LANKEY

Руководство пользователя

Версия 1.0

Оглавление

ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ 3
ТЕРМИНЫ И АББРЕВИАТУРЫ 4
ЛИСТ ИЗМЕНЕНИЙ 6
ВВЕДЕНИЕ 7
1. РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА 8
1.1 Работа с операторами 8
1.1.1 Создание и редактирование пользователя 9
1.1.2 Изменение текущей учетной записи 11
1.2 Настройка системы 12
2. РАБОЧЕЕ МЕСТО ОПЕРАТОРА КОНТРОЛЯ РИСКОВ 13
2.1 Банковские хосты 13
2.2 Просмотр списка терминалов 14
2.3 Менеджмент ключей 15
2.4 Изменение состояния ключей 15
2.4.1 Изменение статуса ключей из внешнего файла 16
2.4.2 Изменение статуса ключей через WEB интерфейс 16
2.5 Контроль работы сервера 17
2.6 Изменение текущей учетной записи 19
3. РАБОЧЕЕ МЕСТО ОПЕРАТОРА ТЕРМИНАЛЬНОЙ СЕТИ 20
3.1 Банковские хосты 20
3.2 Менеджмент терминалов 22
3.3 Регистрация терминалов 22
3.3.1 Регистрация терминалов через WEB интерфейс 22
3.3.2 Регистрация терминалов из внешних файлов 24
3.4 Менеджмент ключей 25
3.5 Загрузка ключей 26
3.6 Изменение состояния ключей 27
3.6.1 Изменение статуса ключей из внешнего файла 27
3.6.2 Изменение состояния ключей через WEB интерфейс 27
3.7 Контроль работы сервера 28
3.8 Изменение текущей учетной записи 30
4. СЕРВИСНЫЕ ФУНКЦИИ РАБОЧИХ МЕСТ ОПЕРАТОРА 32
4.1 Настройки отчетов 32

4.2 Функции меню настройки 32
4.2.1 Колонки 32
4.2.2 Фильтр 33
4.2.3 Строки на странице 34
4.2.4 Формат 34
4.2.5 Контрольная точка 34
4.2.6 Сохранение и сброс настройки отчета 35
4.2.7 Выгрузить 36
ПРИЛОЖЕНИЕ №1 ТРЕБОВАНИЯ PCI SECURITY VERSION 3.0 37

ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

Таблица 1. Используемые обозначения

Обозначение	Комментарий
Полужирный	Наименование кнопок
Курсив	Наименование пунктов меню, файлов и элементов программного интерфейса на компьютере
⚠	Примечание

ТЕРМИНЫ И АББРЕВИАТУРЫ

Таблица 2. Термины и аббревиатуры

Термины и аббревиатуры	Определение
Банк	Заказчик специального ПО
ГО	Головной офис
KMS	Key Management System – приложение SV Система учета и генерации криптографических ключей
S/N	Серийный номер POS-терминала
POS	POS-терминал, эквайером которого является банк, для установки в ПВН банка или в ТСП
SV	Хост банка
CMS	Бэк-офис банка
RKI	Remote Key Injection – программное обеспечение, вендора POS-терминалов, обеспечивающее удаленную загрузку TMK в POS
Raptor	Сервер приложений, который используется для взаимодействия с HSM с целью генерации криптографических ключей
Stunnel	SSL/STL сервер
TMK	Terminal Master Key – мастер-ключ терминала, под которым проводится обмен рабочими ключами
ZMK	Zone Master Key – ключ DES, которым шифруются ключи TMK, используемые для обмена информацией между двумя субъектами. ZMK используется для передачи TMK на RKI
LMK	Local Master Key – локальный мастер-ключ, представляющий собой ключ верхнего уровня, который используется и хранится в HSM
HSM	Программно-аппаратный модуль безопасности, который генерирует наборы секретных криптографических ключей для последующей загрузки в целевое устройство
ДТС	Департамент терминальной сети
ДРТ	Департамент развития технологий
ДП	Департамент процессинга
ДКР	Департамент контроля рисков
СЗК/KDH	Система Загрузки Ключей (LANKEY)
ПС	Платежные системы (МПС, НСПК, VPAY) или операции on-us в межхосте
Single Merchant	Мерчант, у которого для каждого POS используется отдельный Terminal_ID

Термины и аббревиатуры	Определение
Multi Merchant	Мерчант, у которого для одного POS используется несколько Terminal_ID
TermId	Основной внутренний идентификатор терминала в SV
Terminal_ID	Основной уникальный параметр, по которому: • осуществляется регистрация POS в TMS • осуществляется установка конфигурации, а также взаимодействие POS с СЗК
Host_ID	Уникальный идентификатор хоста внутри банка
Key_ID	Уникальный идентификатор TMK в банке
Check value	Проверочное значение ключа TMK или ZMK
ЖЦ	Жизненный цикл
СГК	Банковский скрипт генерации ключей
GUI	Graphical user interface – графический пользовательский интерфейс
MFT	Managed File Transfer – управляемая передача файлов на базе ПО EFT Server Enterprise компании GlobalScape. Это решение может работать FTP/SFTP/FTPS сервером и запускать по расписанию или иному виду событий какой-либо исполняемый файл
TMS	Система параметризации POS-терминалов

ЛИСТ ИЗМЕНЕНИЙ

Таблица 3. Лист изменений

Версия	Дата	Автор	Детали
1.0	15.06.2023	Лисайчук Ф.В.	Создание документа

ВВЕДЕНИЕ

Настоящее руководство, разработанное компанией «Лантер», подробно описывает специфику работы СЗК (LANKEY). Цель документа – обучение пользователей работе с программным обеспечением LANKEY.

1. РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА

Рабочее место Администратора осуществляет следующие функции:

- Заведение и менеджмент операторов системы СЗК
- Регистрация новых пользователей, распределение функционала
- Изменение учетных записей операторов, сброс и назначение паролей
- Настройка сервера СЗК
- Настройка ключевых параметров сервера
- Настройка сетевых параметров сервера.

Доступ к рабочему месту Администратора осуществляется через WEB-сервис. Во время инсталляции системы создается пользователь с правами администратора (логин: admin, пароль: admin). После успешной установки пользователь с правами администратора заходит в систему с логином и паролем по умолчанию (в дальнейшем пароль можно поменять).

1.1 Работа с операторами

После входа в систему открывается список операторов системы. В системе предусмотрены следующие типы операторов:

- Администратор
- Оператор ТС (Терминальной Сети)
- Оператор КР (Контроля Рисков)
- Аудитор.

Каждому типу оператора в системе предусмотрены права, соответствующие его роли.

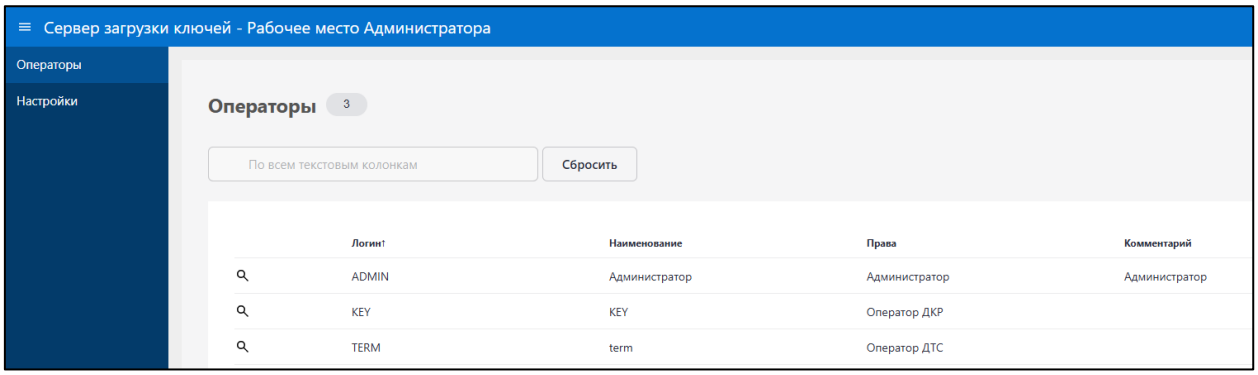


Рисунок 1. Меню операторы

1.1.1 Создание и редактирование пользователя

Для регистрации нового оператора нажмите кнопку **Создать**. Откроется карточка *Редактирование пользователя*.

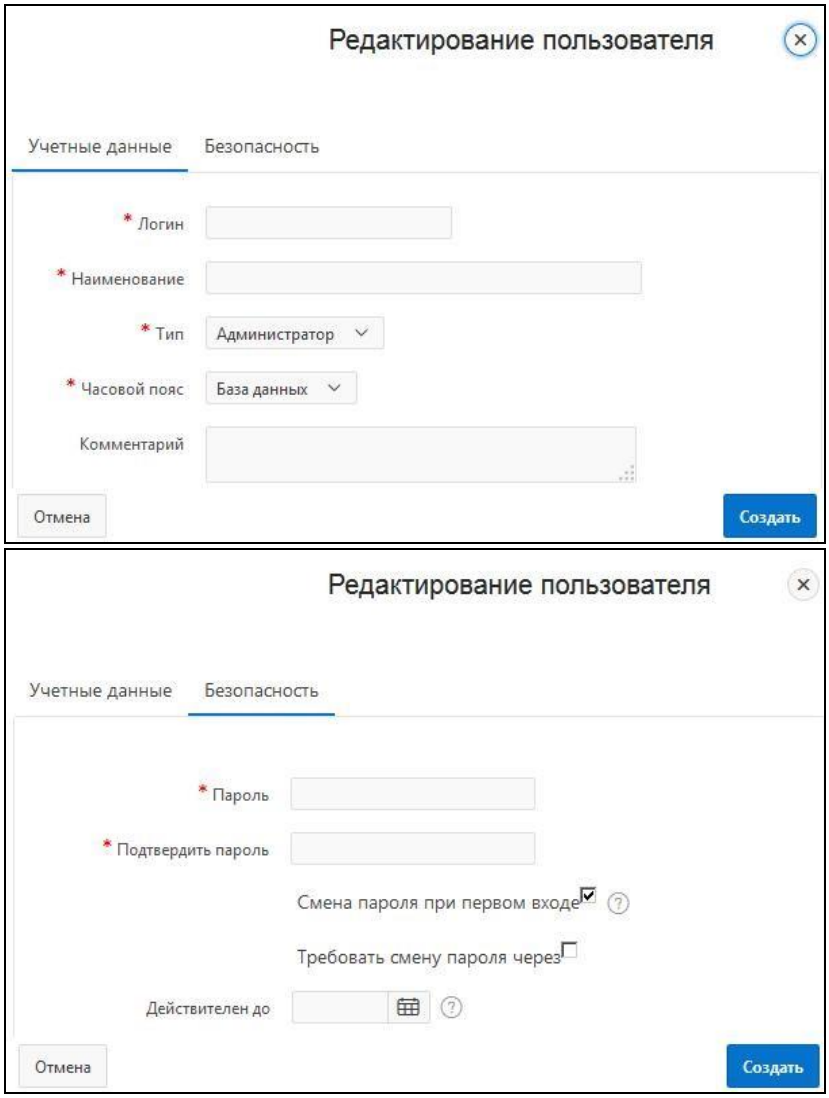


Рисунок 2. Карточка Редактирование пользователя

Таблица 4. Описание параметров карточки Редактирование пользователя

Вкладка		Описание
Учетные данные		На этой вкладке вносятся основные данные по пользователю
	Логин	Имя оператора для аутентификации
	Наименование	Имя оператора для отображения
	Тип	Тип оператора с разделением прав работы в системе
	Часовой пояс	Часовой пояс, в котором работает оператор. Нужен для корректного отображения временных данных. По умолчанию принимается часовой пояс БД
Безопасность		На этой вкладке вносятся данные по аутентификации пользователя при входе в систему
	Пароль	Пароль для входа в систему должен содержать алфавитно-цифровые символы в различных регистрах. Допускаются символы только английского алфавита и спец.символы. Пароль должен иметь длину не менее шести символов
	Подтвердить пароль	Подтверждение введенного ранее пароля
	Смена пароля при первом входе в систему	Если данная опция выбрана, то при первом входе в систему под данным логином или при смене пароля, система потребует смену пароля. Эта функция нужна при регистрации нового оператора или при сбросе утерянного пароля, чтобы оператор ввел собственный пароль
	Требовать смену пароля	При выборе данной функции система будет требовать смену пароля через указанный промежуток времени
	Действителен до	Если указана дата, то она определяет срок, до которого данная учетная запись оператора будет действительна. После истечения указанного срока, учетная запись будет не доступна. Если дата не указана, то учетная запись будет актуальна всегда

Для редактирования учетной записи оператора необходимо нажать по кнопке  в списке операторов. Откроется карточка *Редактирование пользователя*, в которой будет небольшое отличие во вкладке *Безопасность*.

На данной вкладке можно сбросить текущий пароль для выбранного оператора и ввести новый для входа в систему. При первом входе в систему после сброшенного пароля пользователю будет предложено сменить пароль.

