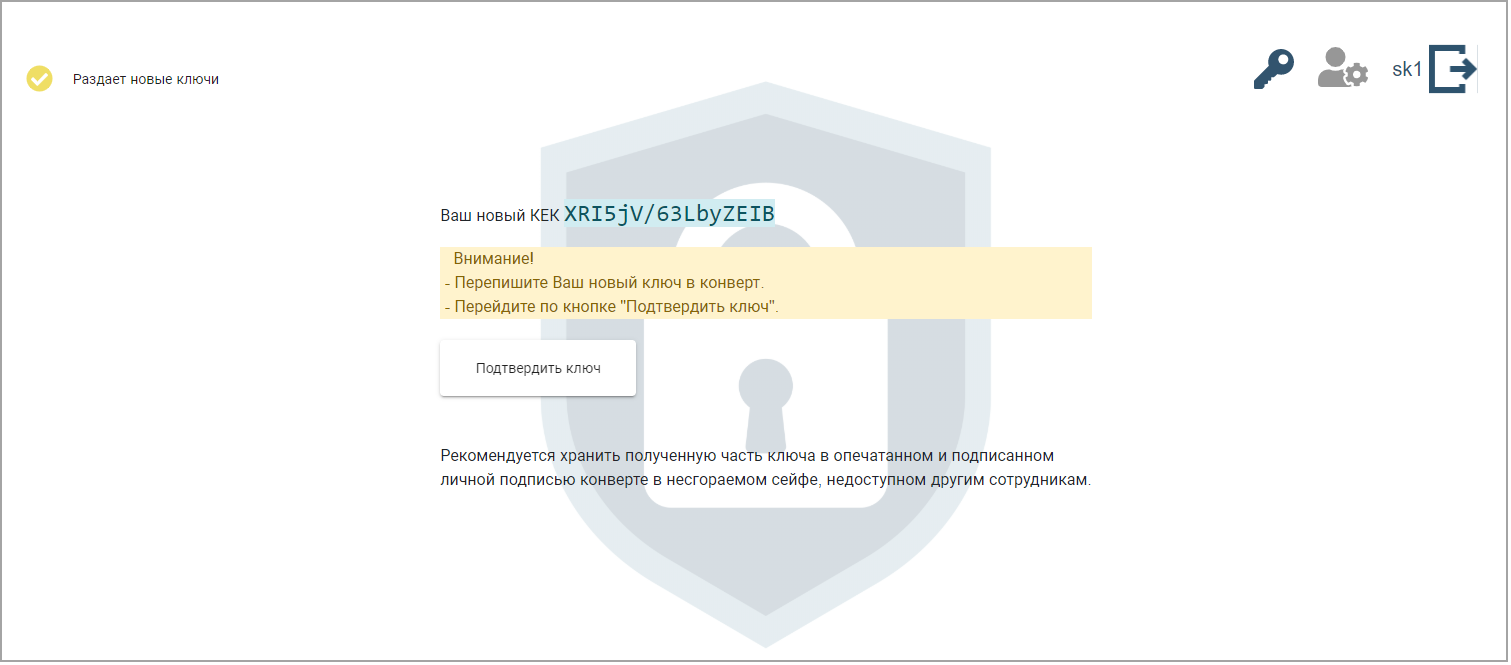


Рис. 26 Страница хранителя ключа, получение нового КЕК

На странице будет выведено значение, которое необходимо запомнить/сохранить, на странице также находится подсказка с рекомендациями по сохранению ключа.

***Шаг 2.*** Скопируйте и сохраните полученную часть секрета.

|  |  |
| --- | --- |
| info_button_32 | Рекомендуется хранить полученную часть ключа в опечатанном и подписанном личной подписью конверте в несгораемом сейфе, недоступном другим сотрудникам |

***Шаг 3.*** Для подтверждения получения части секрета нажмите на кнопку Подтвердить ключ.

На странице хранителя будет отображено поле подтверждения нового ключа КЕК.

