2021

Руководство пользователя АРМ ПАК «Звезда»

НИИМЭ

Оглавление

АННОТАЦИЯ

Документ предназначен для операторов и администраторов Криптосервиса.

Первое чтение следует осуществлять по порядку: после краткого введения изложены требования к среде окружения и варианты установки АРМ. Затем следует раздел сценариев, которые описывает типичные сценарии использования АРМа. В конце документ расположен справочный раздел с детальным описанием всех графических элементов управления.

Список сокращений

Криптосервис – основная библиотека, обеспечивающая работу системы ПАК Звезда.

Интерфейс API admin_service – сокетный интерфейс Криптосервиса, по которому АРМ подключается к Криптосервису.

Ключевой контейнер – логическая структура данных Криптосервиса см. 1.

Проблема – состояние Криптосервиса, требующее отклика оператора см. 1.

Событие – нештатная ситуация, которая произошла в ходе работы Криптосервиса см. 1.

Ресурсы Криптосервиса – представляют собой исчерпаемые объекты Криптосервиса.

ЭБКС / HSM – чип, предназначений для выполнения криптографических операций.

Кластер – массив ЭБКС, обеспечивает отказоустойчивость и распределяет нагрузку.

Синхронная сессия – логические соединение между Криптосервисом и клиентом см. 1.

1 ВВЕДЕНИЕ

АРМ ПАК «Звезда», далее АРМ, представляет собой ПО на базе платформы .NET Framework для мониторинга и управления состоянием Криптосервиса (модуль системы ПАК «Звезда»). АРМ не расширяет возможностей Криптосервиса и позволяет делать только то, что разрешено в API Криптосервиса.

Для взаимодействия с Криптосервисом АРМ использует сокетное подключение. Безопасность передаваемых данных по этому каналу связи возлагается на среду окружения и не рассматривается в рамках этого документа.

АРМ позволяет:

- Создавать, удалять и изменять ключевые контейнеры и ключи.
- Создавать, удалять и изменять параметры клиентов Криптосервиса.
- Создавать, удалять и изменять параметры пользователей АРМ.
- Управлять сертификатами Криптосервиса.
- Отслеживать ошибки и события Криптосервиса.
- Отслеживать нагрузку на Криптосервис.
- Изменять настройки криптосервиса.

Общие принципы GUI:

1. Пользователь после логина попадает в основное окно, которое включает:
    a. Меню слева, определяет, что будет отображаться в окне справа
    b. Окно справа от меню отображает информацию, соответствующую выбранному пункту меню слева.
    c. Статусная строка внизу, отображает информацию о фоновых процессах.
2. Отдельные секции на экране «Управление клиентами» такие как «Информация о клиенте», «Список задач клиента» и т.д. можно сворачивать.
3. Кнопки с текстом «…» означают, что при их нажатии отобразится контекстное меню.
4. Все редактируемые поля и кнопки действий подразумевают осознанные действия пользователя, не требуют подтверждений, их действие нельзя отменить.
5. Успешный результат выполнения каких-либо операций отображается в виде изменения соответствующих полей, если это подразумевается операцией. Ошибки выполнения операций отображаются в виде модальных окон в момент их появления.
6. В всех модальных окнах работают кнопки Esc и Enter для отмены или подтверждения операции соответственно.
7. Подчеркнутый текст означает ссылки.
8. Список клиентов поддерживает множественный выбор (Ctrl+ ЛКМ, Shift + ЛКМ)
9. Информация, введенная в любом окне, сохранится при переходе в другое окно, за исключением модальных окон.

10. В каждый момент времени к Криптосервису может быть подключен только один АРМ.

2 Установка

АРМ поставляется в виде portable версии. Для установки распакуйте архив в любую папку, удовлетворяющую требованиям к окружению.

Требования к среде окружения:

- ОС Windows 7+.
- .Net Framework 4.7.2+
- Права на установку TCP соединения с сервером, на котором расположен Криптосервис.
- Права на создание файлов в директории установки АРМ.

3 Сценарии использования

Этот раздел содержит основные сценарии использования АРМ. Для подробной информации обо всех функциях АРМа см. Справочник.

3.1 Первый запуск

Перед запуском АРМ следует убедиться, что Криптосервис запущен и нормально работает, а также что интерфейс API admin_service не занят другим приложением.

Для запуска АРМ необходимо запустить файл iot_admin.exe. Пользователь должен увидеть экран подключения. При первом запуске ip адрес сервера, на котором расположен Криптосервис, еще не известен, поэтому его необходимо задать в меню «НАСТРОЙКИ», расположенном в правом верхнем углу экрана подключения. В случае успешного подключения пользователь должен увидеть форму для ввода логина и пароля, в противном случае АРМ будет пытаться подключаться по указанному IP адресу пока не подключится или не будет закрыт.

Стандартные настройки Криптосервиса подразумевают наличие роли admin с неограниченными правами. Используя эту роль, администратор имеет возможность зайти в АРМ и настроить список операторов.

Таблица 1 Параметры роли по умолчанию

Login	admin
Password	admin

После успешного входа, пользователь попадает в основное окно АРМа и может приступить к первоначальной настройке.

Начальная настройка должна включать в себя:

1. Создание ключевых контейнеров
2. Смену пароля роли администратора по умолчанию
3. Создание ролей для операторов

3.1.1 Создание ключевых контейнеров

Для работы Криптосервиса необходимо создать ключевые контейнеры и ключи. Для этого пользователь должен перейти на вкладку «Управление ключами».

Минимальный набор ключевых контейнеров состоит из:

1. Ключевой контейнер с назначением «Сброс микросхемы»
2. Ключевой контейнер с назначением «Защита канала»
3. Ключевой контейнер с назначением «Замена ключей клиента»

Ключевой контейнер с назначением «ЭП сервера» следует создавать в случае если требуется подписывать сообщения клиентов на Криптосервисе.

Ключевой контейнер с назначением «Функции УЦ», если предполагается встраивать Криптосервис во внешнюю структуру PKI или планируется использовать Криптосервис в качестве УЦ.

Для создания необходимых ключевых контейнеров необходимо выбрать нужное назначение в списке слева и нажать кнопку «Создание ключевого контейнера». В АРМе при создании ключевого контейнера автоматически создается первый ключ в этом контейнере. Дополнительные ключи в любом контейнере можно создать при помощи кнопки «Сгенерировать» в правой части экрана «Управление ключами».

На данный момент АРМ не позволяет создавать больше одного ключевого контейнера каждого типа.

3.1.2 Смена пароля роли администратора по умолчанию

В целях безопасности рекомендуется сменить стандартный пароль роли admin. Это можно сделать на экране «Управление учетными записями», затем выбрать роль admin и воспользоваться кнопкой «Смена пароля».

3.1.3 Создание ролей операторов

В случае если администратор является не единственным предполагаемым пользователем АРМ, следует создать учетные записи для каждого пользователя на экране «Управление учетными записями» используя кнопку «Добавить». Экран создания пользователя предоставляет возможность выбирать полномочия см. Таблица 2.

Завершив указанные выше этапы, Криптосервис можно считать готовым к работе.

3.2 Клиенты ПАК «Звезда»

3.2.1 Регистрация

Для добавления новых клиентов в Криптосервис пользователь АРМ, обладая соответствующими полномочиями, может воспользоваться кнопкой «Регистрация» на экране «Управление клиентами».

Окно регистрации позволяет настраивать параметры создаваемых клиентов, а также указать нужна ли автоматическая *активация*.

Следует отметить, что клиенты на выходе процедуры регистрации не готовы к работе. Для завершения процесса создания клиентов необходимо передать информацию о новых клиентах из Криптосервиса в центр *персонализации* фактических устройств, провести персонализацию и, затем, обновить информацию о клиентах на Криптосервисе. Весь этот процесс находится вне рамок АРМа и производится внешними средствами.

3.2.2 Работа с клиентами

После того как процедура регистрации клиентов была полностью завершена, включая персонализацию, пользователь АРМ может просматривать и изменять параметры всех клиентов на экране «Управление клиентами».

Этот экран разделен на две части: список клиентов слева и информация о выбранном клиенте справа. Список позволяет выбирать клиентов и поддерживает *фильтрацию* по различным параметрам. Элементы управления в области информации о клиенте позволяют производить различные операции с конкретным клиентом.

В случае, когда в списке слева выбрано больше одного клиента, появляется экран *групповых операций,* которые позволяют применить определенный список операций ко всем выбранным клиентам.

3.3 Регламентные процедуры

АРМ позволяет настроить систему уведомлений для помощи в проведении регламентных процедур. На экране «Настройки» можно указать за какой период времени до истечения срока действия ключа/пароля требуется уведомлять оператора. По наступлении указанного срока Криптосервис начнет генерировать *проблему*, которая попадет в экран «Проблемы», где ее можно эффективно решить.