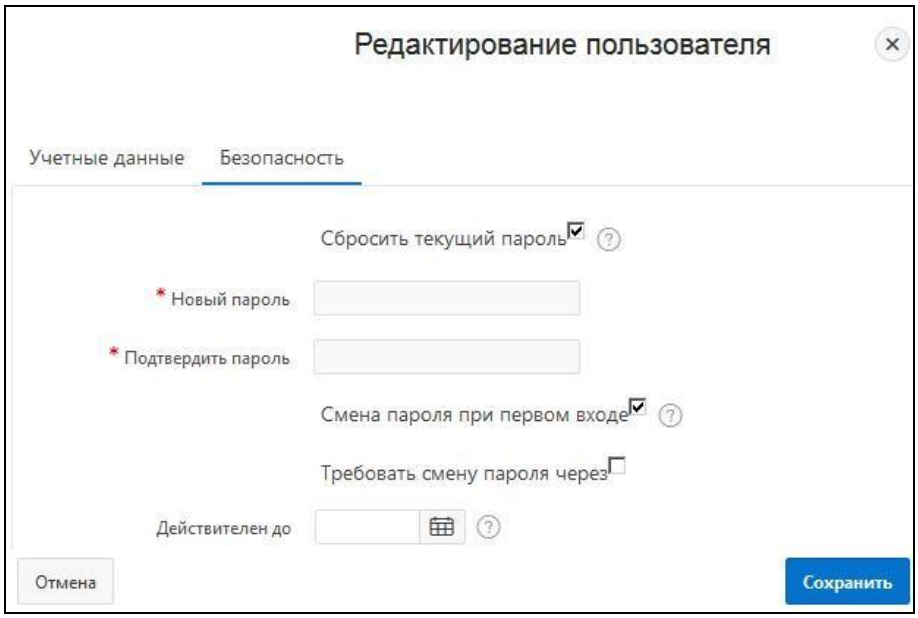


Рисунок 3. Сброс пароля в карточке Редактирование пользователя

1.1.2 Изменение текущей учетной записи

Изменить свой пароль и некоторые данные оператор может через форму *Изменение учетных данных*.

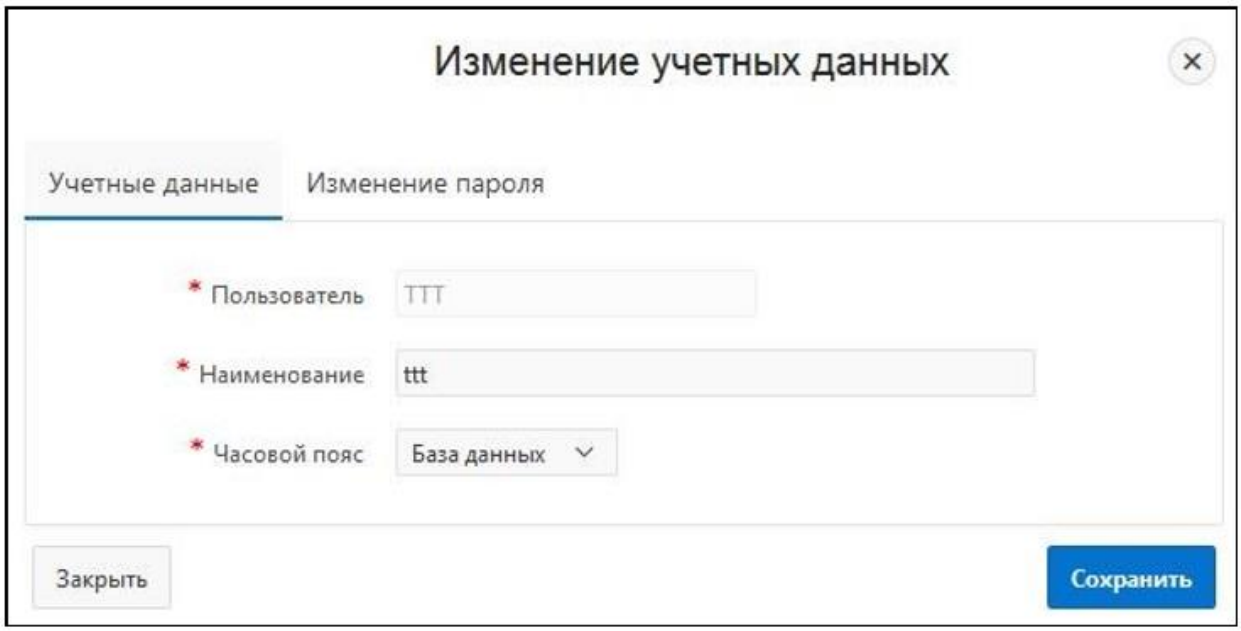


Рисунок 4. Изменение учетных данных

Для изменения пароля введите во вкладке *Изменение пароля* текущий пароль, а затем новый пароль с подтверждением.

1.2 Настройка системы

В меню *Настройки* задаются ключевые и сетевые параметры системы.

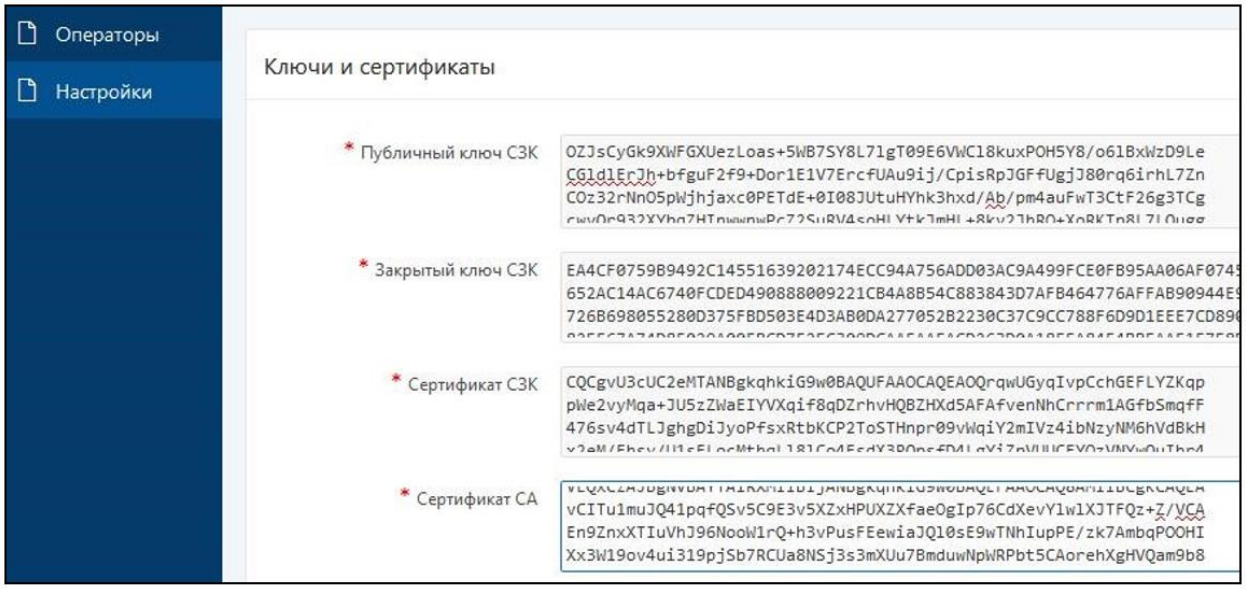


Рисунок 5. Меню Настройки

После инсталляции системы необходимо сформировать *Публичный ключ СЗК* и *Закрытый ключ СЗК*. Данная процедура выполняется с помощью кнопки **Перевыпустить ключи СЗК**. *Сертификат СЗК* и *Сертификат СА* необходимо получить у вендора терминалов. Для доступа к HSM определяют его адрес и порт. В системе предусмотрено два HSM: один основной, второй резервный. Для определения основного HSM используется переключатель.

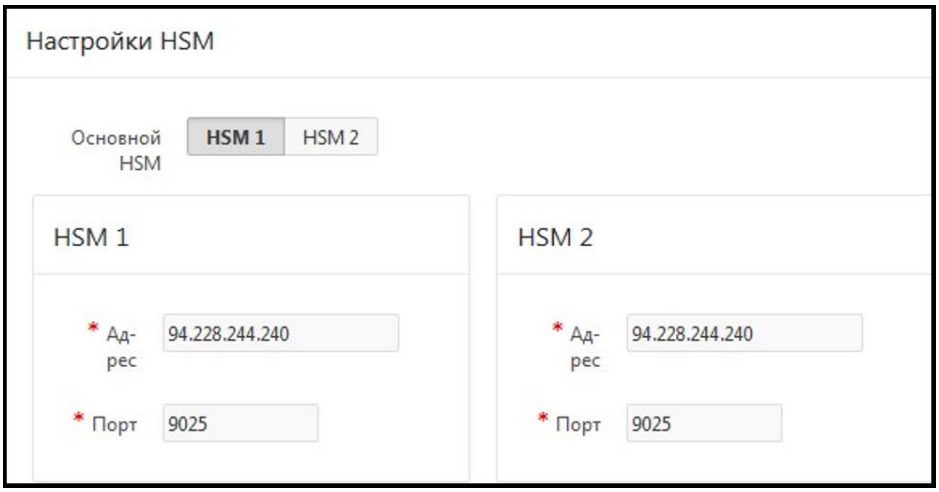


Рисунок 6. Настройки HSM

2. РАБОЧЕЕ МЕСТО ОПЕРАТОРА КОНТРОЛЯ РИСКОВ

Рабочее место оператора ДКР определяет следующие функции:

- Просмотр справочника хостов
- Просмотр терминалов
- Менеджмент состояния ключей
  - Просмотр текущего состоянии ключей с фильтрами по каждому полю
  - Изменение состояния ключей (загрузка состояния ключей ТМК из внешнего файла, редактирование состояния ключа через WEB интерфейс)
- Контроль работы сервера по функциям загрузки ключей.

Доступ к рабочему месту оператора ДКР осуществляется через WEB-сервис.

2.1 Банковские хосты

Для работы со списком банковских хостов необходимо выбрать пункт меню *Хосты*.

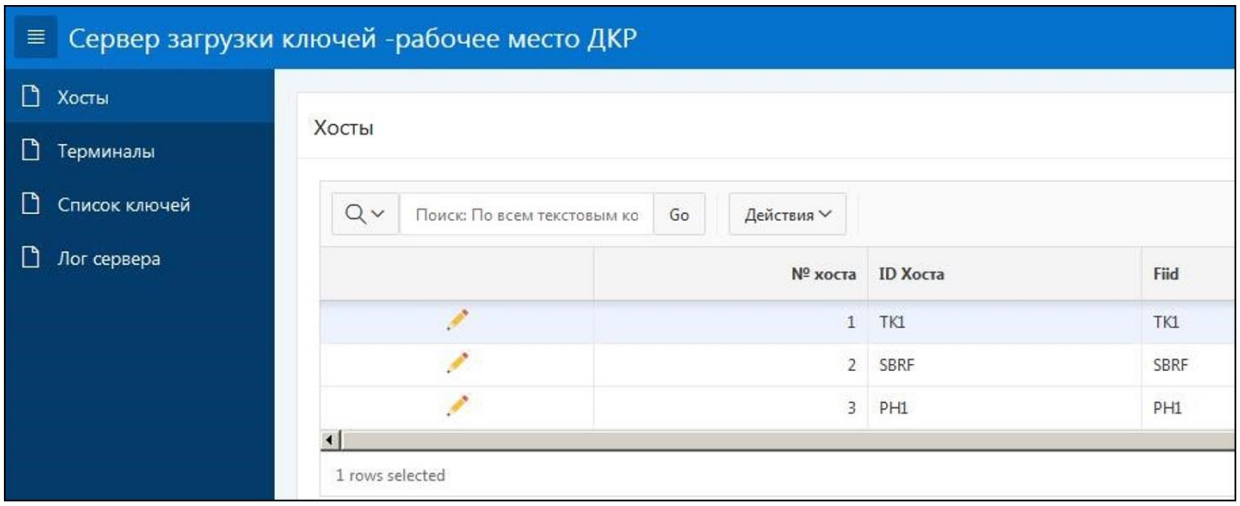


Рисунок 7. Меню Хосты

Для редактирования профиля хоста необходимо нажать значок  слева от записи. Откроется карточка *Редактирование хоста*.

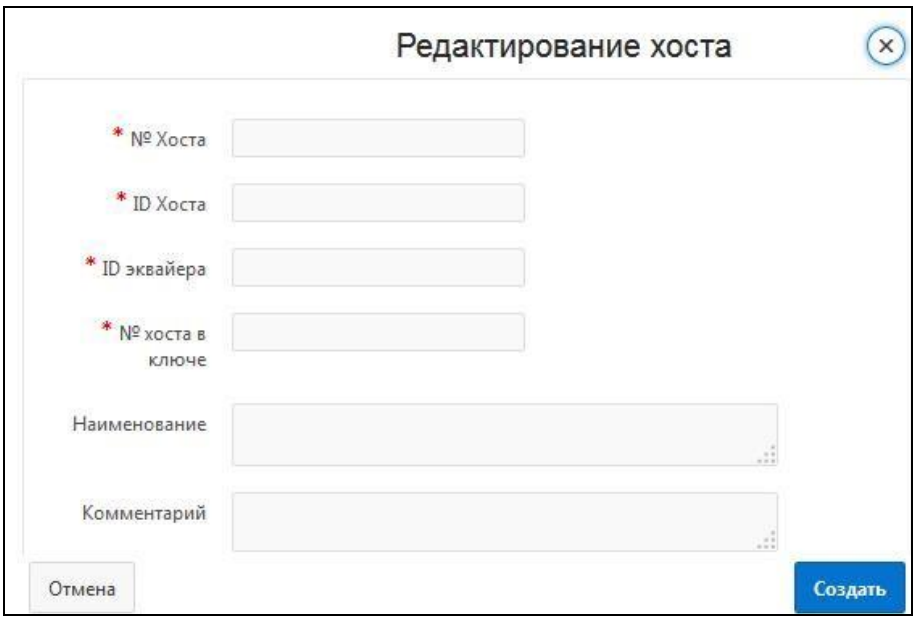


Рисунок 8. Карточка Редактирование хоста

В ней для редактирования доступен только параметр *Комментарий*.

2.2 Просмотр списка терминалов

Для работы со списком терминалов необходимо выбрать пункт меню *Терминалы*.