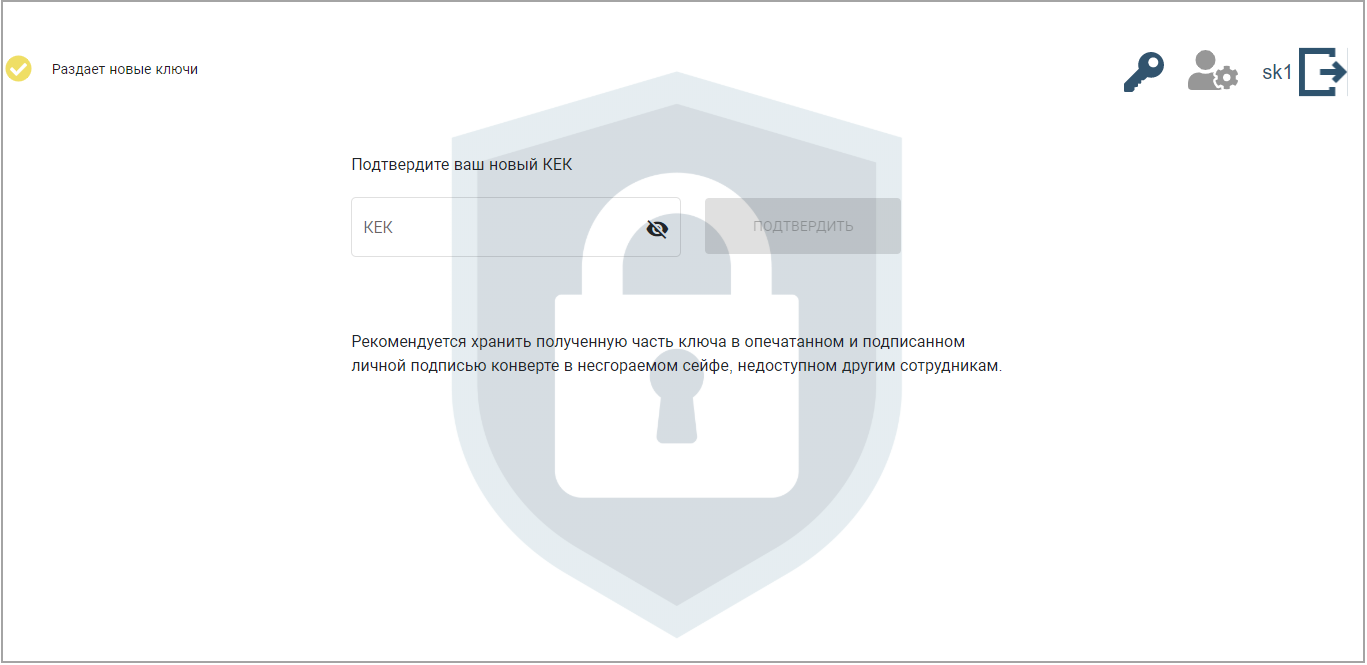


Рис. 27 Страница хранителя ключа, подтверждение нового ключа

***Шаг 4.*** Введите значение КЕК и нажмите на кнопку **Подтвердить**.

* При неправильном вводе ключа будет выведено сообщение об ошибке.