3.3.1 Отзыв мастер ключа

Типичный сценарий отзыва мастер ключа выглядит следующим образом:

За некоторое время до истечения срока действия ключа *Криптосервис* начнет генерировать *проблему*, которая будет отображаться в АРМе на вкладке «Проблемы». На этой вкладке оператор может перейти к обработке *проблемы*, что в данном случае перенесет его на вкладку «Управление ключами», где будет автоматически выбран ключ с истекающим сроком действия. Оператору остается нажать кнопку «Отозвать», в результате чего ему предложат выбрать новый ключ для клиентов, которые используют данный ключ, после чего *Криптосервис* сформирует серию заданий на смену ключа для всех вовлеченных клиентов.

3.3.2 Смена ключей клиентов

За некоторое время до истечения срока действия ключей клиентов Криптосервис начнет генерировать *проблему,* которая будет отображаться в АРМе на вкладке «Проблемы». На этой вкладке оператор может перейти к обработке *проблемы*, что в данном случае перенесет его на вкладку «Управление клиентами», где будут автоматически выбраны все вовлеченные клиенты и оператор увидит стандартное окно Групповых операций, где ему остается выбрать операцию инкремента версии или загрузки мастер ключа.

3.4 Сертификаты и PKI

АРМ позволяет встроить текущий инстанс Криптосервиса в иерархию PKI или использовать Криптосервис в качестве УЦ. Для этого на экранах «Управление клиентами», «Управление ключами» и «PKI» есть элементы управления, которые позволяют сохранять запросы на сертификаты, сами сертификаты и загружать внешние сертификаты для разных типов ключей.

3.4.1 Генерация сертификатов для клиентских устройств

В случае, когда Криптосервис выступает в роли УЦ для генерации сертификатов клиентских устройств следует выполнить следующий алгоритм:

1. Перейти на вкладку управление клиентами
2. Выбрать группу клиентов, для которых необходимо сгенерировать сертификаты
3. В меню групповых операций выбрать пункт «Сгенерировать сертификаты на ключе УЦ (Kca.cs)»
4. Убедиться, что в окне результатов групповой операции все операции выполнены успешно.

3.4.2 Получение сертификата внешнего УЦ на ключ УЦ

Если оператор хочет встроить Криптосервис во внешнюю иерархию PKI для этого потребуется подписать ключ УЦ во внешнем УЦ, типичный сценарий выглядит так:

1. Если сертификат внешнего УЦ уже загружен как точка доверия в АРМ, перейти к п. 4, если нет перейти к п.2
2. Перейти на вкладку PKI главного меню.
3. Воспользоваться кнопкой «Добавить» справа от списка доверенных сертификатов, где необходимо выбрать сертификат внешнего УЦ. В случае успешной загрузки сертификат отобразится в списке доверенных.
4. Перейти на вкладку «Управление ключами».
5. Выбрать назначение ключа «Функции УЦ»
6. Выбрать ключ УЦ, который будет встраиваться во внешнюю иерархию PKI.
7. Воспользоваться кнопкой «PKI».
8. Выбрать пункт «Сохранить запрос на сертификат» в открывшемся диалоге выбрать папку куда будет сохранен запрос. Стоит отметить, что файлов запросов может быть больше 1, так как некоторые ключи *кластеризуются* Криптосервисом, в этом случае в следующем шаге необходимо сгенерировать сертификат для каждого запроса.
9. Используя запрос на сертификат, сгенерировать сертификат во внешнем УЦ.
10. Воспользоваться кнопкой «PKI».
11. Выбрать пункт «Загрузить сертификат», в открывшемся диалоге выбрать файл(ы), полученные в п.9. В случае ошибок они будут показаны в виде диалоговых окон, в противном случае операция выполнена успешно.

3.4.3 Получение сертификатов внешнего УЦ для клиентских устройств

Типичный сценарий загрузки сертификатов внешнего УЦ для клиентских устройств выглядит так:

1. Если сертификат внешнего УЦ уже загружен как точка доверия в АРМ, перейти к п. 4, если нет перейти к п.2
2. Перейти на вкладку PKI главного меню.
3. Воспользоваться кнопкой «Добавить» справа от списка доверенных сертификатов, где необходимо выбрать сертификат внешнего УЦ. В случае успешной загрузки сертификат отобразится в списке доверенных.
4. Перейти на вкладку «Управление клиентами»
5. Выбрать группу клиентов, для которых необходимо сгенерировать сертификаты.

6. В меню групповых операций выбрать пункт «Сохранить запросы на сертификат», в открывшемся диалоге выбрать папку, куда будут сохранены запросы.
7. Для каждого запроса из п.6 необходимо сгенерировать сертификат во внешнем УЦ.
8. Перейти на вкладку «PKI» основного меню.
9. Воспользоваться кнопкой «Импортировать клиентские сертификаты», в открывшемся диалоге выбрать файлы сертификатов, полученные в п.7.
10. В открывшемся окне групповой операции импорта будут отображены результаты операции.

3.5 Мониторинг

АРМ предоставляет следующие средства для мониторинга состояния Криптосервиса:

1. Проблемы (см. 4.2.5)
2. События (см. 4.2.6)
3. Информация о нагрузке (см. 4.2.4)
4. Телеметрия

3.5.1 Проблемы и события

В ходе работы оператора могут возникать *события* и *проблемы*, которые попадают в соответствующие разделы меню слева. При их возникновении напротив названия пункта появляется красный индикатор «new». Разделы предоставляют информацию о *событиях/проблемах* и упрощают их обработку.

3.5.2 Информация о нагрузке

На экране «Мониторинг криптосервиса» отображается текущая нагрузка на Криптосервис и его *ресурсы*. В верхней части экрана располагается общая информация о состоянии Криптосервиса, а также информация о занятых ресурсах. Ниже располагаются диаграммы текущей нагрузки на каждый отдельный *ЭБКС* в *кластере* Криптосервиса.

3.5.3 Телеметрия

На экране «Мониторинг криптосервиса» кнопка «Сохранить телеметрию» позволяет сохранить данные о нагрузке на Криптосервис за выбранный период для дальнейшей обработки внешними аналитическими средствами. Формат телеметрической информации см. Таблица 3.

4 Справочник

4.1 Окно подключения

Окно подключения отображается сразу после запуска АРМа. При первом запуске в АРМе необходимо настроить ip адрес Криптосервиса через меню «Настройки» в правом верхнем углу экрана. IP адрес должен совпадать с настройками, заданными в конфигурационном файле Криптосервиса для интерфейса admin. После сохранения настроек АРМ сохраняет их в файле на жестком диске в директории установки и в дальнейшем будет использовать их для установки подключения.

Рисунок 1 Окно подключения. Попытка подключения

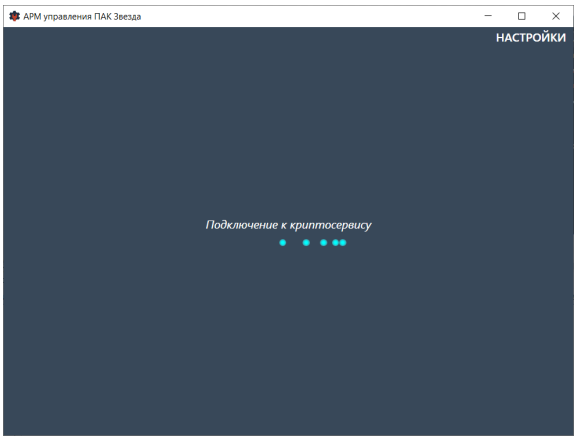
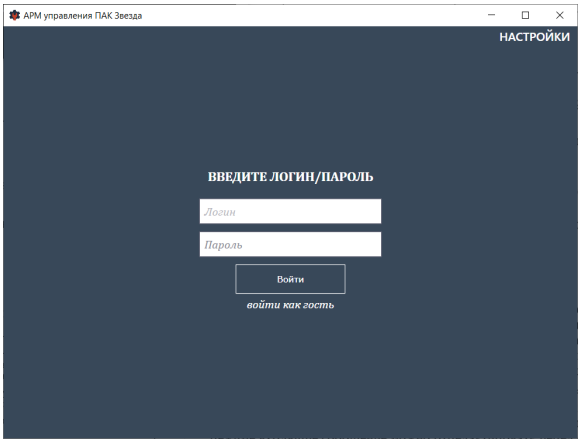