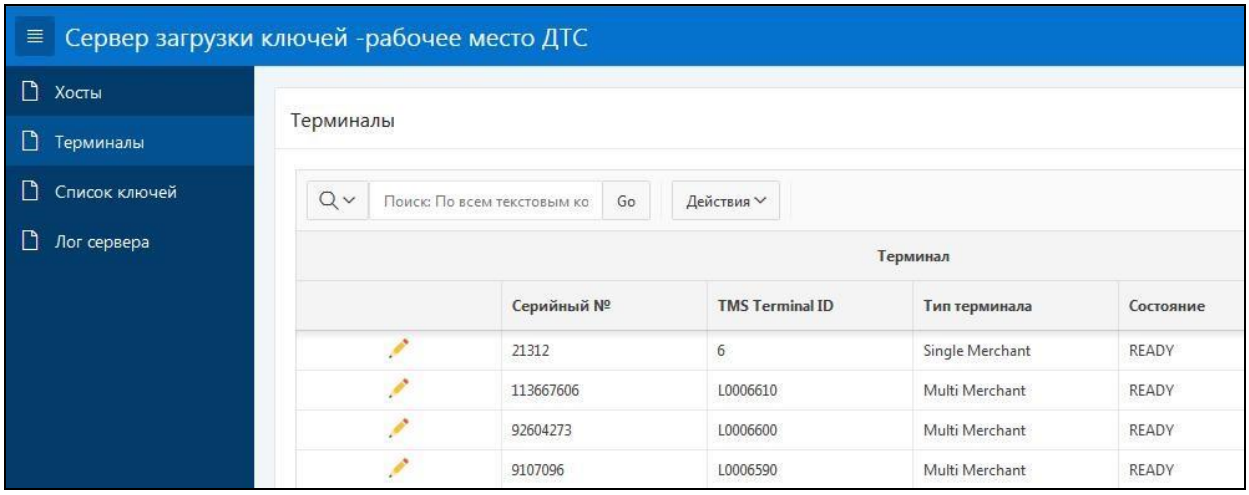


Рисунок 9. Меню терминалы

Для формирования списков терминалов или поиска по каждому полю можно построить фильтры. Для этого необходимо нажать мышкой по заголовку поля. После этого выпадет список доступных значений для определения фильтра по данному полю. После выбора требуемого значения список терминалов модифицируется относительно установленного фильтра.

2.3 Менеджмент ключей

Для работы с ключами необходимо выбрать пункт меню *Список ключей*.

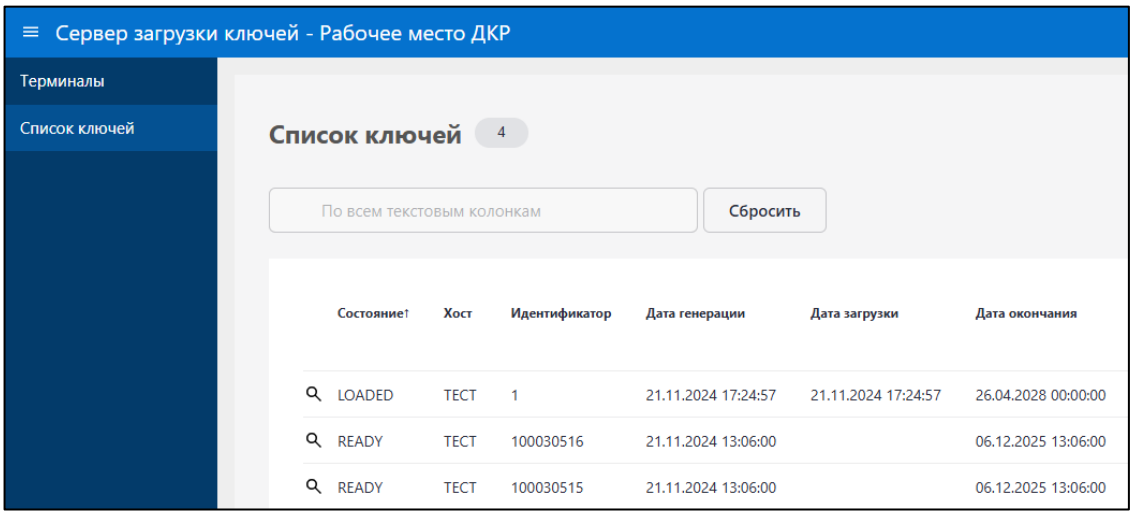


Рисунок 10. Меню Список ключей

Для формирования списков ключей или поиска, по каждому полю можно настроить фильтры. Для этого необходимо нажать мышкой по заголовку поля. После этого выпадет список доступных значений для определения фильтра по данному полю.

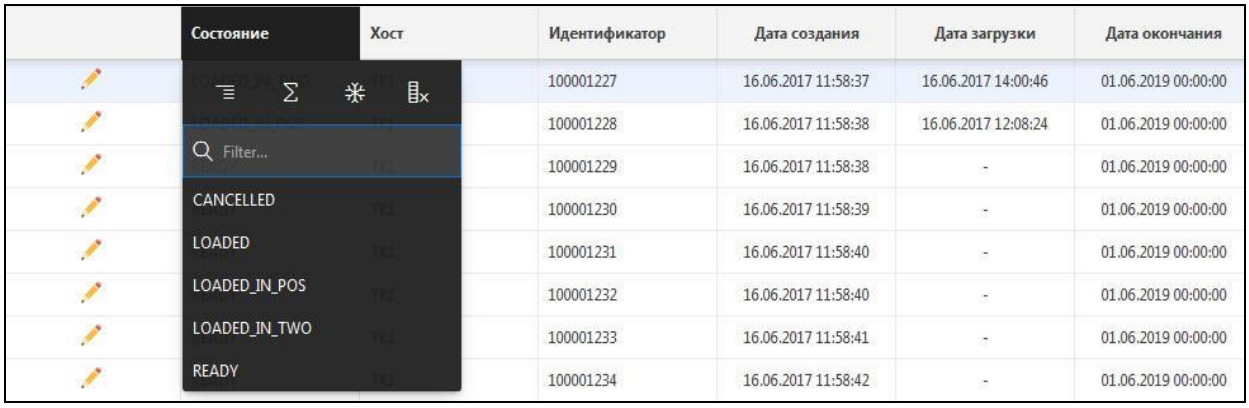


Рисунок 11. Настройка фильтров

После выбора требуемого значения список ключей модифицируется относительно установленного фильтра.

2.4 Изменение состояния ключей

По мере жизни статус ключа может меняться автоматически. Для принудительного изменения статуса ключа существуют два способа:

- Загрузка статуса ключей из внешнего файла

- Изменение статуса через WEB интерфейс.

2.4.1 Изменение статуса ключей из внешнего файла

Изменение статуса выполняется с помощью кнопки **Загрузка файла состояния ключей**. При нажатии этой кнопки откроется окно для выбора файла со списком состояния ключей.

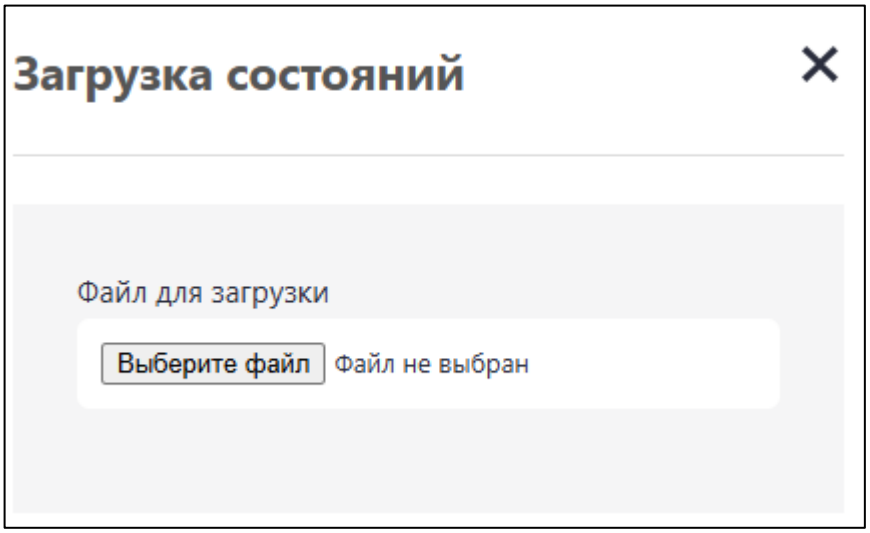


Рисунок 12. Загрузка файла состояния ключей

После выбора файла необходимо нажать кнопку **Загрузить файл статусов ключей**.

2.4.2 Изменение статуса ключей через WEB интерфейс

Для изменения статуса ключей через WEB интерфейс необходимо нажать мышкой по кнопке редактирования слева от записи ключей. При этом появляется форма редактирования информации по ключу.

Изменения доступны как для ключей TMK, так и ZMK. На вкладке *Информация по ключу* можно проконтролировать текущее состояние ключа и основные его параметры. Если не установлен флажок *Запретить отсылку в TWO*, то информация по статусу ключа после сохранения будет передана в TWO. TWO – это система автоматической привязки ключей на авторизационном банковском хосте. На закладке *История ключа* можно посмотреть жизненный цикл состояния ключа.

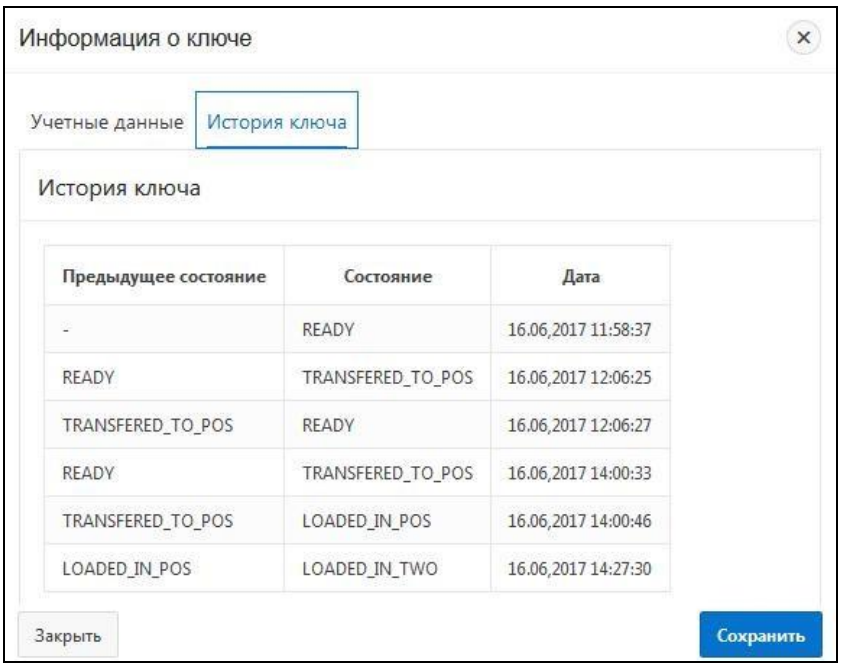


Рисунок 13. Информация о ключе

2.5 Контроль работы сервера

Контроль за работой сервера осуществляется через просмотр логов работы процедур СЗК.

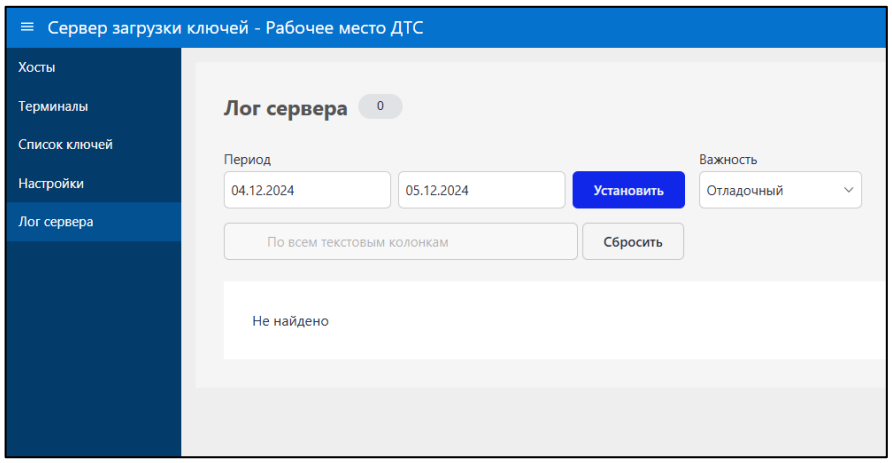


Рисунок 14. Лог сервера

Лог сервера СЗК можно просмотреть за определенный промежуток времени. Промежуток времени можно задать с точностью до секунды. В заголовке отчета задаются поля начальной и конечной дат просмотра. Если в поле даты нажать мышкой по иконке календаря, то появится интерактивное окно установки даты.

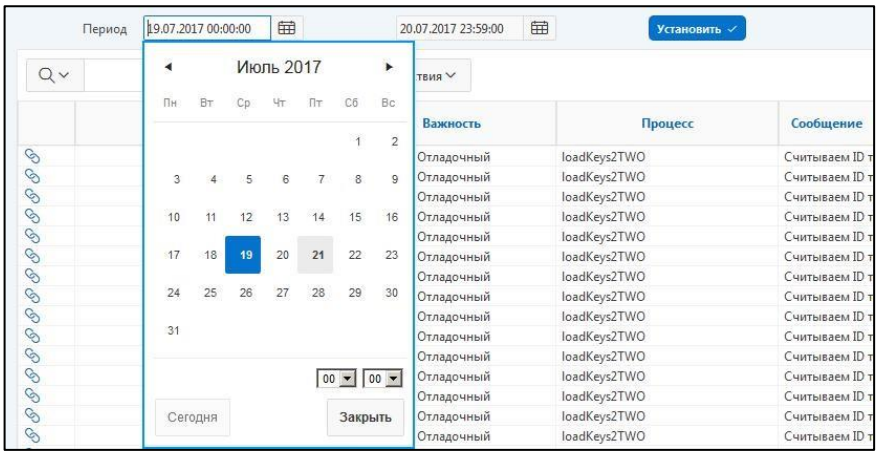


Рисунок 15. Календарь

Для принятия установленной даты в интерактивном окне необходимо щелкнуть по кнопке **Закрыть**. Для обновления отчета после изменения периода просмотра необходимо нажать по кнопке **Установить** в заголовке отчета. В заголовке отчета можно определить список записей лога по критической важности состояния записи.