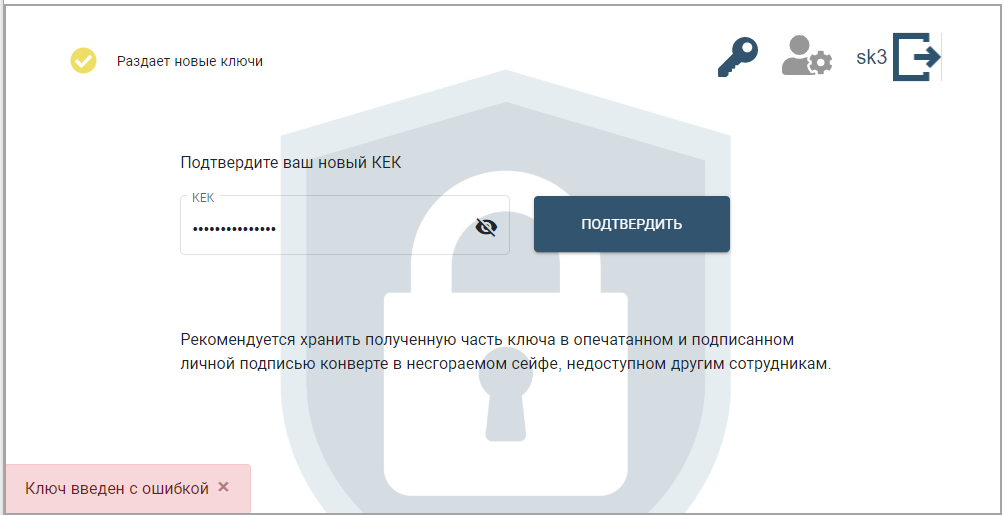


Рис. 28 Страница хранителя ключа, сообщение об ошибке подтверждения ключа

Введите верное значение нового КЕК.

* При правильном вводе части секрета будет выведено сообщение о его успешном подтверждении.



Рис. 29 Страница хранителя ключа, успешное подтверждение KEK

|  |  |
| --- | --- |
| info_button_32 | При перешифровке данных в ЛК хранителя отображается значок соответствующего режима работы ПО СКЗД    Рис. 30 Страница хранителя ключа, режим перешифровывания данных |

Ввод хранителем действующего ключа КЕК

***Шаг 1.*** После перезапуска ПО СКЗД необходимо ввести действующий ключ КЕК. На странице хранителя отобразится поле для его ввода.

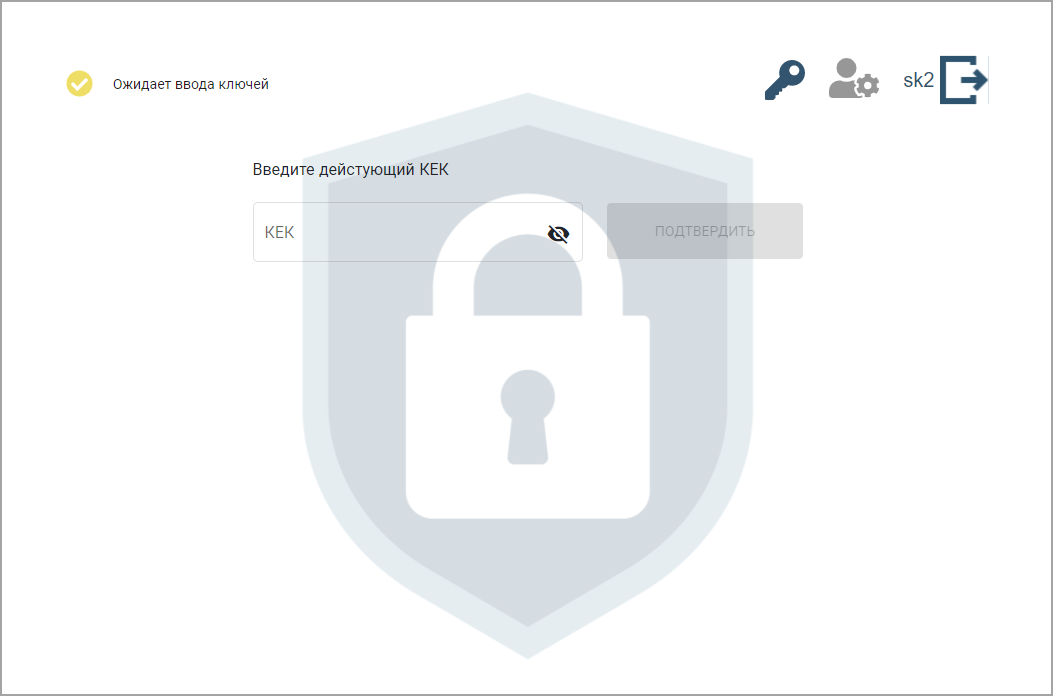


Рис. 31 Страница хранителя ключа, ввод действующего ключа

***Шаг 2.*** Введите действующее значение КЕК и нажмите на кнопку **Подтвердить**.

* При неправильном вводе ключа КЕК окно не закроется и будет выдано сообщение об ошибке.
* При правильном вводе ключа КЕК окно будет закрыто. Будет отображено сообщение об успешном введении части секрета.