Рисунок 2 Окно подключения. Подключение установлено



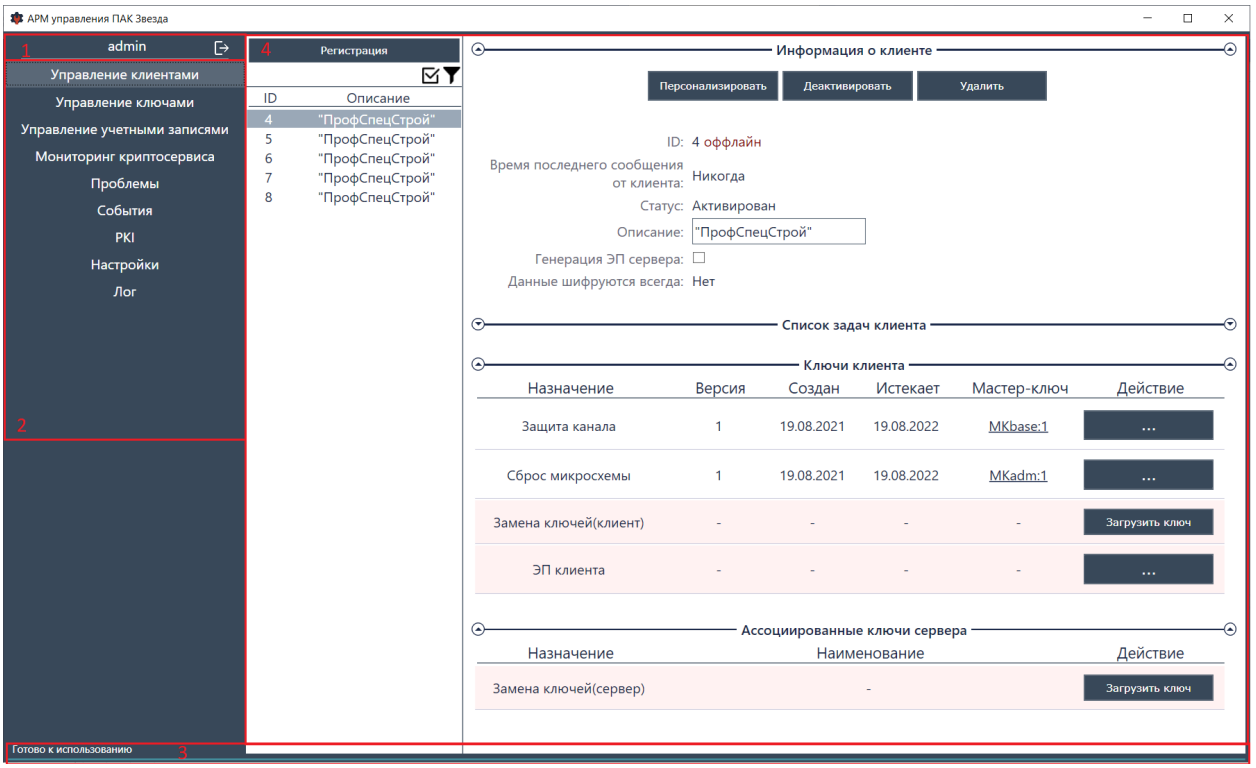
Если подключение успешно установлено, АРМ предложит форму логина/пароля, а также вариант входа в гостевом режиме.

Гостевой режим позволяет осуществлять функции мониторинга, но не позволяет изменять состояние Криптосервиса каким-либо образом.

4.2 Основное окно

После того как пользователь успешно ввел логин и пароль, он попадает в основное окно:

Рисунок 3 Основное окно



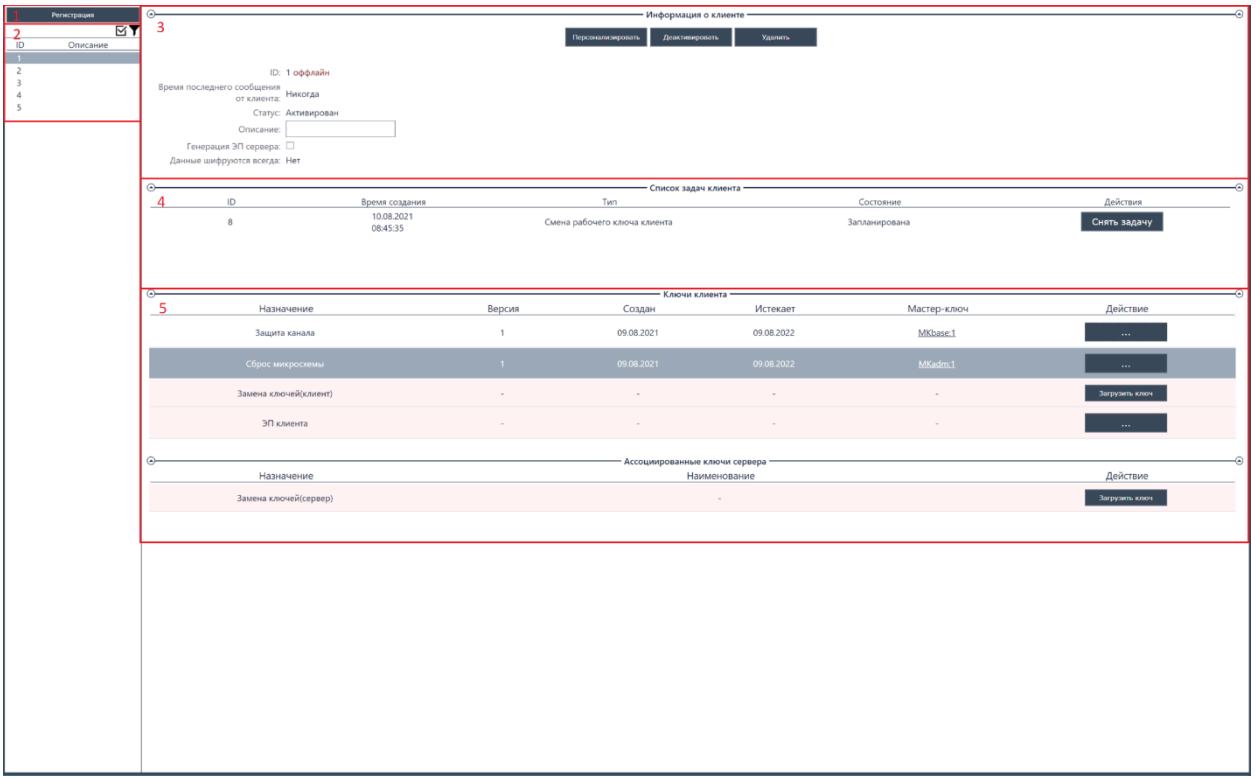
Это окно состоит из четырех зон:

1. В левом верхнем углу располагается информация о текущем пользователе и также кнопка выхода возврата на экран подключения (с выходом из текущего пользователя)
2. Ниже находится основное меню, которое содержит все экраны доступные в текущей версии АРМа. Стоит обратить внимание, что пункты меню «Проблемы» и «События» могут иметь индикатор «new», который означает что в этом разделе имеются нерассмотренные *проблемы* или *события*.
3. Внизу окна находится статусная зона, в ней отображается информация о текущих выполняемых задачах АРМа. Стоит отметить, что после успешного логина, АРМ пытается подгрузить основную информацию из базы данных Криптосервиса в фоновом режиме. В зависимости от объема базы данных и пропускной способности канала АРМ-Криптосервис время полной загрузки может варьироваться. Во избежание ошибок и неопределенного поведения следует дождаться статуса «Готово к использованию» перед началом работы.
4. Зона №4 меняется свое содержимое в зависимости от текущего выбранного пункта меню.

4.2.1 Экран «Управление клиентами»

Данный экран содержит все информацию о клиентах Криптосервиса, доступную через АРМ.

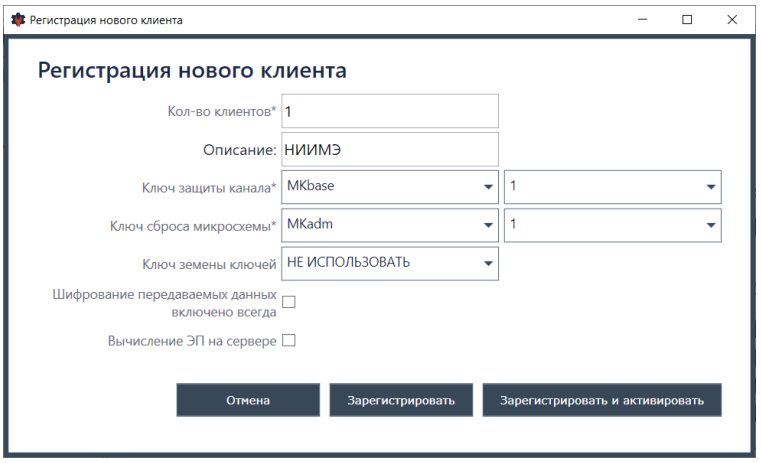
Рисунок 4 Экран "Управление клиентами"



Экран можно разделить на 5 зон:

1. Кнопка регистрации новых клиентов находится в верхнем левом углу. Она позволяет регистрировать произвольное количество клиентов и конфигурировать их параметры. Поля со * являются обязательными. Внизу окна расположены кнопки, позволяющие отменить операцию, зарегистрировать или зарегистрировать и активировать клиентов.