После выбора состояния список записей лога обновиться автоматически. Для формирования списка лога или поиска по каждому полю можно построить фильтры. Для этого необходимо нажать мышкой по заголовку поля. После этого выпадет список доступных значений для определения фильтра по данному полю. После выбора требуемого значения, список записей лога модифицируется относительно установленного фильтра. Контроль за текущим состоянием ключей можно осуществлять через сводные отчеты, которые появляются на начальной странице при входе в систему.

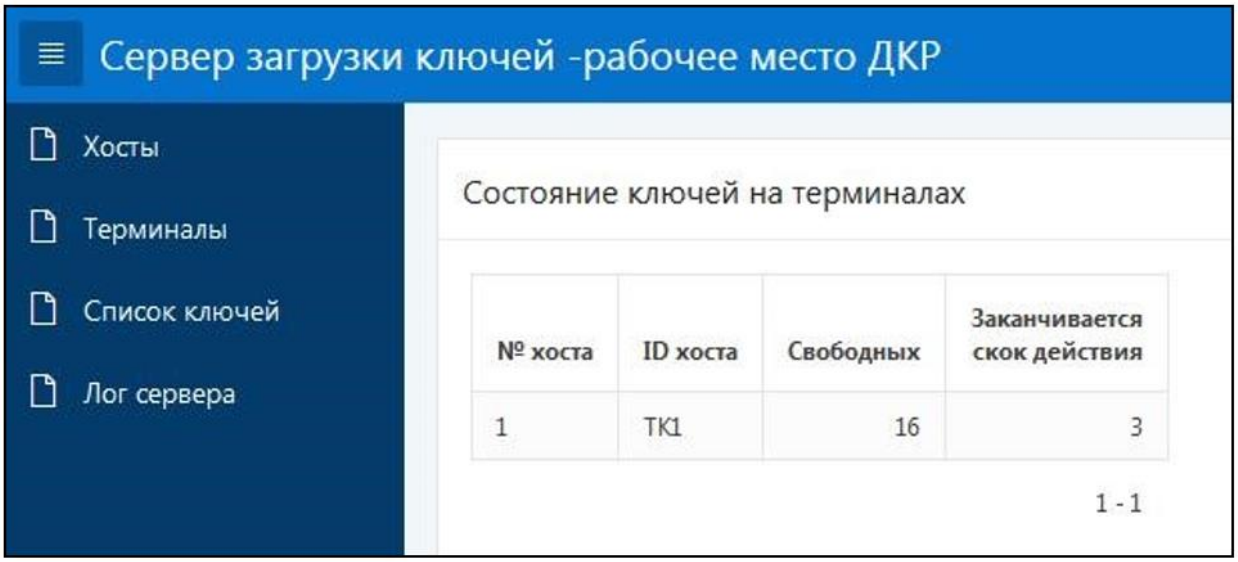


Рисунок 16. Сводные отчеты

2.6 Изменение текущей учетной записи

Изменить свой пароль и некоторые данные оператор может через карточку *Изменение учетных данных*.

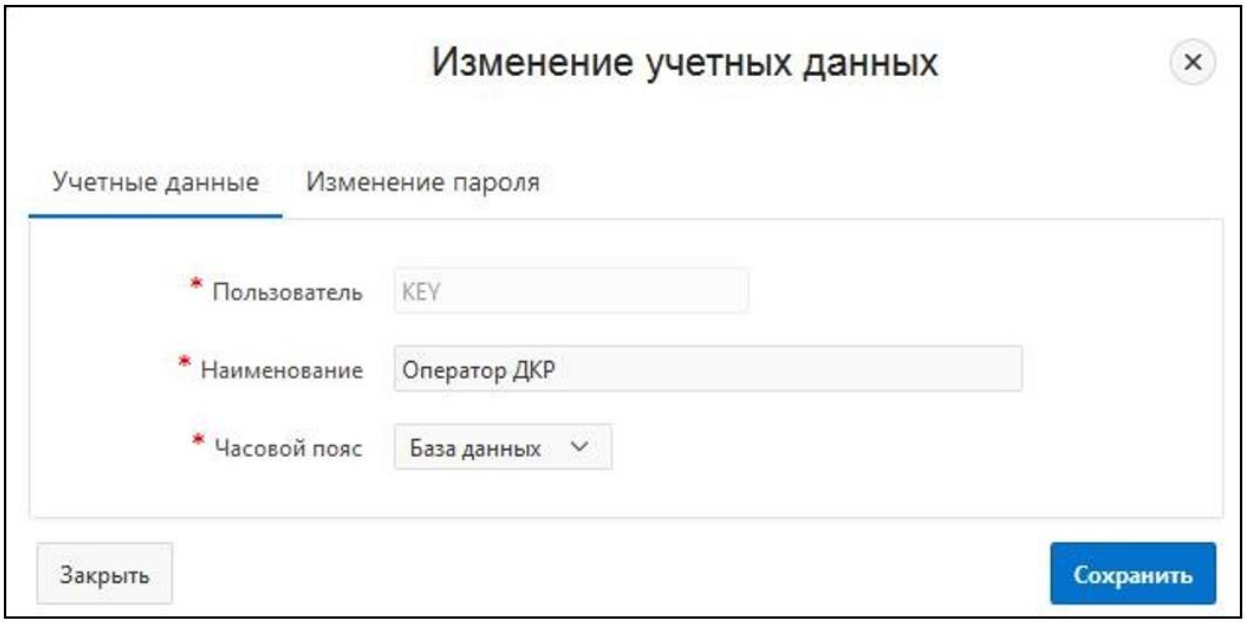


Рисунок 17. Изменение учетных данных

Для изменения пароля введите во вкладке *Изменение пароля* текущий пароль, а затем новый пароль с подтверждением.

3. РАБОЧЕЕ МЕСТО ОПЕРАТОРА ТЕРМИНАЛЬНОЙ СЕТИ

Рабочее место оператора Терминальной Сети определяет следующие функции:

- Ведение справочника банковских хостов
- Менеджмент терминалов
  - регистрация терминалов через WEB интерфейс
  - регистрация терминалов из внешних файлов в виде списков
  - настройка терминалов из внешних файлов в виде списков
  - просмотр списков терминалов и их состояний с фильтрами по полям.
- Менеджмент состояния ключей
  - просмотр текущего состоянии ключей с фильтрами по каждому полю
  - загрузка списка ключей ТМК из внешнего файла
  - изменение состояния ключей (загрузка состояния ключей ТМК из внешнего файла, редактирование состояния ключа через WEB интерфейс)
- Контроль работы сервера по функциям загрузки списков терминалов и состояния ключей.
  - просмотр логов загрузки списков терминалов
  - просмотр логов взаимодействия с терминалами по загрузке ТМК
  - просмотр логов взаимодействия с системой автоматической привязки ключей
  - контроль работы сервера по функциям загрузки ключей.

Доступ к рабочему месту оператора ТС (терминальной сети) осуществляется через WEB-сервис.

3.1 Банковские хосты

Для работы со списком банковских хостов необходимо выбрать пункт меню *Хосты*.

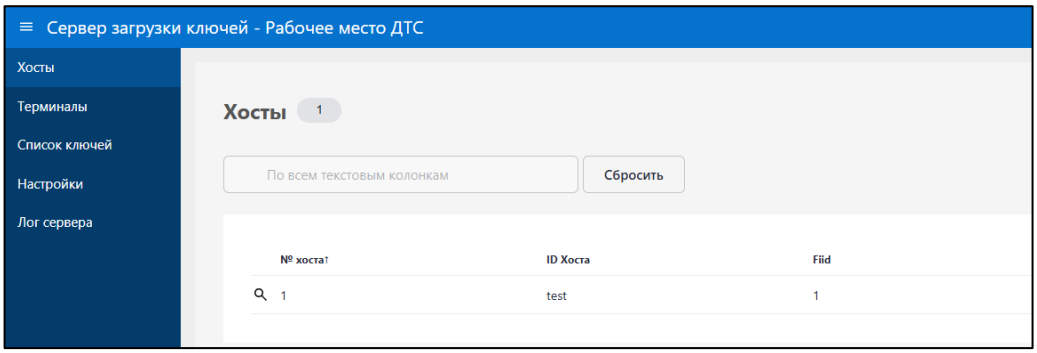


Рисунок 18. Меню Хосты

Для создания нового банковского хоста необходимо нажать кнопку **Создать**. При этом открывается новое окно для ввода данных по банковскому хосту.

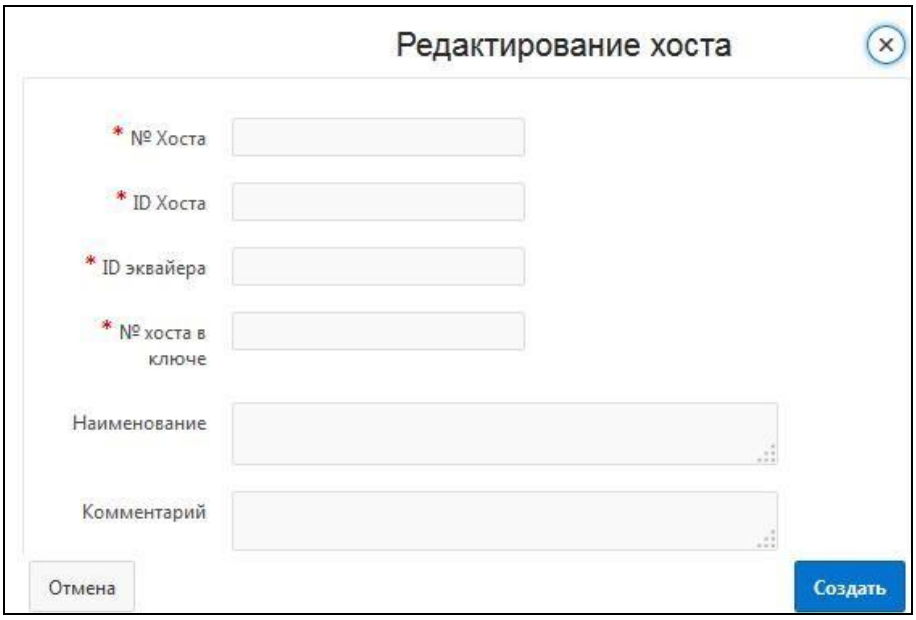


Рисунок 19. Карточка Редактирование хоста

Таблица 5. Параметры карточки Редактирование хоста

Поле	Описание
N Хоста	Номер хоста в системе СЗК
ID Хоста	ИД хоста в банковской системе
ID эквайера	ИД эквайера в банковской системе
N хоста в ключе	Идентификатор хоста в идентификаторе ключа (необходим при создании ключа)

Для редактирования карточки хоста необходимо нажать кнопку слева от записи.

3.2 Менеджмент терминалов

Для работы со списком терминалов необходимо выбрать пункт меню *Терминалы*.

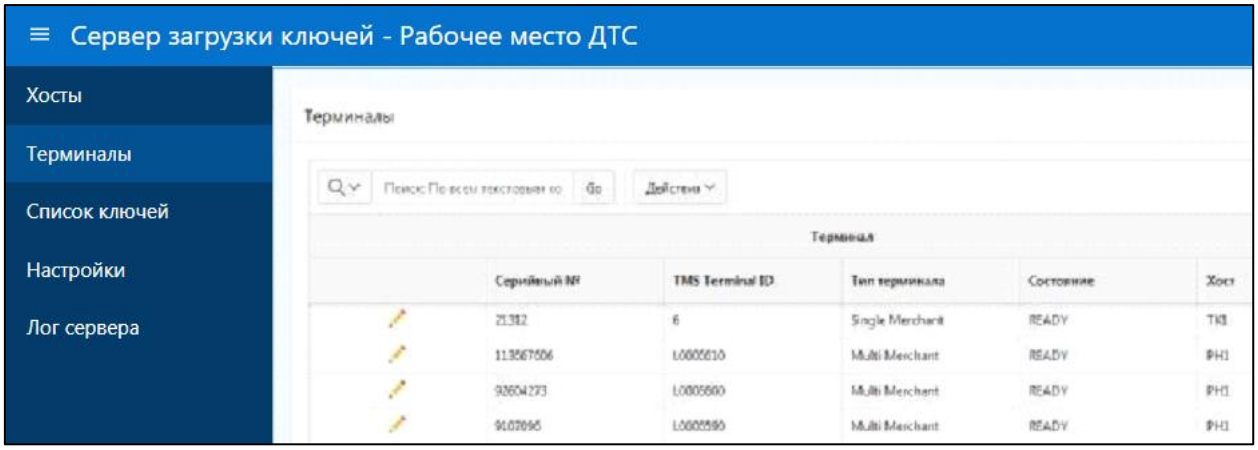


Рисунок 20. Меню Терминалы

Для формирования списков терминалов или поиска по каждому полю можно построить фильтры. Для этого необходимо нажать по заголовку поля. После этого выпадет список доступных значений для определения фильтра по данному полю. После выбора требуемого значения, список терминалов модифицируется относительно установленного фильтра.