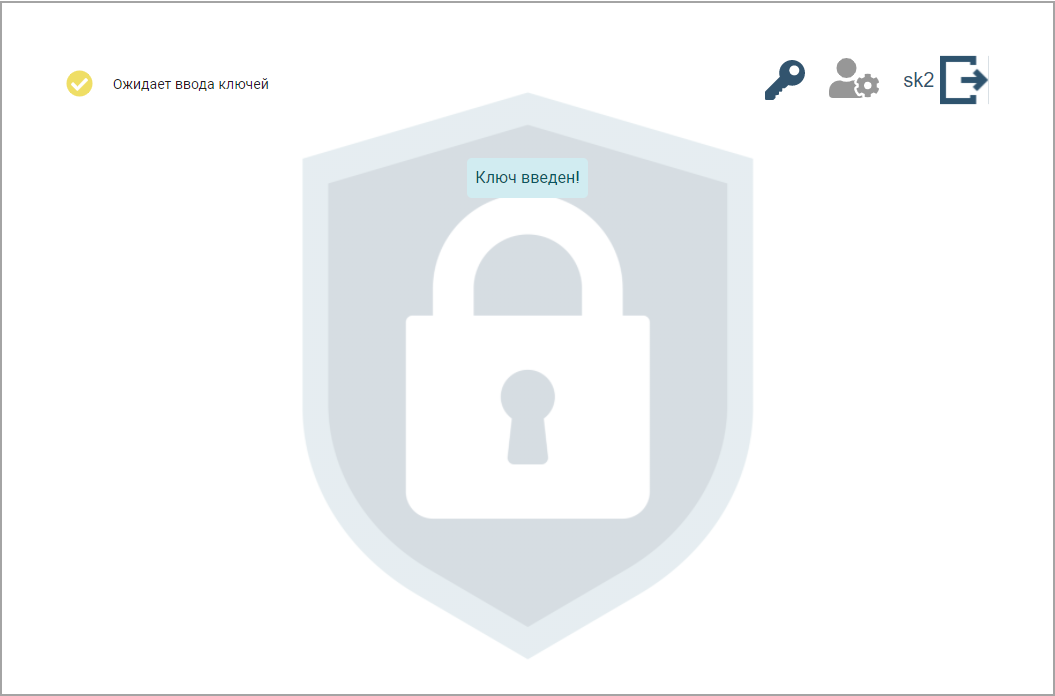


Рис. 32 Страница хранителя ключа, успешный ввод части секрета

Если части секрета были введены верно хотя бы тремя хранителями, секрет успешно восстанавливается, ПО СКЗД переходит в состояние «Работает в обычном режиме».