Рисунок 5 Окно регистрации клиентов



2. Вторая зона содержит список зарегистрированных клиентов и содержит краткую информацию – ID и описание для каждого из них. Над списком расположены кнопки: «выбрать всех» и «Фильтры» (см. 4.2.1.1).
3. Зона №3 содержит общую информацию о клиенте, выбранном в списке слева. В этой зоне расположены все операции, которые не связаны с ключами клиента.
4. Ниже располагается область текущих задач клиента – в ней отображается список запланированных или выполняющихся, но не завершенных задач выбранного

клиента. Кнопка «Снять задачу» позволяет отменить запланированное задание. По завершении задачи она исчезает из списка.

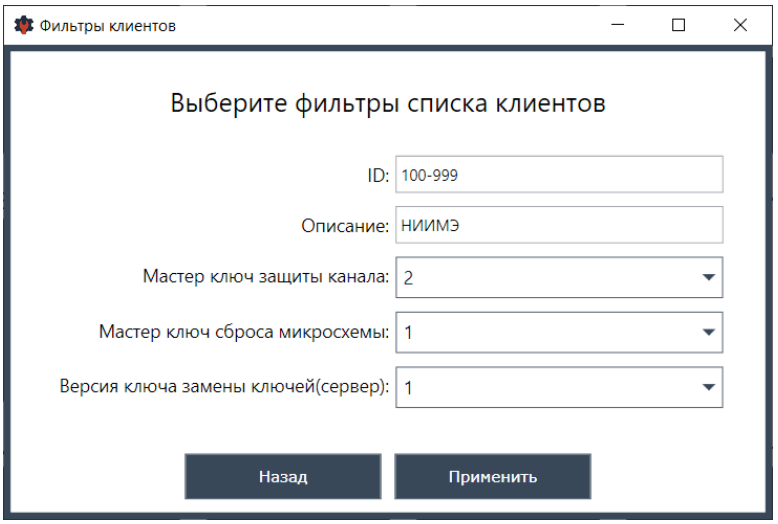
5. Зона №5 содержит информацию о ключах клиента и ассоциированных ключах сервера. Кнопки «…» открывают контекстное меню с доступными операциями для выбранного ключа. Их содержимое меняется в зависимости от типа ключа и его состояния:
    a. Для защиты канала и сброса микросхемы доступны операции:
        i. Смена ключа клиента – генерация нового ключа клиента на том же мастер ключе.
        ii. Смена мастер ключа – замена мастер ключа для выбранного ключа клиента с последующей генерацией нового ключа.
    b. Для ключей с назначением «Замена ключей(клиент)» и «Замена ключей(Сервер)» доступна только операция загрузки/смены ключа.
    c. Для ключа с назначением «ЭП клиента» доступны следующие операции:
        i. Загрузить ключ – загрузка ключа, отображается, когда ключ еще ни разу не загружался для этого клиента.
        ii. Сменить ключ – сгенерировать новую версию ключа, отображается если ключ уже был ранее загружен.
        iii. Сгенерировать сертификат на ключе УЦ(Kca.cs) – позволяет сгенерировать сертификат для этого ключа на ключе ЭП сервера. Отображается после загрузки ключа и, если сертификат еще не был загружен/сгенерирован.
        iv. Сохранить запрос на сертификат позволяет сохранить запрос на сертификат, используя который можно сгенерировать сертификат во внешнем УЦ и загрузить его в АРМ. Отображается после первой смены ключа и, если сертификат еще не был загружен/сгенерирован.
        v. Загрузить сертификат позволяет загрузить сертификат, созданный во внешнем УЦ. Отображается после загрузки ключа и, если сертификат еще не был загружен/сгенерирован.

4.2.1.1 Фильтры

Список клиентов поддерживает фильтрацию клиентов по набору полей. Все поля суммируются через логическое «И».

Обратите внимание что список может быть отфильтрован, например, в результате перехода к ошибкам группой операции. Когда активен какой-либо фильтр это явно написано над списком клиентов. Отменить фильтрация можно нажатием на кнопку «Х».

Рисунок 6 Окно фильтров клиентов



В примере на Рисунок 6 изображен фильтр клиентов, который ищет клиентов, у которых одновременно выполнены следующие условия:

1. Id попадают в диапазон 100-999 включительно
2. Описание включает в себя слово «НИИМЭ»
3. Мастер ключ защиты канала имеет версию 2
4. Мастер ключа сброса микросхемы имеет версию 1
5. Ключе замены ключей(сервер) имеет версию 1

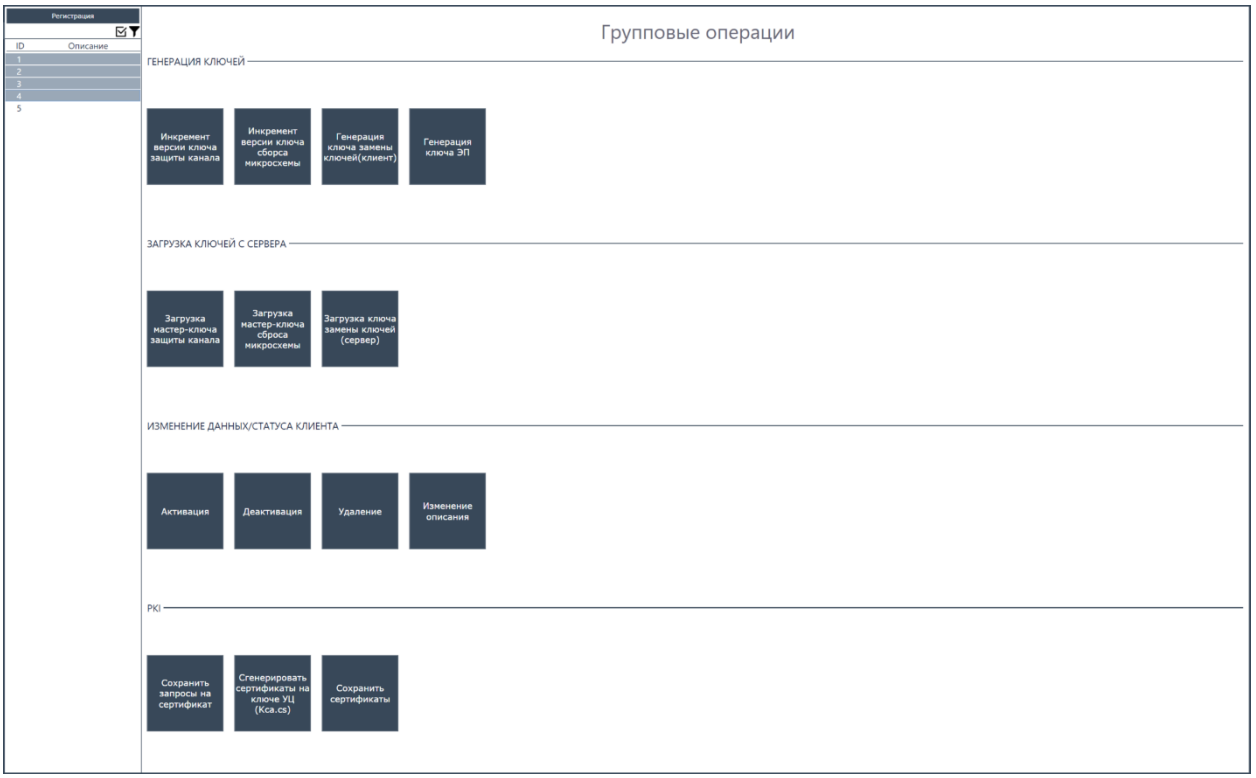
4.2.1.2 Групповые операции

Если пользователь выбрал больше одного клиента в списке слева (вручную или в результате применения фильтра) отображается экран групповых операций. Этот экран содержит все доступные групповые операции, при этом для части или всех клиентов выбранная операция может быть неприменима. В этом случае операция начнется, но будет провалена для неподходящих клиентов. После выбора операции отобразится окно, в котором будет отображаться информация о ходе ее проведения и ее итоги.

Групповую операцию нельзя прервать.

Если в ходе операции произошли ошибки, будет доступна кнопка перехода к группе клиентов, для которых операция провалилась. Эта кнопка работает как фильтр клиентов и не отправляет никаких команд Криптосервису.