3.3 Регистрация терминалов

Терминалы на сервере СЗК можно регистрировать двумя способами:

- Регистрация через WEB интерфейс
- Регистрация терминалов из внешних файлов.

3.3.1 Регистрация терминалов через WEB интерфейс

Для регистрации нового терминала нажмите кнопку **Создать**. Откроется карточка *Редактирование терминала*.

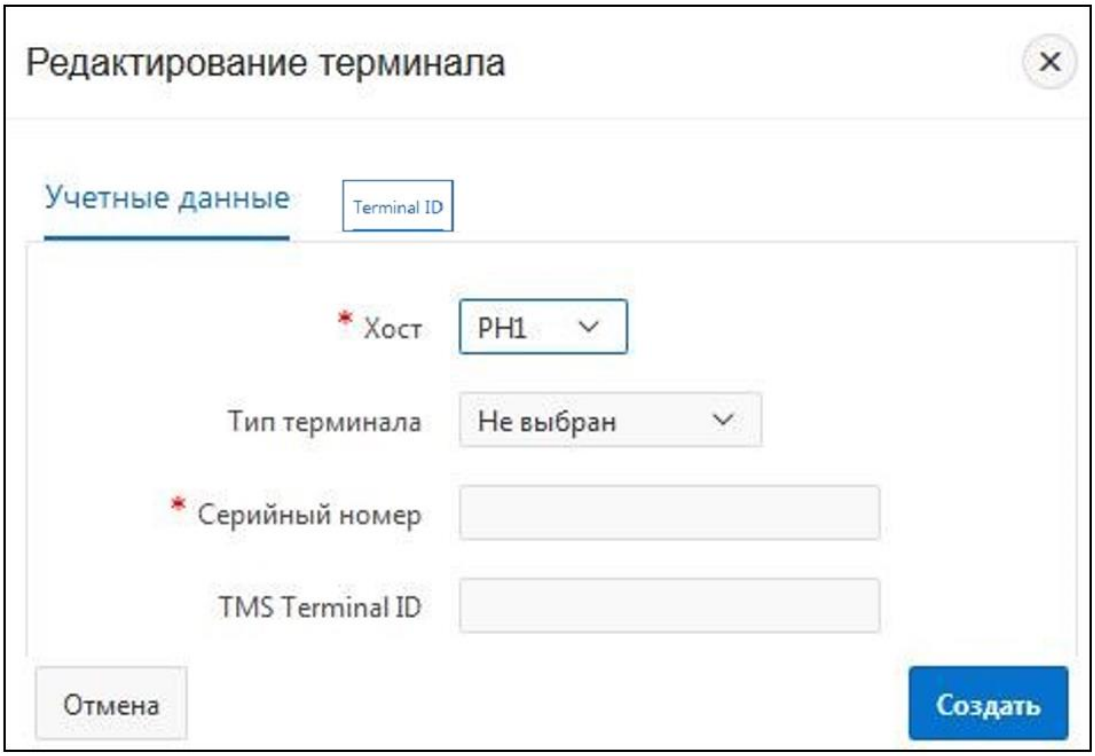
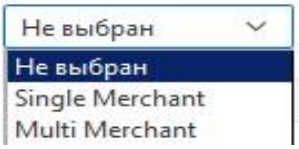


Рисунок 21. Карточка Редактирование терминала

Таблица 6. Параметры карточки Редактирование терминала. Вкладка Учетные данные

Поле	Описание
Хост	Банковский хост, где зарегистрирован терминал
Тип терминала	Тип обслуживания терминалом коммерсантов. Если терминал обслуживает одного коммерсанта, то тип SingleMerchant и терминал имеет один Terminal_ID. Если терминал обслуживает нескольких коммерсантов, то тип MultiMerchant и терминал имеет несколько Terminal_ID.  После выбора типа терминала, появляется закладка Terminal ID, для ввода параметров терминала.
Серийный номер	Серийный номер терминала (пробивается на шилдике терминала)
Terminal ID на ТМС	Идентификатор терминала на ТМС. Может отличаться от Terminal ID на хосте

Параметры вкладки Terminal ID отличаются в зависимости типа терминала.

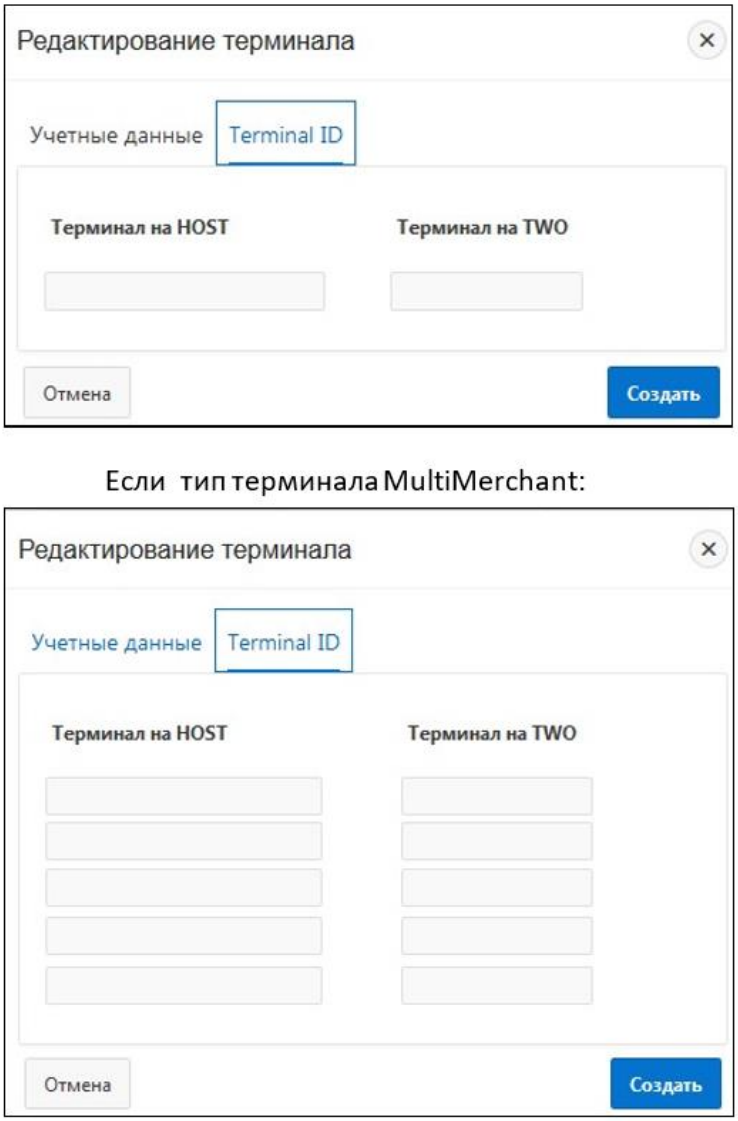


Рисунок 22. Вкладка Terminal ID

- Терминал на Host – Terminal ID зарегистрированный на банковском хосте
- Терминал на TWO – Terminal ID зарегистрированный на TWO.

Для редактирования карточки хоста необходимо нажать кнопку слева от записи. Откроется карточка Редактирование терминала

3.3.2 Регистрация терминалов из внешних файлов

Для регистрации и изменения параметров списком необходимо нажать кнопку **Загрузить файл**. Откроется окно *Загрузка файла*.

Есть два типа формата внешних файлов загрузки:

- Список серийных номеров, когда регистрируются новые терминалы
- Список конфигураций терминалов, когда принимаются параметры конфигурации терминалов. При этом если терминал не зарегистрирован в системе, то происходит регистрация нового терминала.

Для загрузки внешнего файла, необходимо выбрать его через кнопку **Обзор**. Этот файл должен быть доступен с локальной машины, на которой работает оператор ТС (Терминальной Сети). Также необходимо указать тип формата выбранного файла: список серийных номеров или конфигурация POS. После выбора файла необходимо нажать на кнопку **Загрузить**. При этом произойдет обработка файла и результат работы отобразится в окне отчета. После закрытия окна загрузки файла окно списка терминалов модифицируется соответственно изменениям, которые были во внешнем файле.

3.4 Менеджмент ключей

Для работы с ключами необходимо выбрать пункт меню *Список ключей*.

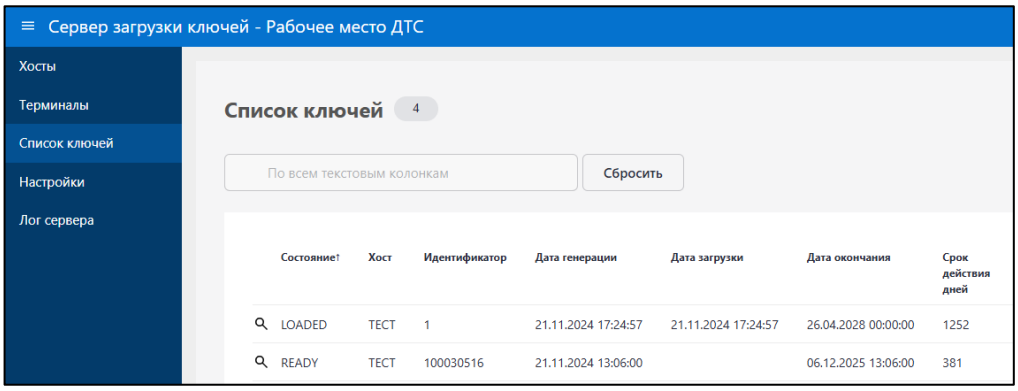


Рисунок 23. Меню Список ключей

Для формирования списков ключей или поиска, по каждому полю можно построить фильтры. Для этого необходимо нажать по заголовку поля. После этого выпадет список доступных значений для определения фильтра по данному полю.

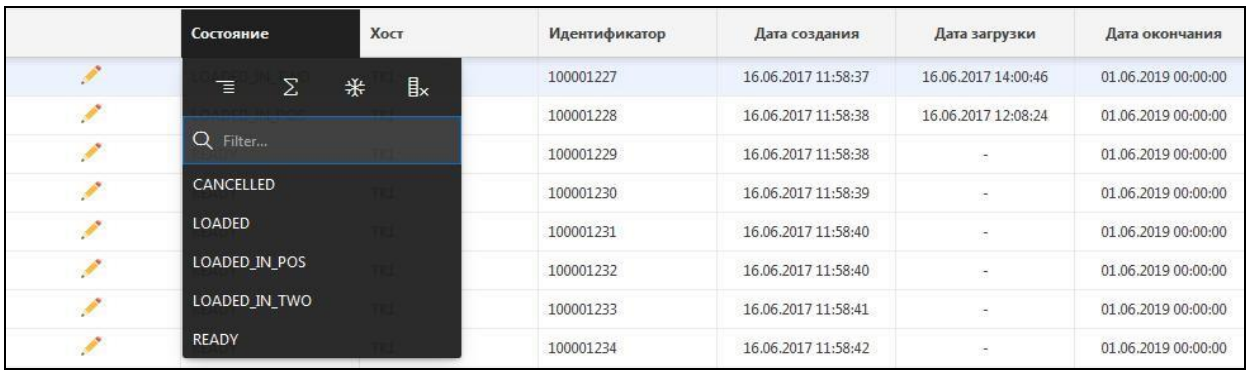


Рисунок 24. Настройка фильтров

После выбора требуемого значения список ключей модифицируется относительно установленного фильтра.

3.5 Загрузка ключей

Ключи ТМК на сервер СЗК загружаются из внешних файлов. Но для загрузки ключа вначале необходимо определить ключ ZMK для банковского хоста. Для этого необходимо нажать кнопку **Ввод ZMK** в заголовке списка ключей. Откроется карточка *Ввод ключа ZMK*.

Таблица 7. Параметры карточки Ввод ключа ZMK

Поле	Описание
Хост	Выбор банковского хоста, для которого необходимо определить ключ ZMK
Идентификатор ключа	Идентификатор ключа должен быть уникален во всем диапазоне ключей, независимо от типа ключа
Значение ключа	Значение ключа ZMK. Ключ должен быть шифрован под LMK HSM СЗК

После сохранения новый ключ ZMK примет статус *LOADED*, а предыдущий, если таковой имелся, сбросится в состояние *CANCELLED*. В дальнейшем статус ключа можно поменять в учетной записи ключа через WEB интерфейс. После создания ключа ZMK для хоста можно загружать список ключей ТМК. Для этого необходимо нажать кнопку **Загрузка ключей из файла**. Далее, выбрать файл и установить срок жизни ключей. После выбора файла и установки срока жизни ключей необходимо нажать кнопку **Загрузить файл ключей**. Будет выполнена обработка файла и её результат будет

выведен на экран. Все новые загруженные ключи перейдут в состояние *READY*.

3.6 Изменение состояния ключей

По мере жизни статус ключа может меняться автоматически. Для принудительного изменения статуса ключа существуют два способа:

- Загрузка статуса ключей из внешнего файла
- Изменение статуса через WEB интерфейс.

3.6.1 Изменение статуса ключей из внешнего файла

Изменение статуса выполняется с помощью кнопки **Загрузка файла состояния ключей**. При нажатии этой кнопки откроется окно для выбора файла со списком состояния ключей.