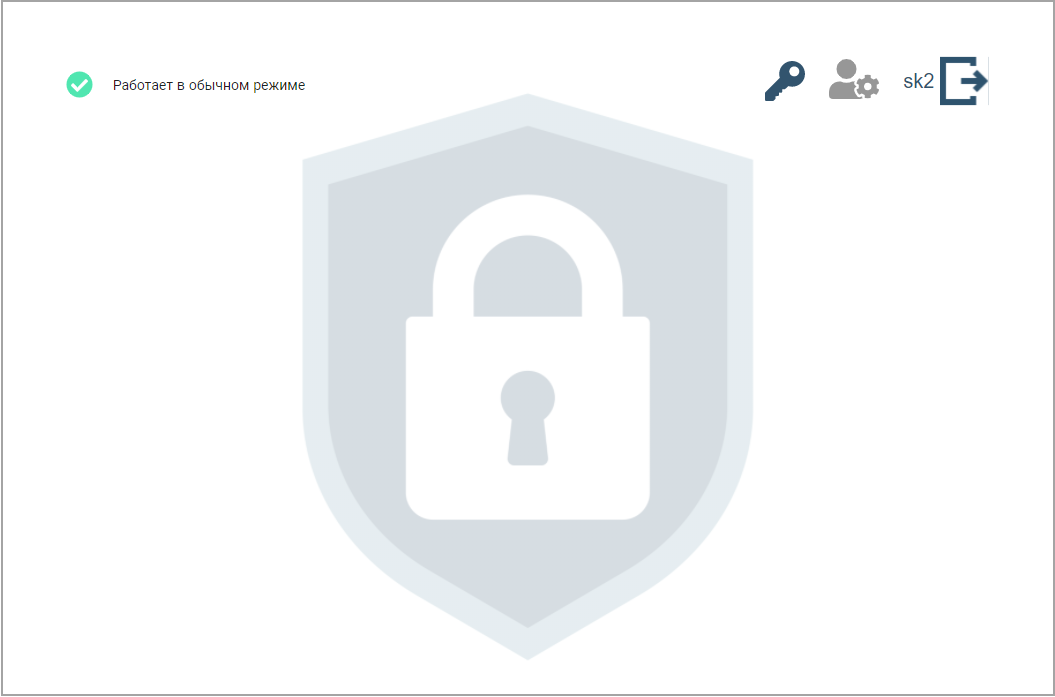


Рис. 33 Страница хранителя ключа при успешном восстановлении секрета

# ВЗАИМОДЕЙСТВИЕ АРМ 407-П С ПО СКЗД

АРМ 407-П при работе с ПО СКЗД позволяет

* Принимать только зашифрованные запросы Росфинмониторинга в АРМ, после расшифрования выделять из них номера банковских карт (PAN), отправлять их на ПО СКЗД для шифрования;
* отображать РАN, сохраненные в БД ПО СКЗД, в маскированном виде при просмотре запросов и выводе их на печать.

|  |  |
| --- | --- |
| info_button_32 | При попытке принять запрос в расшифрованном виде отображается окно с сообщением: *«При работе с системой криптографической защиты данных прием запросов должен осуществляться только в зашифрованном виде».*  Прием запроса при этом не осуществляется |

## Настройка АРМ для работы с ПО СКЗД

Распакуйте файл **cryptoserver.cfg** из дистрибутивав **%Каталог АРМ%\Config**.

Чтобы настроить АРМ 407-П для работы с ПО СКЗД, откройте в папке %Каталог АРМ%\Config файл **cryptoserver.cfg** на редактирование и введите (отредактируйте) строку с адресом, по которому устанавливается соединение АРМ   
с ПО СКЗД:

CryptoServerURL=<протокол>://<адрес сервера>:<порт>/secure-store/

<адрес сервера> – IP адрес или доменное имя компьютера, на котором установлено ПО СКЗД

<протокол> - по умолчанию http  
<порт> - порт указанный ранее в секции **<** **socket-binding-group >,** для <socket-binding name="http" port=

## Требования к лицензии

Для работы с ПО СКЗД АРМ 407 требуется особая лицензия.

|  |  |
| --- | --- |
| info2.png | По вопросам приобретения лицензии обращайтесь в службу технической поддержки **АО «Комита»**:   * по телефону 8 (812) 578–01–96; * по адресу электронной почты [5780196@comita.ru](mailto:5780196@comita.ru) |

## Авторизация в ПО СКЗД

Авторизация пользователя в ПО СКЗД производится после авторизации и входа в АРМ 407-П. Откроется окно регистрации.