Рисунок 7 Управление клиентами. Групповые операции



На момент написания документа поддерживаются следующие групповые операции:

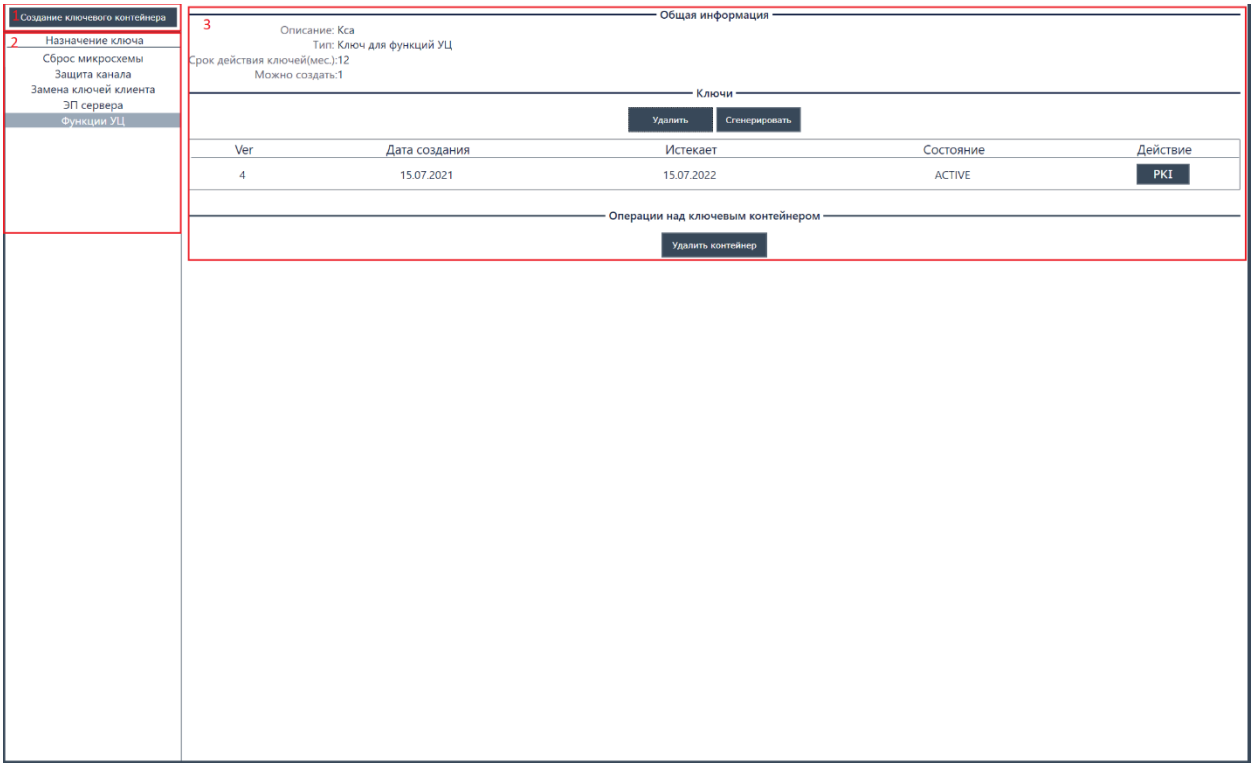
1. Инкремент версии ключа защиты канала – позволяет сгенерировать и загрузить новую версию ключа защиты канала на том же мастер ключе для всех выбранных клиентов.
2. Инкремент версии ключа защиты канала – позволяет сгенерировать и загрузить новую версию ключа сброса микросхемы на том же мастер ключе для всех выбранных клиентов для всех выбранных клиентов.
3. Генерация ключа замены ключей(клиент) – позволяет сгенерировать и загрузить новую версию ключа замены ключей (ключ клиента) для всех выбранных клиентов.
4. Генерация ключа ЭП – позволяет сгенерировать и загрузить новую версию ключа ЭП для всех выбранных клиентов.
5. Загрузка мастер ключа защиты канала – позволяет сменить мастер ключ защиты канала и сгенерировать новый ключ защиты канала для всех выбранных клиентов.
6. Загрузка мастер ключа сброса микросхемы – позволяет сменить мастер ключ сброса микросхемы и сгенерировать новый ключ сброса микросхемы для всех выбранных клиентов.
7. Загрузка ключа замены ключей (сервер) – позволяет загрузить открытую компоненту ассоциированного ключа замены ключей Криптосервиса для всех выбранных клиентов.
8. Активация – позволяет активировать всех выбранных клиентов.
9. Деактивация – позволяет деактивировать всех выбранных клиентов.
10. Удаление – позволяет удалить всех выбранных клиентов. Клиенты должны быть предварительно деактивированы.
11. Изменение описание – позволяет сменить описание выбранной группе клиентов.

12. Сохранить запросы на сертификат – позволяет выгрузить в выбранную папку запросы на сертификаты для выбранной группы клиентов.
13. Сгенерировать сертификаты на ключе УЦ(Kca.cs) – позволяет сгенерировать сертификаты на серверном ключе УЦ для выбранной группы клиентов.
14. Сохранить сертификаты – позволяет выбрать папку и сохранить в нее сертификаты выбранной группы клиентов.

4.2.2 Экран «Управление ключами»

Этот экран предоставляет информацию о всех ключевых контейнерах, созданных в Криптосервисе. Здесь расположены функции по созданию, удалению, модификации ключевых контейнеров и ключей в них. А также здесь находятся функции PKI для серверных ключей.

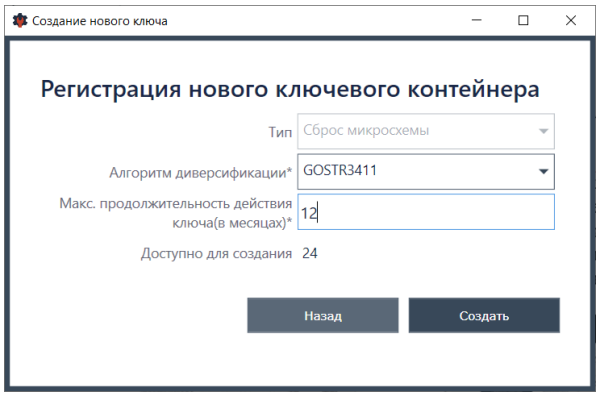
Рисунок 8 Управление ключами.



Экран можно разделить на 3 зоны:

1. Кнопка создания новых ключевых контейнеров отображает модальное окно, которое позволяет настроить параметры создаваемого контейнера, а также отображает информацию о том сколько ключей можно еще создать для этого типа контейнера. На данный момент средствами АРМ можно создать только один контейнер для каждого назначения ключа. Контейнеры, созданные вне АРМ, могут не отображаться.

Рисунок 9 Диалог создания нового ключевого контейнера



2. Список назначений ключей, которые поддерживаются в АРМе. Поскольку в АРМе поддерживается только один контейнер для каждого назначения, при выборе конкретного назначения автоматически выбирается соответствующий контейнер, если он был создан.
3. В зоне №3 отображается информация о контейнере с выбранным назначением и список ключей этого контейнера. У каждого ключа отображаются его параметры и доступные операции над ним. Содержимое этой зоны может отличаться для разных назначений ключевого контейнера.

4.2.3 Экран «Управление учетными записями»

Данный экран позволяет просматривать и добавлять пользователей АРМ, а также редактировать их полномочия.