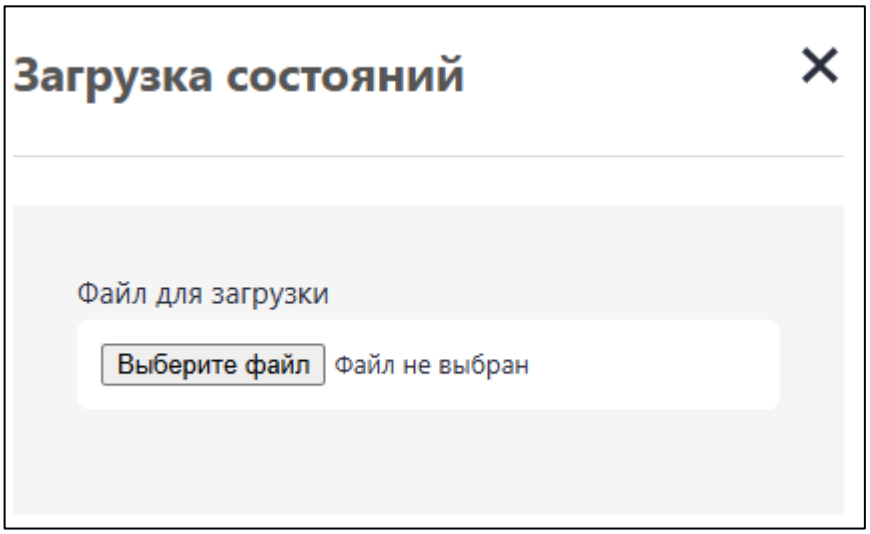


Рисунок 25. Загрузка файла состояния ключей

После выбора файла необходимо нажать кнопку **Загрузить файл статусов ключей**.

3.6.2 Изменение состояния ключей через WEB интерфейс

Для изменения статуса ключей через WEB интерфейс необходимо нажать мышкой по кнопке редактирования слева от записи ключей. При этом появляется форма редактирования информации по ключу.

Изменения доступны как для ключей TMK, так и ZMK. На вкладке *Информация по ключу* можно проконтролировать текущее состояние ключа и основные его параметры. На вкладке *Учетные данные* пользователь может изменить состояние ключа. Для пользователя доступно одно значение *COMPROMISED*. Если не установлен флажок *Запретить отсылку в TWO* (система автоматической привязки ключей на авторизационном банковском хосте), то информация по статусу ключа после сохранения будет передана в TWO. На вкладке *История ключа* доступен для просмотра жизненный цикл состояния ключа.

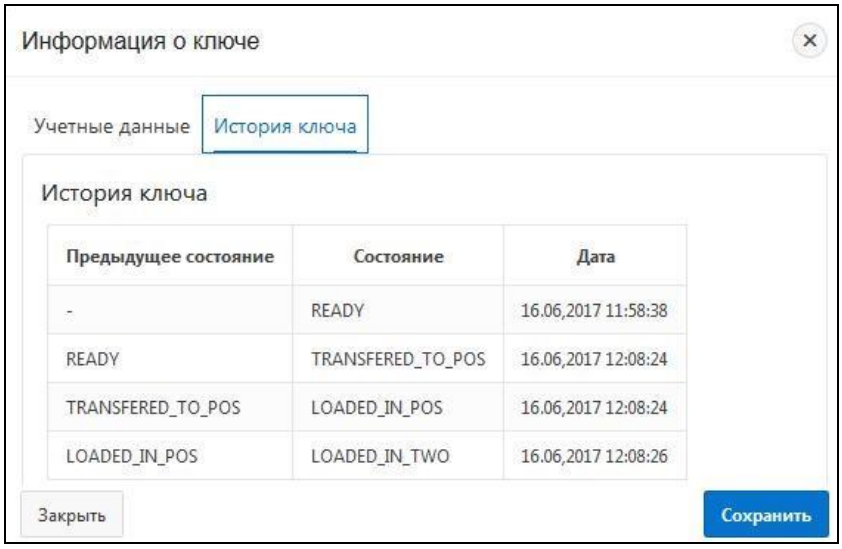


Рисунок 26. Информация о ключе

3.7 Контроль работы сервера

Контроль за работой сервера осуществляется через просмотр логов работы процедур СЗК.

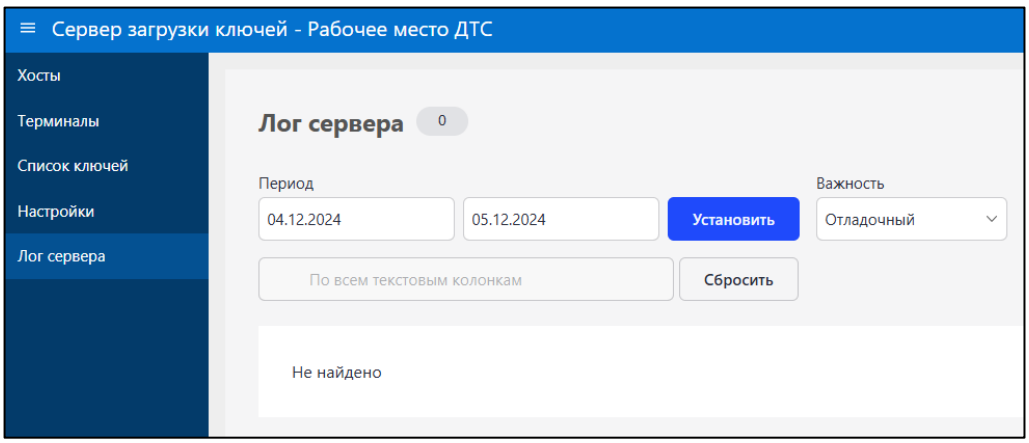


Рисунок 27. Лог сервера

Лог сервера СЗК можно просмотреть за определенный промежуток времени, который можно задать с точностью до секунды. В заголовке отчета задаются поля начальной и конечной дат просмотра. Если в поле даты нажать по иконке календаря, то появится интерактивное окно установки даты.

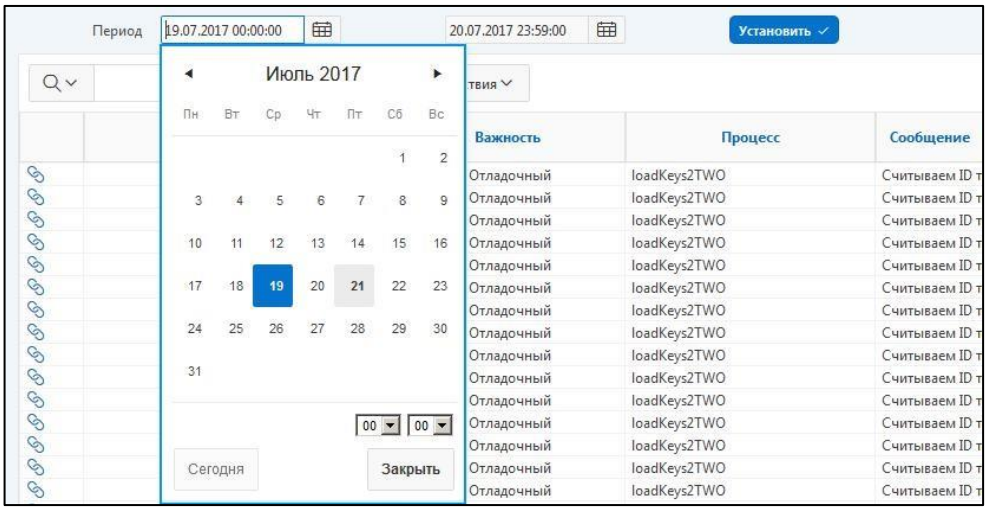


Рисунок 28. Календарь

Для установки выбранной даты в интерактивном окне необходимо щелкнуть по кнопке **Закрыть**. Для обновления отчета после изменения периода просмотра необходимо щелкнуть по кнопке **Установить** в заголовке отчета. В заголовке отчета можно определить список записей лога по критической важности состояния записи. После выбора состояния список записей лога обновится автоматически. Для формирования списка лога или поиска по каждому полю можно построить фильтры. Для этого необходимо нажать по заголовку поля. После этого откроется выпадающий список доступных значений для определения фильтра по данному полю.

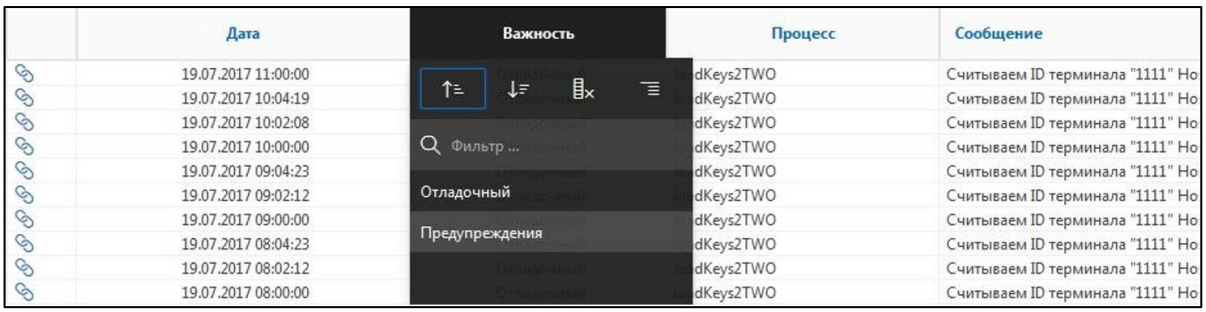


Рисунок 29. Выбор фильтра

После выбора требуемого значения, список записей лога модифицируется относительно установленного фильтра.

Контроль за текущим состоянием терминалов и ключей на терминалах можно осуществлять через сводные отчеты, которые появляются на начальной странице при входе в систему.

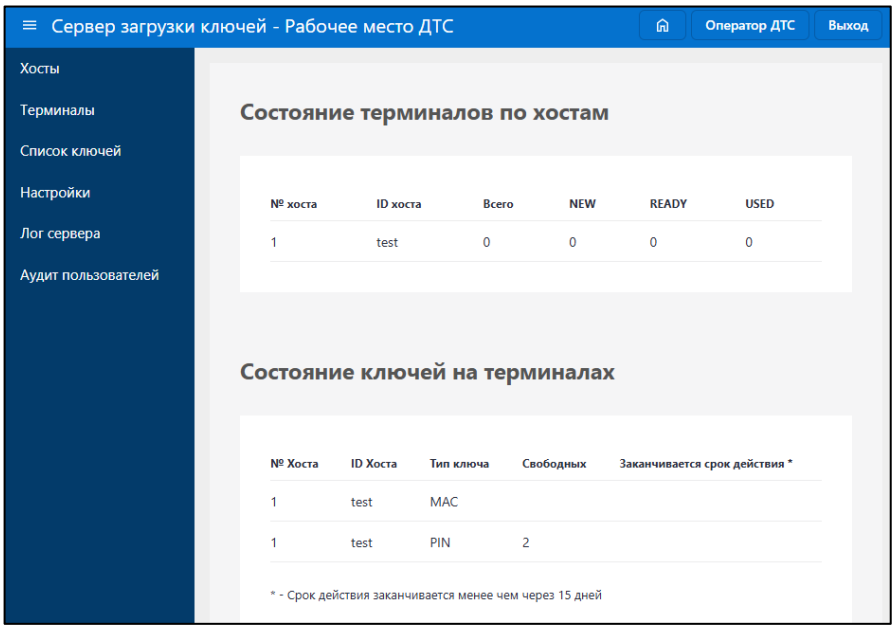


Рисунок 30. Сводные отчеты

3.8 Изменение текущей учетной записи

Изменить свой пароль и некоторые данные оператор может через карточку *Изменение учетных данных*.

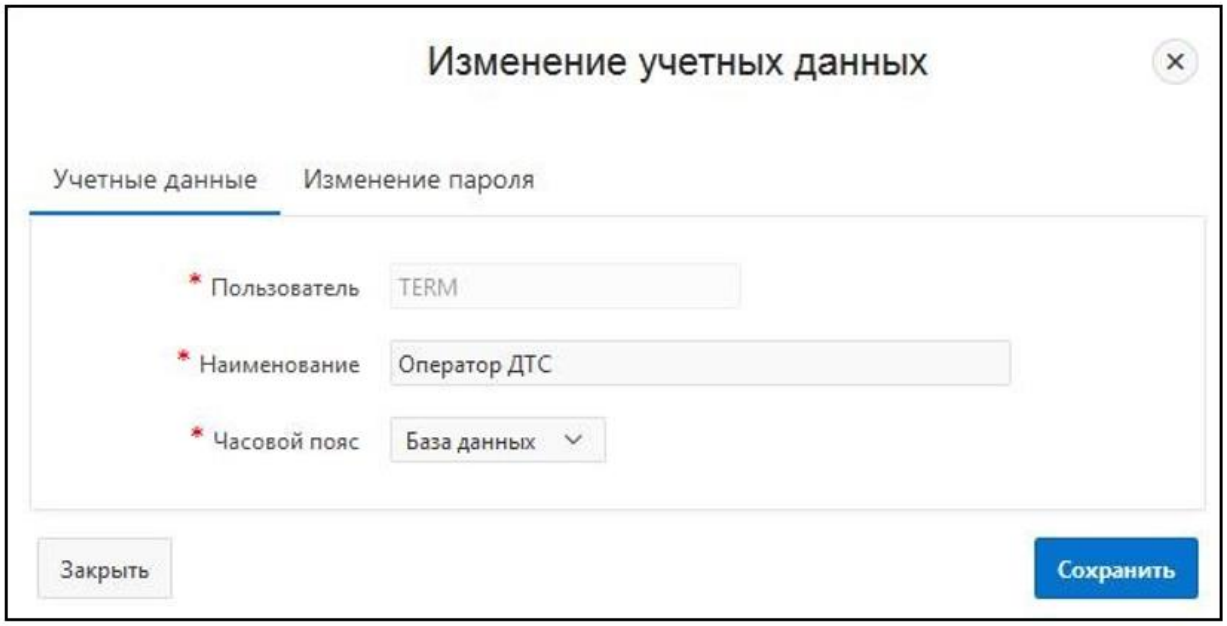


Рисунок 31. Изменение учетных данных

Для изменения пароля введите во вкладке *Изменение пароля* текущий пароль, а затем новый пароль с подтверждением.