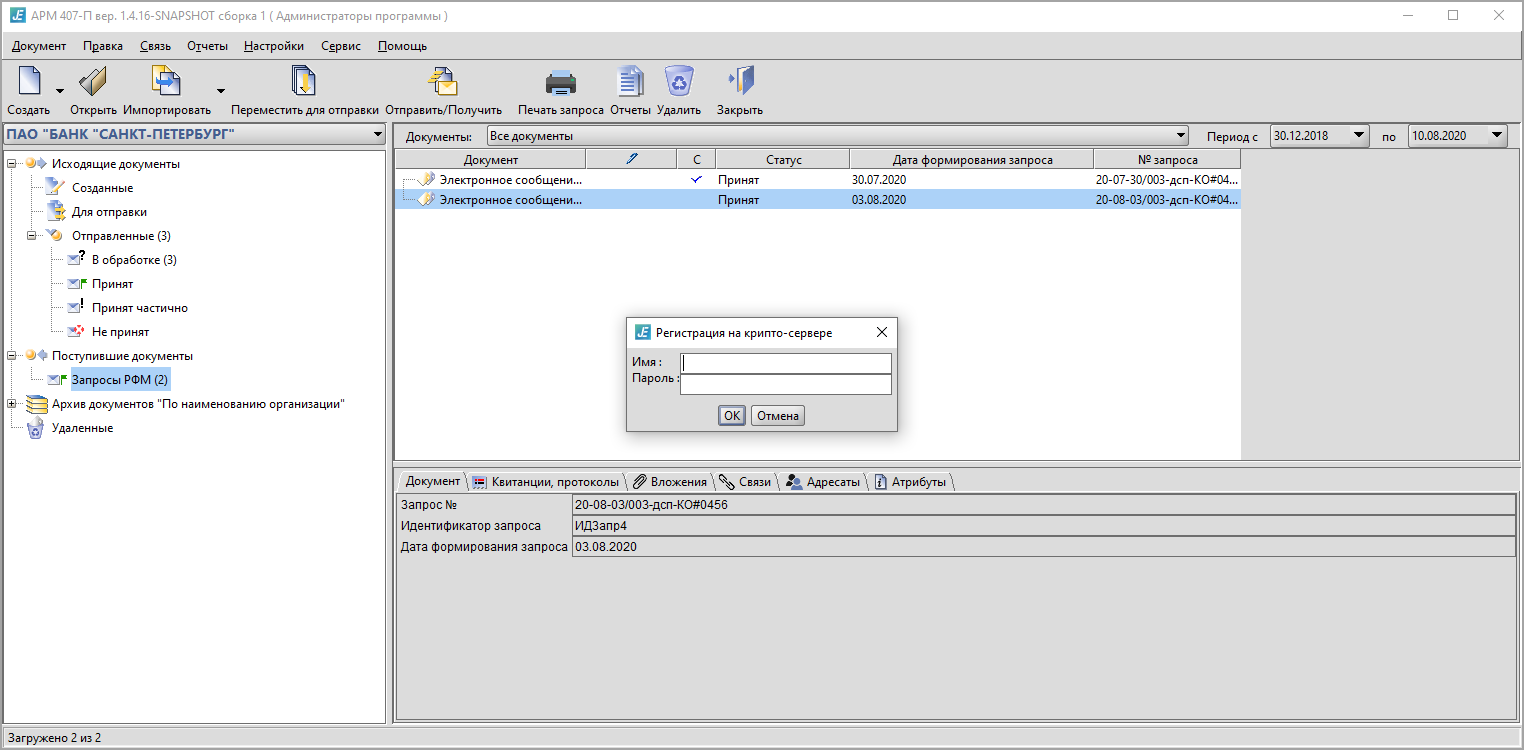


Рис. 33 Авторизация в ПО СКЗД после входа в АРМ

Для авторизации на ПО СКЗД введите имя пользователя и пароль, выданный администратором ПО СКЗД, нажмите ОК.

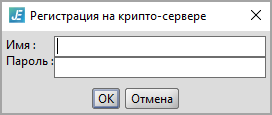


Рис. 34 Окно авторизации в ПО СКЗД

|  |  |
| --- | --- |
| info_button_32 | При нажатии в окне регистрации на кнопку **Отмена** появится окно предупреждения.    Рис. 35 Окно подтверждения работы без ПО СКЗД  Нажмите **ОК**. При этом работу с АРМ можно продолжить только без применения ПО СКЗД.  При получении запросов, открытии запросов на просмотр или печать, пользователю будет повторно предложено авторизоваться в ПО СКЗД |

При успешной авторизации пользователя работа в АРМ будет продолжена с применением системы криптографической защиты. Значения PAN в запросах при их просмотре, выводе на печать будут отображаться в маскированном виде (с заменой символов номера карты с 7-го по 12-й на символы (\*), например, 482173\*\*\*\*\*\*9058).