Таблица 2 Полномочия пользователей АРМ

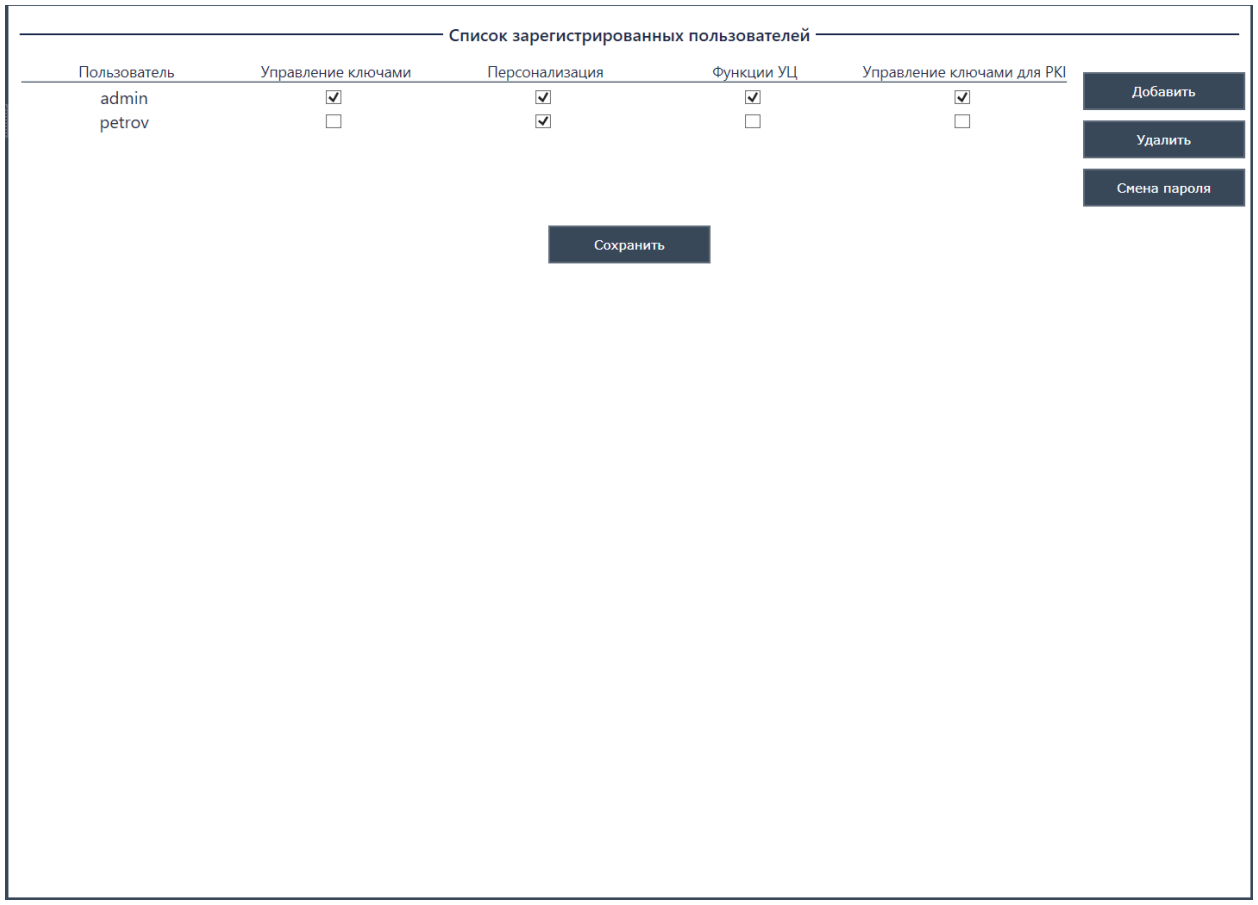
Полномочие	Описание
Управление ключами	Разрешает пользоваться некоторыми кнопками, связанными с ключами, но не только лишь всеми.
Персонализация	Позволяет пользоваться кнопкой «Персонализация», которой у вас нет.
Функции УЦ	Видимо кнопки, в тексте которых есть слова «PKI» и «сертификат» начнут что-то делать, но это не точно.
Управление ключами для PKI	Это запасной вариант: если полномочие «Функции УЦ» не помогло можно попробовать это.

В Криптосервисе всегда есть пользователь admin с максимальными полномочиями. Его нельзя удалить.

В Криптосервисе есть невидимый пользователь Guest, которому доступны «базовые операции» что бы это ни значило.

Операторов можно добавлять, удалять и изменять их полномочия, но нельзя переименовывать.

Рисунок 10 Управление пользователями



Кнопка «Сохранить» определяет пользователей, у которых были изменены полномочия и отправляет запрос на их изменение в Криптосервис.

4.2.4 Экран «Мониторинг криптосервиса»

Экран мониторинга позволяет отслеживать нагрузку и состояние Криптосервиса.

Рисунок 11 Мониторинг Криптосервиса

В верхней части экрана расположена общая информация о работе криптосервиса:

1. Статус *HSM* показывает сколько *HSM* функционируют нормально и сколько их всего.
2. Время непрерывной работы показывает время с последнего перезапуска Криптосервиса.
3. Кол-во открытых *синхронных сессий* показывает сколько сейчас открыто сессий и может служить индикатором зависших сессий.

Далее располагается таблица занятых ресурсов Криптосервиса, которая отображает сколько еще можно создать ключей/пользователей.

Ниже находятся слоистые диаграммы нагрузки, первая показывает нагрузку в сообщениях в секунду. Вторая отражает ту же нагрузку, но в байтах в секунду. Каждый слой соответствует отдельному чипу в *кластере*. Справа от каждой диаграммы находится индикатор суммарной нагрузки, измеряемый в тех же единицах что и соответствующая ему диаграмма.

Так же на экране находится кнопка «Сохранить телеметрию», которая позволяет выгрузить архив телеметрии за выбранный период. Телеметрия сохраняется в формате CSV в:

Таблица 3 Формат телеметрической информации

Timestamp	WrapCnt	WrapData	UnwrapCnt	UnwrapData	ComputeDSCnt	PackKeyCnt

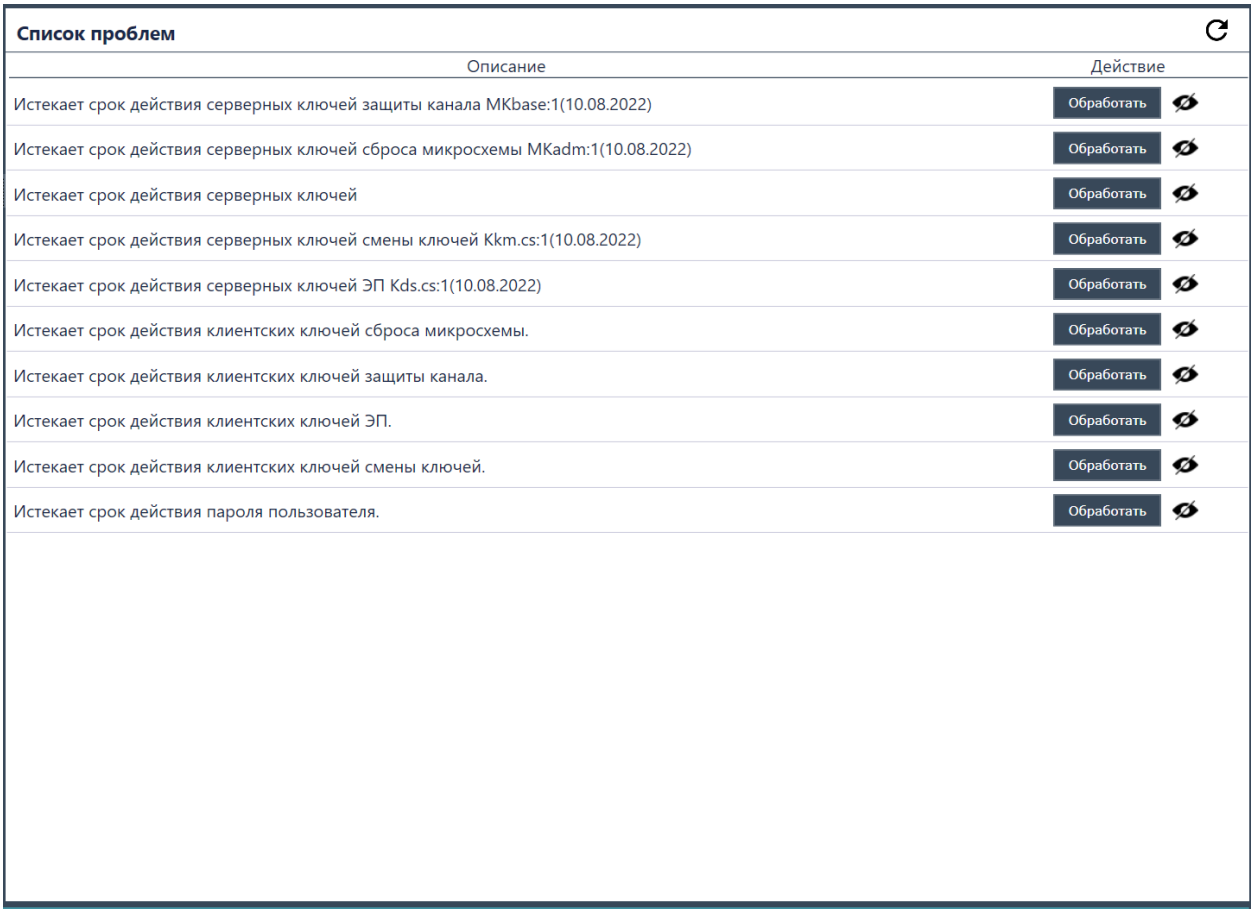
Где

- Timestamp – метка времени в виде Unix Timestamp
- WrapCnt – количество Wrap команд обработанных к моменту Timestamp
- WrapData – объем данных Wrap команд обработанных к моменту Timestamp
- UnwrapCnt – количество Unwrap команд обработанных к моменту Timestamp
- UnwrapData – объем данных Unwrap команд обработанных к моменту Timestamp
- ComputeDSCnt – количество вычисленных Криптосервисом ЭП к моменту Timestamp
- PackKeyCnt – количество административных сообщений смены ключа клиента

4.2.5 Экран «Проблемы»

На экране «Проблемы» отображается информация о ситуациях, возникших в Криптосервисе и которые требуют отклика от администратора. *Проблемы* не хранятся в базе данных, но вычисляются Криптосервисом. Для того чтобы *проблема* перестала генерироваться необходимо предпринять шаги по устранению причины *проблемы*. Удалить *проблему* без ее фактического решения невозможно.