4. СЕРВИСНЫЕ ФУНКЦИИ РАБОЧИХ МЕСТ ОПЕРАТОРА

4.1 Настройки отчетов

Для гибкого управления отчетами в системе предусмотрены дополнительные инструменты. Выбор осуществляется нажатием кнопки **Действия**, которая есть в каждом отчете.

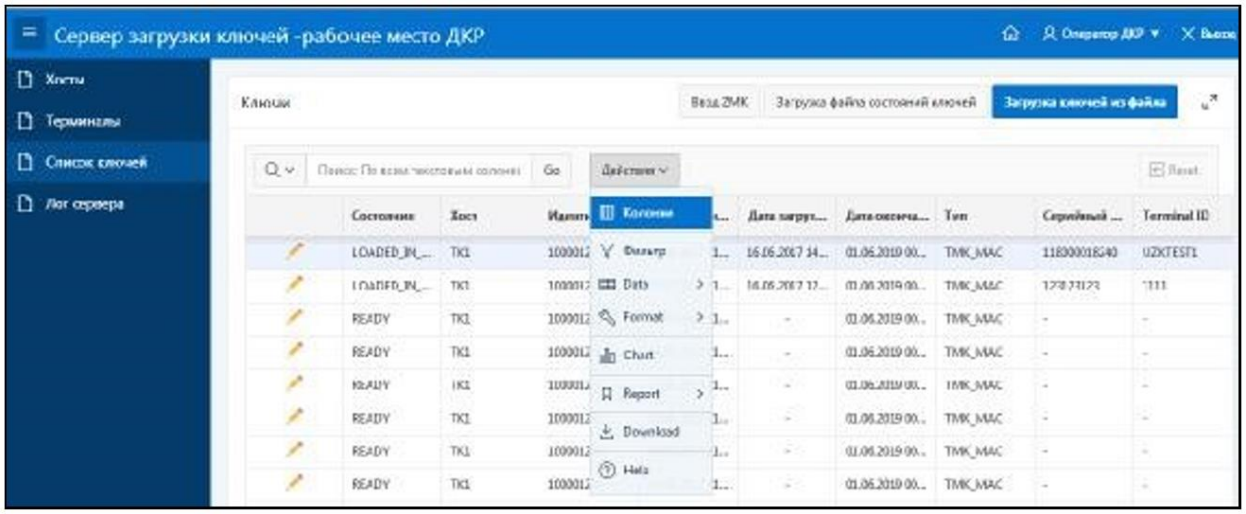


Рисунок 32. Настройки отчетов

4.2 Функции меню настройки

4.2.1 Колонки

Функция предназначена для выбора столбцов таблиц, отображаемых на экране.

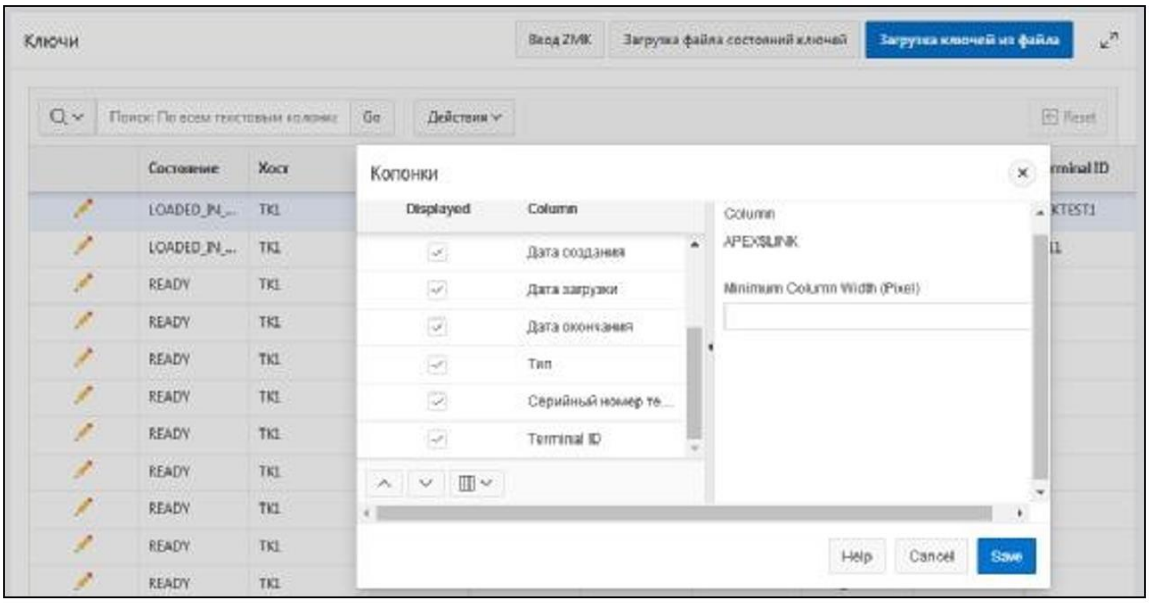


Рисунок 33. Колонки

Список столбцов редактируется флажками. Снимите флажки со столбцов, которые не должны отображаться в отчете. Стрелками слева можно изменять порядок столбцов. Нажмите на поле с названием столбца и переместите его вверх или вниз по списку. Для сохранения изменений нажмите кнопку **Save**.

4.2.2 Фильтр

Функция фильтра позволяет сделать выборку по гибким правилам по любым столбцам или строкам.

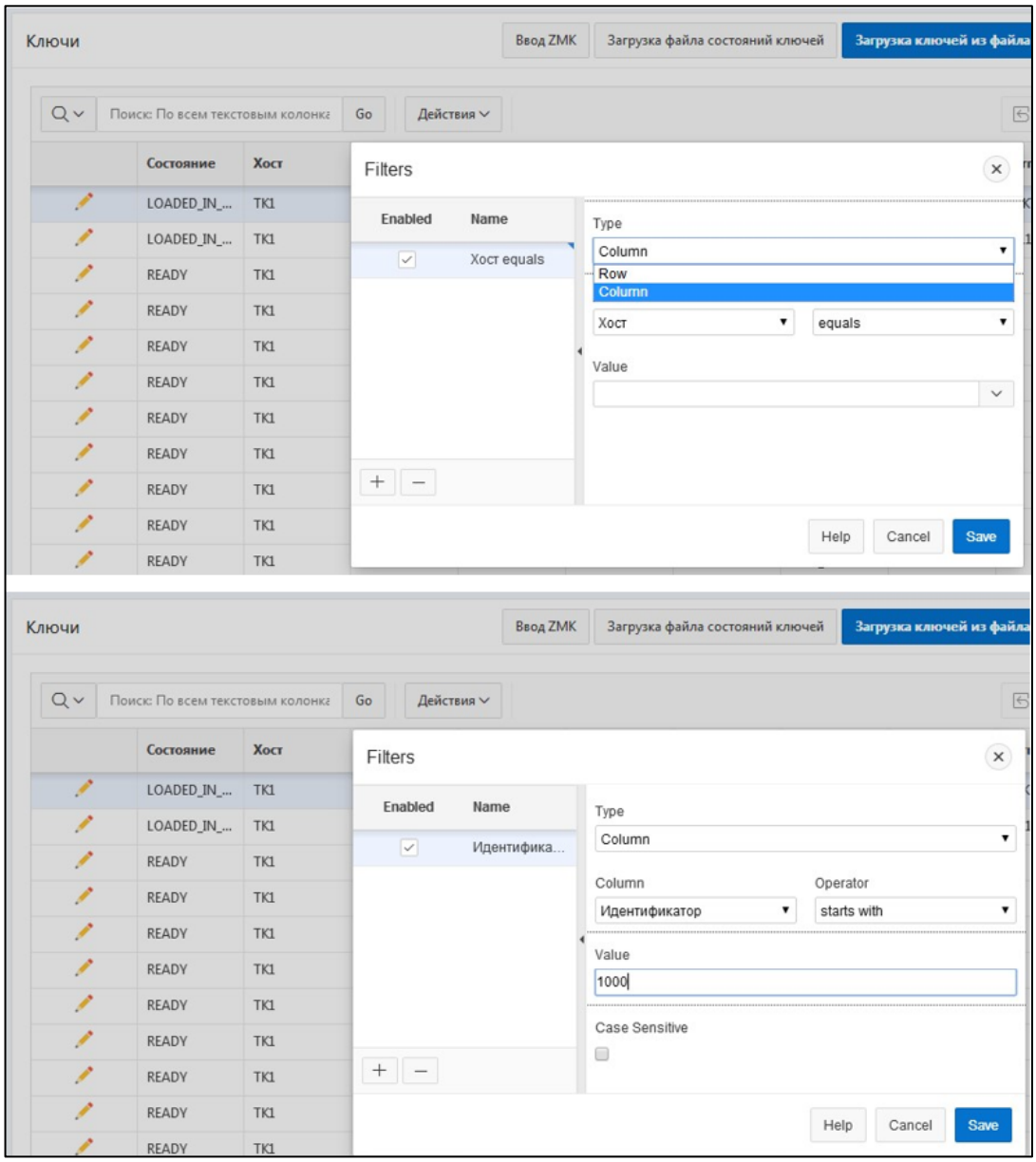


Рисунок 34. Фильтр_1

Фильтр по строкам позволяет выбирать данные, указывая условие отбора в нотации СУБД Postgres.

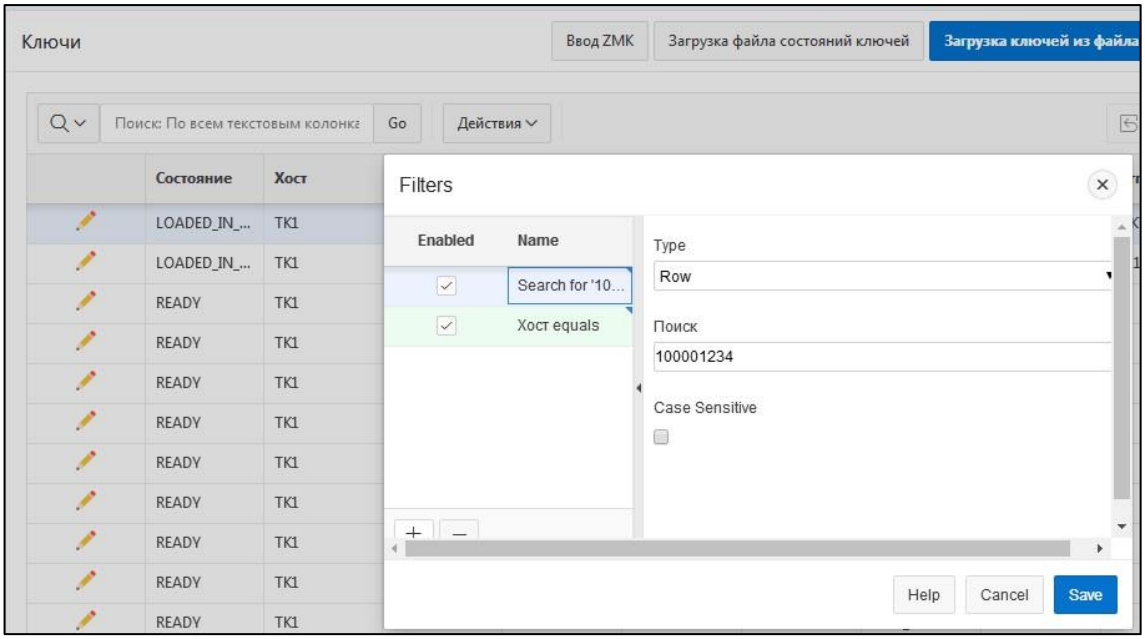


Рисунок 35. Фильтр_2

4.2.3 Строки на странице

Настройка количества строк, выводимых на страницу. Под страницей понимается HTML-страница, формируемая для показа браузером. Не рекомендуется применять для показа опцию *Все* для больших таблиц.

4.2.4 Формат

Опция *Сортировка* позволяет выполнять сортировку строк при показе по настраиваемому списку полей.

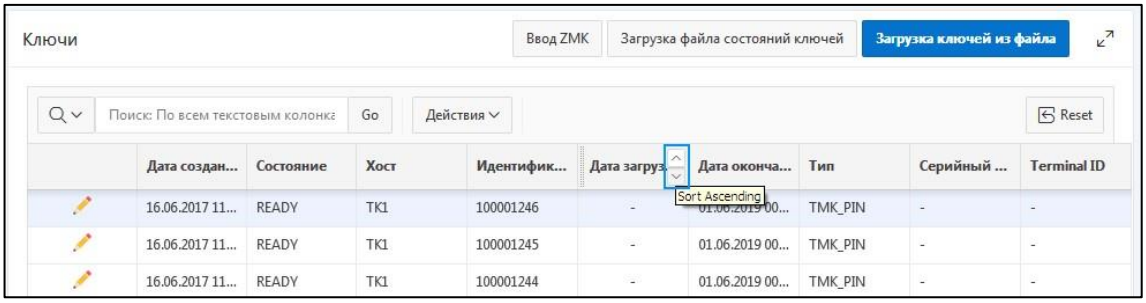


Рисунок 36. Опция Сортировка

4.2.5 Контрольная точка

Опция *Control Break* позволяет группировать идентичные по настроенному значению столбца строки.