## Изменение пароля

Пароль пользователя должен быть изменен при первом использовании и по истечении 90 дней его использования.

|  |  |
| --- | --- |
| info_button_32 | После 15-минутного простоя сеанс работы пользователя с ПО СКЗД прерывается с требованием повторного ввода пароля для разблокировки |

Пароль можно изменить как [через интерфейс ПО СКЗД](#_Смена_пароля_пользователем) , так и через интерфейс АРМ (порядок замены аналогичен).

Для смены пароля в АРМ:

***Шаг 1***. Вызовите меню **Сервис → Сменить пароль пользователя cryptoserver.**

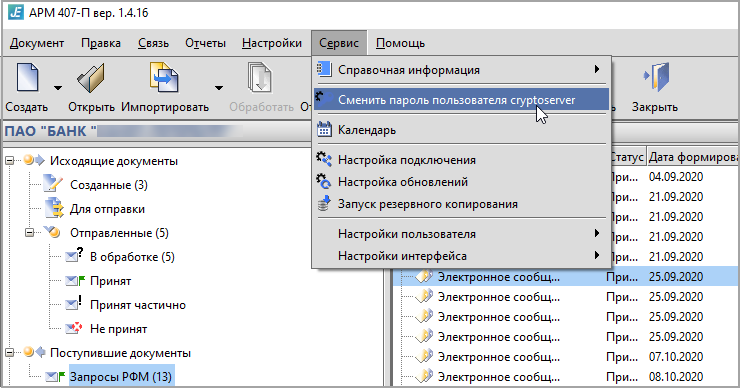


Рис. 36 Меню **Сервис → Сменить пароль пользователя cryptoserver**

Откроется окно *«Установка пароля»*.

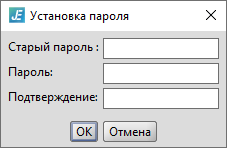


Рис. 37 Окно «Установка пароля»

***Шаг 2*.** Введите текущий пароль в поле **Старый пароль**: и новый пароль в поле **Пароль**: повторите ввод в поле **Подтверждение**: и нажмите на кнопку OK.

|  |  |
| --- | --- |
| info_button_32 | Пароль может содержать цифры от 0 до 9 и латинские символы верхнего регистра от А до Z и нижнего регистра от a до z. Размер пароля должен составлять от 8 до 30 символов |

Если пароли введены верно, окно закроется, новый пароль будет установлен с сообщением об этом в окне *«Информация»*.

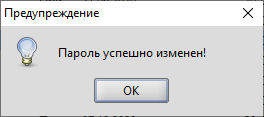


Рис. 38 Окно «Информация»

***Шаг 3.*** Нажмите на кнопку ОК. В результате окно закроется, и операция смены пароля будет успешно завершена.

# ЛОГИРОВАНИЕ СИСТЕМЫ

В системе протоколируются (логируются) события в таблице **log** БД ПО СКЗД.

Логируются следующие события:

* Вход в систему пользователя (любого типа);
* Блокировка пользователя;
* Выход из системы;
* Изменение данных о пользователе;
* Ввод части секрета хранителем ключа;
* Инициация смены КЕК;
* Получение и подтверждение части секрета;
* Формирование DEK;
* Инициация процесса перешифрования данных;
* Шифрование PAN;
* Расшифрование PAN.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

* **АРМ** – автоматизированное рабочее место;
* **БД** – база данных;
* **ЛК** – личный кабинет пользователя;
* **ПО** – программное обеспечение
* **PAN** – номер банковской карты;
* **DEK** – ключ шифрования PAN;
* **KEK** – ключ шифрования ключей DEK;
* **Хранитель ключа** – пользователь, владеющий частью секрета для восстановления КЕК;
* **AES** (**Advanced Encryption Standard**) – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования США;
* **Режим ECB** – простейший режим работы блочного симметричного алгоритма, применяемый для шифрования небольших объемов данных;
* **Стандарт PA-DSS (Payment Application Data Security Standard)** – стандарт безопасности данных в платёжных приложениях – документ, определяющий требования к приложениям, обрабатывающим данные о держателях карт.