Рисунок 12 Экран Проблемы



АРМ предоставляет информацию о *проблемах*, а также позволяет перейти к объектам, которые задействованы в *проблеме* для ее решения. Также *проблему* можно скрыть, и она перестанет отображаться до следующего обновления списка *проблем*.

Список *проблем* загружается при старте АРМа и при нажатии кнопки обновления, расположенной в правом верхнем углу экрана «Проблемы».

На момент написания документа поддерживаются следующие типы *проблем*:

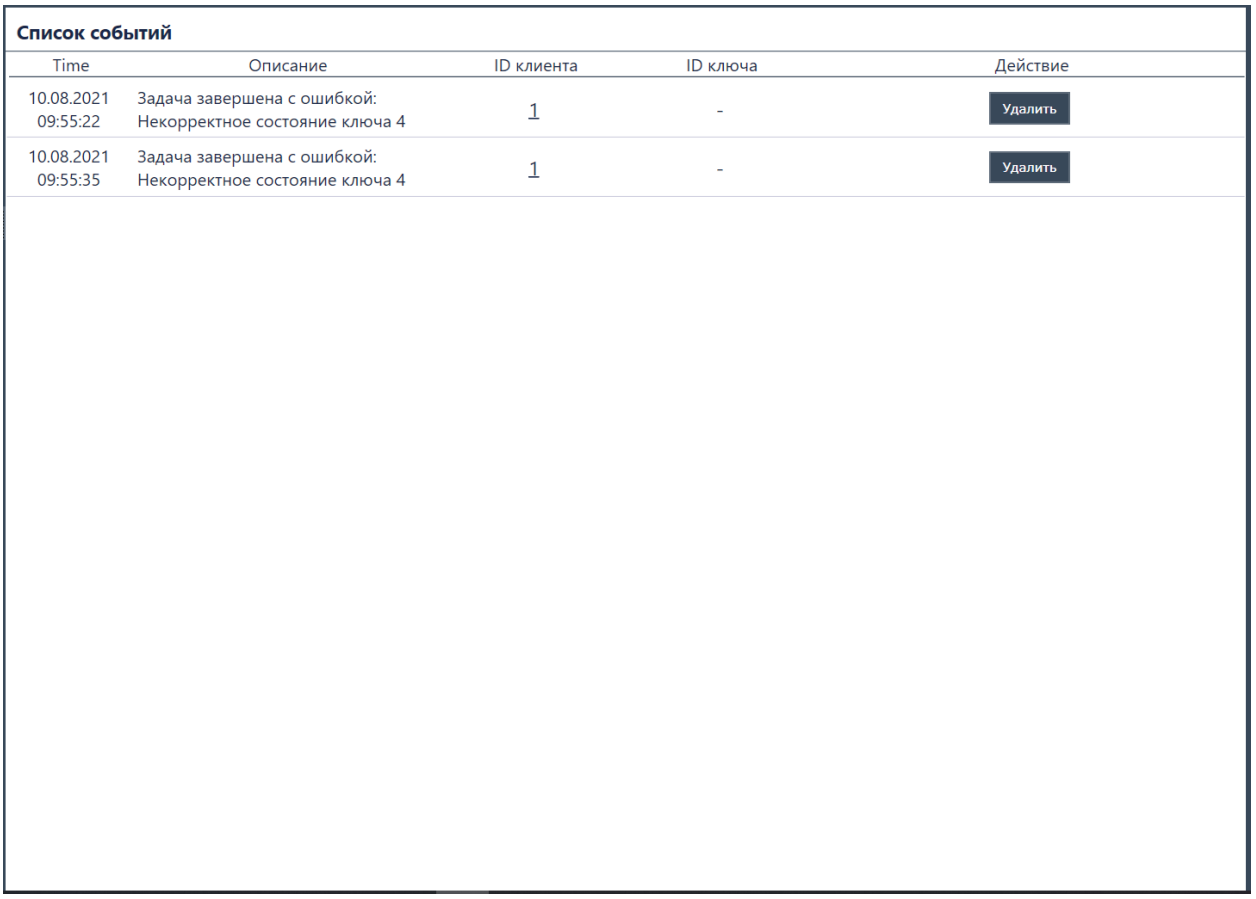
Рисунок 13 Типы проблем

Проблемы	Описание
Истечение срока действия серверного ключа	Возникает за некоторое время (настраивается см. 4.2.8) до истечения серверных ключей
Истечение срока действия клиентского ключа	Возникает за некоторое время (настраивается см. 4.2.8) до истечения клиентских ключей
Истечение срока действия пароля пользователя	Возникает за некоторое время (настраивается см. 4.2.8) до истечения пароля пользователя
Не удалось выполнить задачу	Возникает если были невыполненные задачи

4.2.6 Экран «События»

Экран «События» содержит список *событий*, которые произошли в Криптосервисе за время его работы. *События*, в отличие от *проблем*, носят информационный характер и не требуют отклика оператора. Они хранятся в базе данных криптосервиса до тех пор, пока оператор АРМа не удалит их. *События* также, как и *проблемы* позволяют перейти к связанным объектам.

Рисунок 14 Экран События

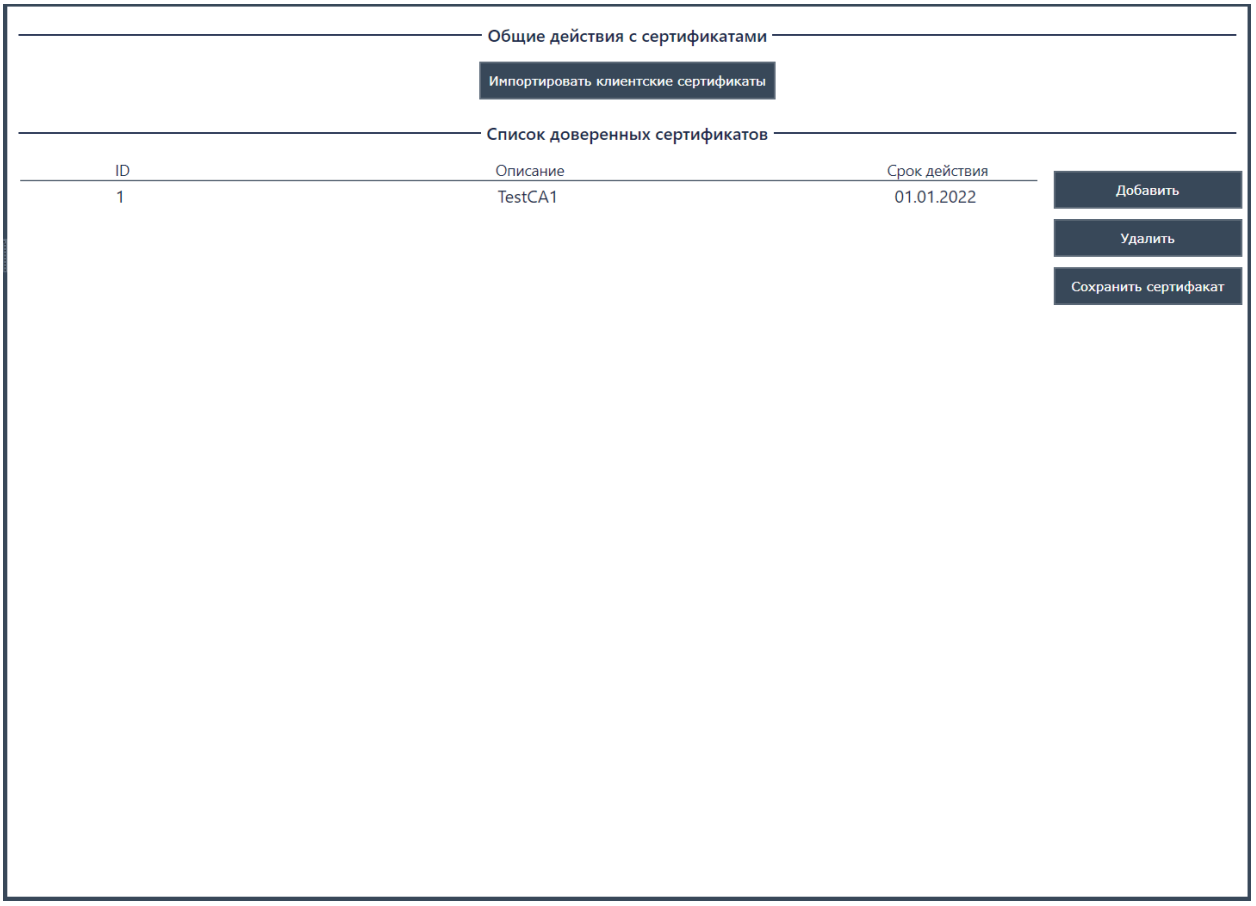


4.2.7 Экран «PKI»

Экран PKI предоставляет доступ к части операций с сертификатами, а именно:

- В верхней части экрана расположена кнопка импорта клиентских сертификатов, которая позволяет выбрать файлы сертификатов для группы клиентов и загрузить их в Криптосервис.
- Ниже располагается таблица загруженных точек доверия. Кнопки справа позволяют добавлять и удалять точки доверия, а также сохранять сертификаты уже загруженных точек доверия.