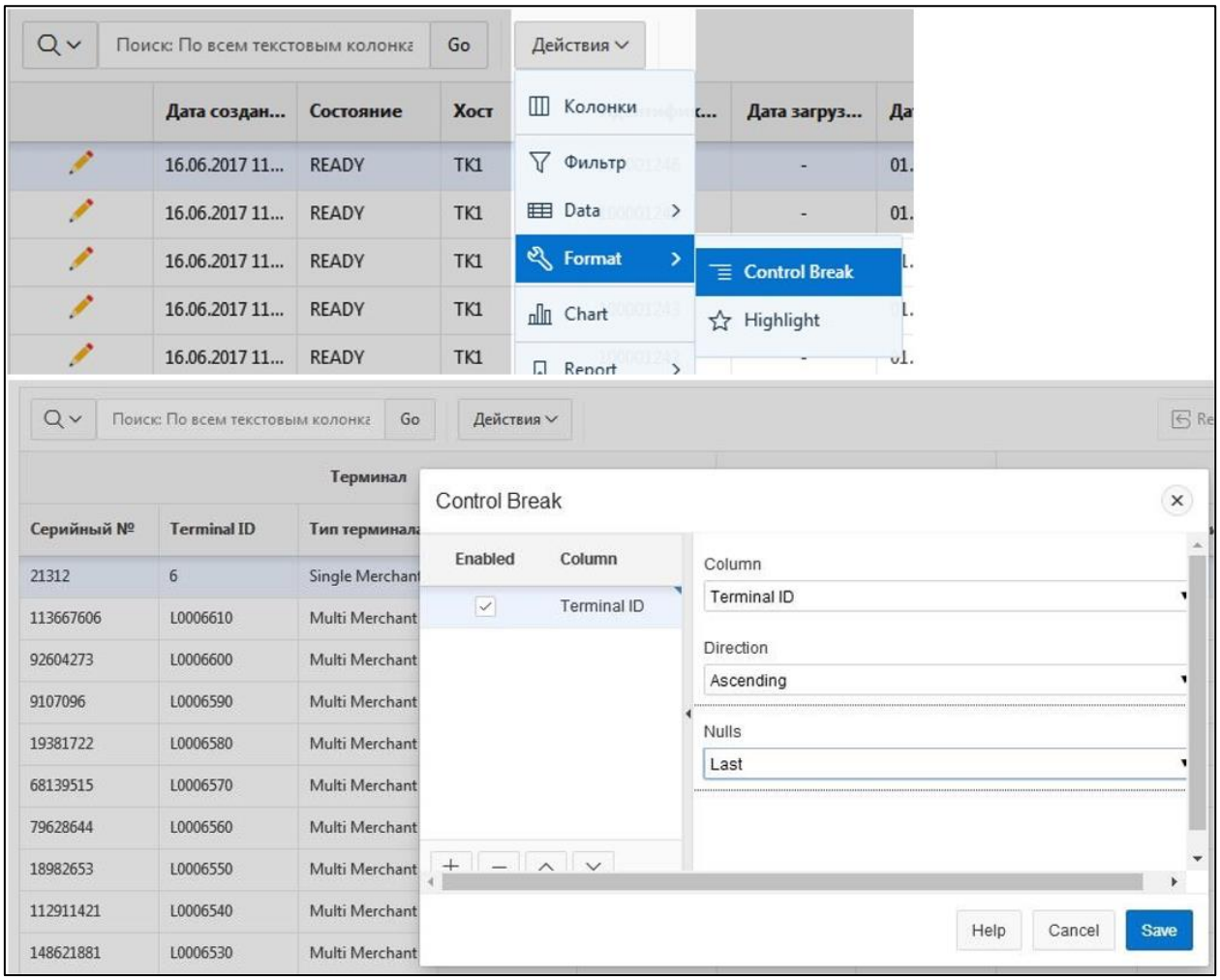


Рисунок 37. Опция Control Break

4.2.6 Сохранение и сброс настройки отчета

Save As – Сохраняет измененный отчет для использования в будущем. Для сохранения необходимо указать название. После сохранения настройки в фильтре *Отчеты* появится название сохранённой настройки. Выбирая этот фильтр, получаем отчет в его сохраненной форме. Reset – Сбрасывает настройки отчета по умолчанию, удаляя все ранее сделанные изменения.

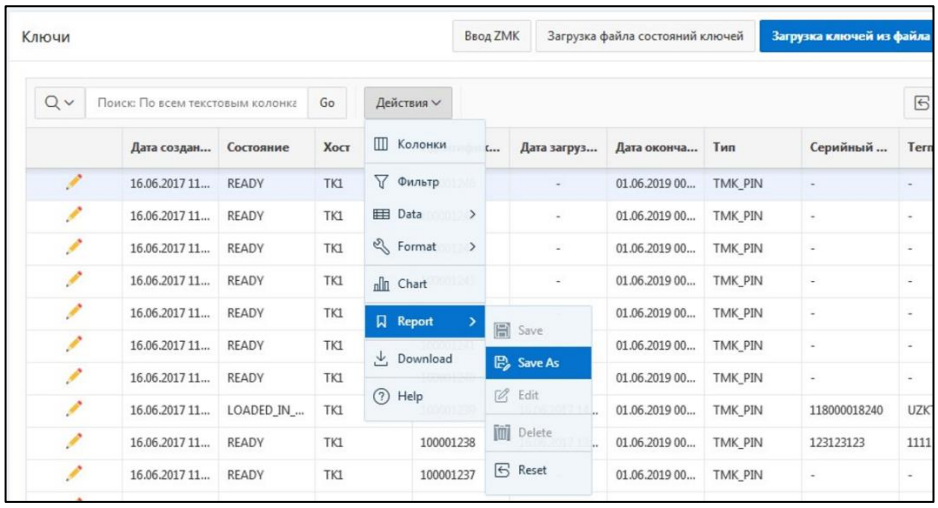


Рисунок 38. Сохранение и сброс отчета

4.2.7 Выгрузить

Опция *Download* позволяет выгрузить набор текущих результатов. Форматы закачки будут отличаться в зависимости от установки и определения отчетов, но могут включать CSV, HTML форматы, также отчет можно послать по электронной почте.

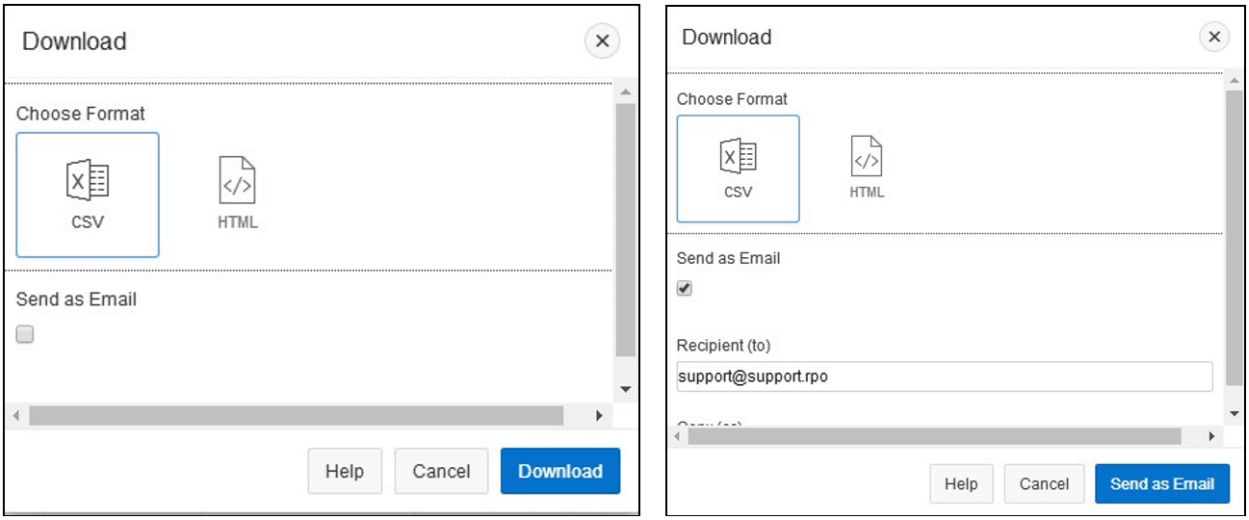


Рисунок 39. Опция Download

ПРИЛОЖЕНИЕ №1 ТРЕБОВАНИЯ PCI SECURITY VERSION 3.0

1. Соответствие LANKEY требованиям документа PCI Security version 3.0

Целевое назначение СЗК (Сервер Загрузки Ключей) – обеспечение управления и удаленной загрузки симметричных TDES мастер-ключей, используя ассиметричные RSA ключи, в соответствии с Normative Annex A – Symmetric Key Distribution using Asymmetric Techniques.

1 СЗК работает с моделями HSM Thales (соответствие требованию 1-3)

- payShield 9000 (сертификат FIPS 140-2 Level 3 и PCI HSM v.1)
- payShield 10K (сертификат FIPS 140-2 Level 3 и PCI HSM v.3)

2 В соответствии с требованием 18-3, СЗК хранит все зашифрованные мастер-ключи в виде “Key Blocks”.

Процесс удаленной загрузки построен по методологии стандарта ANSI X9.24 TR-34. Используется двухпроходной метод (подробное описание процесса приведено ниже) (The Two Pass method is appropriate for where the POI and KDH can communicate in real time. It uses random nonces for the prevention of replay attacks.)

3 Удаленная загрузка применяется только для первичной загрузки TDES мастер-ключей двойной длины двух типов: для PIN (TPMK) и для MAC (TAMK) (в соответствии с Normative Annex B – Key-Injection Facilities)

4 В соответствии с Normative Annex C – Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms для шифрования передаваемых мастер-ключей и цифровой подписи, используются RSA ключи длиной 2048 bits

5 Канал связи между терминалом и СЗК использует SSL шифрование с работой по протоколу TLS v1.2

2. Процесс удаленной загрузки мастер-ключей с СЗК на терминал можно разбить на 2 фазы: Подготовительная и Основная.

Подготовительная фаза (выполняется однократно, применима ко всем терминалам вендора):

- На HSM, к которому подключен СЗК, генерируется пара RSA-ключей и формируется запрос на подпись публичного сертификата (certificate signing request)
- Запрос на подпись направляется вендору терминального оборудования, который, используя приватный ключ из своей пары RSA ключей, формирует публичный сертификат СЗК
- Вендор также предоставляет для СЗК свой самоподписанный корневой сертификат CA (Root CA)
- На каждом терминале генерируется (или загружается в заводских условиях) уникальная пара RSA ключей и формируется публичный сертификат, подписанный вендором (в соответствии с требованием 6-5 Normative Annex B – Key-Injection Facilities)
- На терминал также загружается Root CA вендора (если он не был загружен на фабрике)

Основная фаза (выполняется на каждом терминале):

Терминал формирует online запрос для СЗК, включая в него следующие элементы:

1. Свой уникальный публичный сертификат
2. Серийный номер терминала (S/N)
3. Случайное число (RND)

4. Тип мастер-ключа для загрузки (PIN или MAC)
5. Цифровую подпись, сделанную на вышеперечисленном наборе элементов данных (элементы 1,2,3,4) с помощью своего приватного RSA ключа.

Терминал устанавливает защищенное SSL-соединение (по протоколу TLS v1.2) с СЗК и направляет на него сформированный online запрос СЗК, получив запрос на загрузку мастер-ключа определенного типа от терминала, выполняет следующие действия:

1. С помощью корневого CA сертификата вендора, проверяет (выполняет RSA verify) присланный сертификат терминала
2. Если проверка завершилась успешно, то СЗК, с помощью публичного ключа, из сертификата терминала, проверяет цифровую подпись присланного набора данных (контролирует целостность данных в запросе)
3. Если проверка подписи завершилась успешно, СЗК проверяет серийный номер терминала, по своим внутренним спискам, на предмет разрешения загрузки ключей для него
4. Если эта проверка прошла успешно, тогда СЗК, дает команду на HSM, к которому он подключен, для экспорта мастер-ключа, зашифрованным под публичным RSA ключом терминала.

СЗК формирует ответ для терминала, включая в него следующие элементы:

1. Публичный сертификат СЗК (полученный на подготовительной фазе)
2. Зашифрованный на публичном RSA ключе терминала мастер-ключ нужного типа
3. KCV мастер-ключа
4. Цифровая подпись на наборе данных (часть данных для подписи берется из исходного запроса терминала):

- S/N + RND + тип ключа+ зашифрованный мастер-ключ + сертификат СЗК.
- Подпись формируется по команде СЗК, с помощью HSM, на приватном ключе HSM.

СЗК направляет сформированный ответ в сторону терминала по шифрованному каналу связи терминал, получив ответ от СЗК, выполняет следующие действия:

1. С помощью корневого CA сертификата вендора, проверяет (выполняет RSA verify) присланный сертификат СЗК
2. Если проверка завершилась успешно, то терминал, с помощью публичного ключа, из сертификата СЗК, проверяет цифровую подпись набора данных (контролирует целостность данных в запросе и ответе). Проверяет соответствие S/N, RND и типа ключа
3. Если проверка подписи завершилась успешно, терминал дает команду драйверу пин-пада на загрузку во внутренний пин-пад, полученного мастер-ключа, зашифрованного под публичным ключом терминала
4. Проводит контроль KCV загруженного ключа, значению KCV, полученного от СЗК
5. Результат применения ключа(успешно/неуспешно) – сообщается на СЗК.

Таким образом, в процессе загрузки мастер-ключа происходит взаимная аутентификация сертификатов терминала и СЗК, принадлежащих одной и той же системе PKI (имеющих общий Root CA), а также используется цифровая подпись с включением случайных данных, для предотвращения “атак повтора” (“replay attacks”), “атаки посередине” (“man-in-the-middle” attacks) и для контроля целостности данных. Сам мастер-ключ передается в зашифрованном под публичным ключом терминала виде.

Нормативные документы:

1. PCI PIN Security Requirements and Testing Procedures Version 3.0

2. *ANSI TR-34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport*

3. PCI PIN Security Requirements Technical FAQs (January 2021)