Рисунок 15 PKI



4.2.8 Экран «Настройки»

Экран настройки предоставляет доступ к части настроек Криптосервиса. Фактическая передача настроек происходит по нажатию кнопки «Применить».

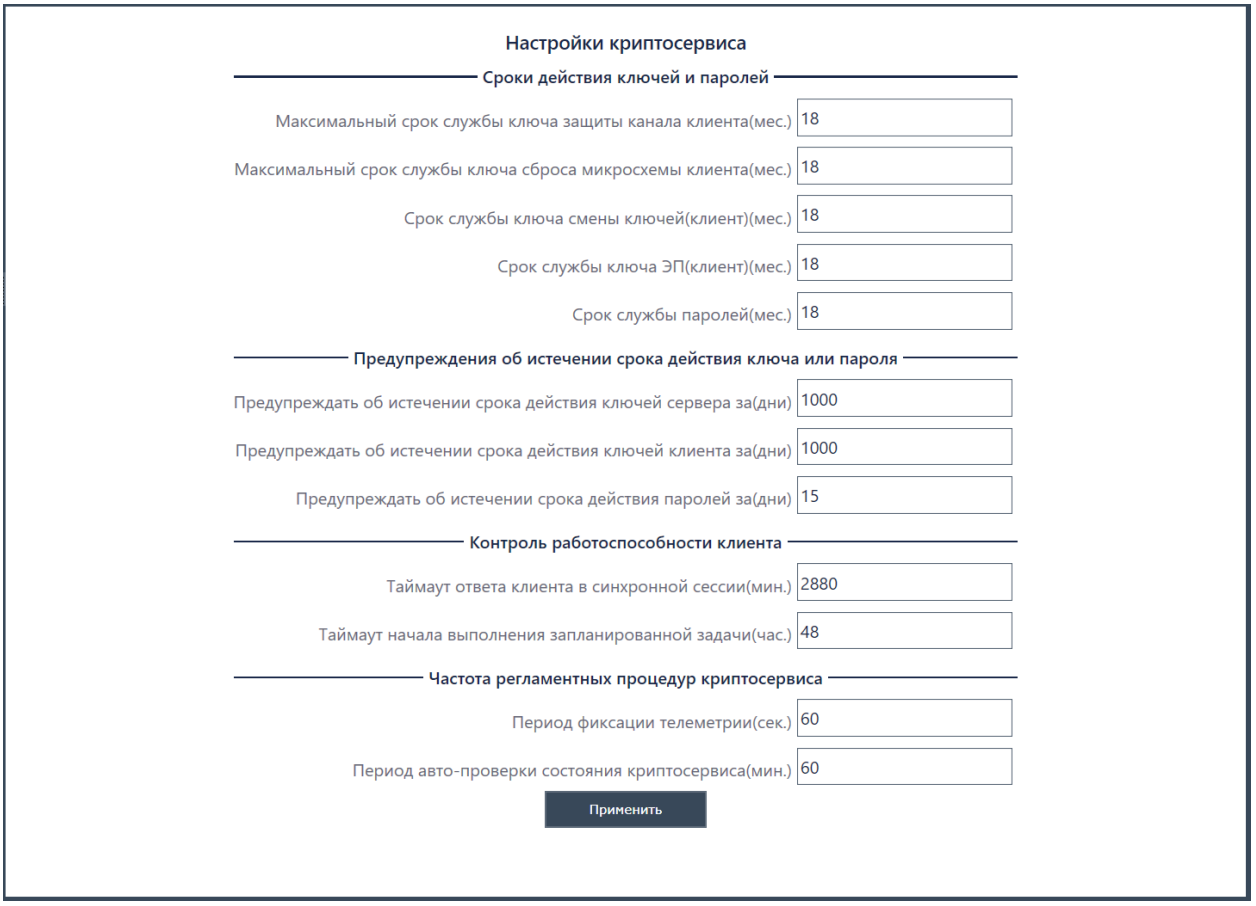
Секция «Сроки действия ключей и паролей» содержит настройки срока действия ключей, создаваемых на экране «Управление ключами» и паролей пользователей на экране «Управление пользователями».

Криптосервис может генерировать *проблемы* (см. Экран «Проблемы») для напоминания оператору о наступлении некоторых событий. Этот механизм можно настроить в секции «Предупреждения об истечении срока действия ключа или пароля».

Для комментария по настройкам из секции «Контроль работоспособности клиента» смотри документацию на Криптосервис.

Секция «Частота регламентных процедур криптосервиса» содержит настройки периодических механизмов Криптосервиса.

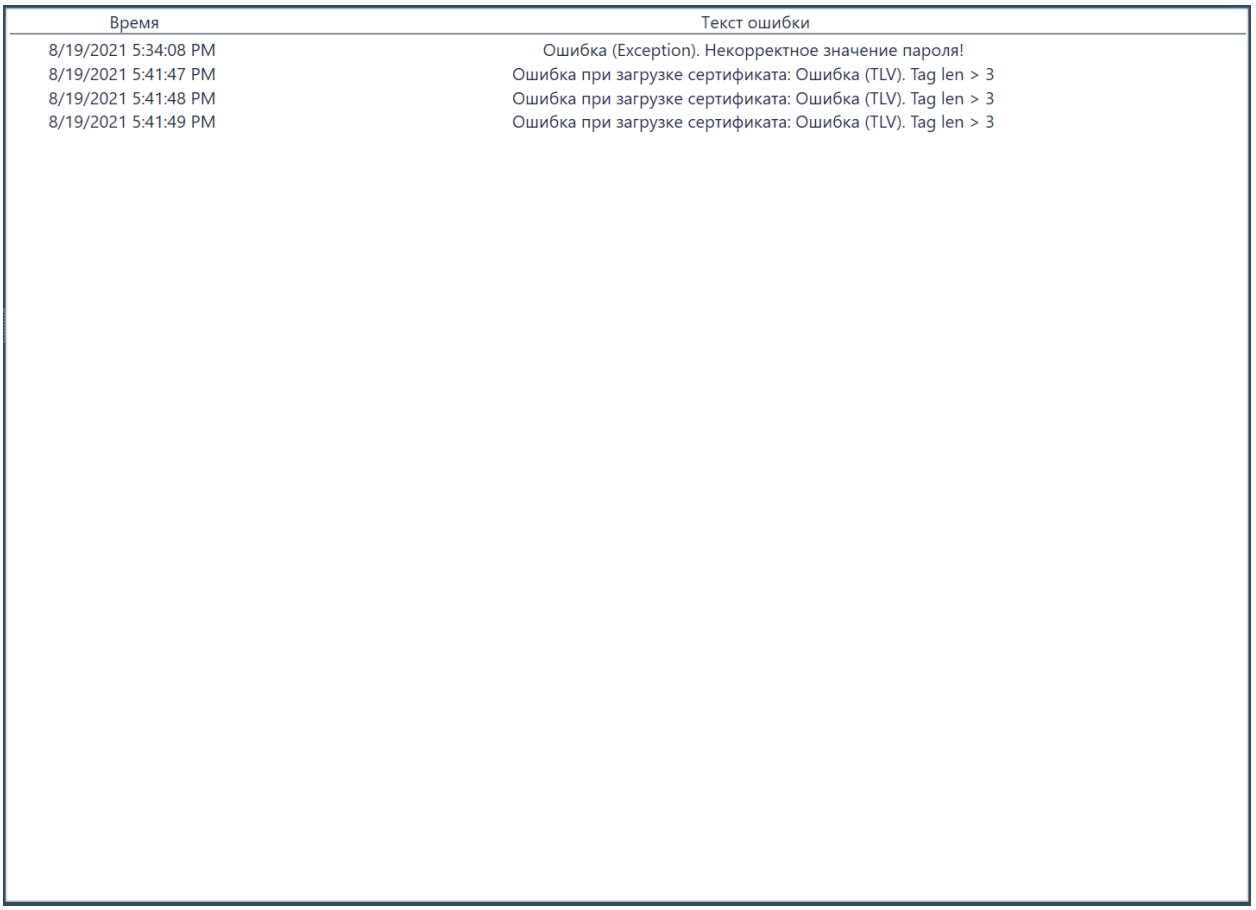
Рисунок 16 Настройки



4.2.9 Экран «Лог»

Экран «Лог» содержит список всех ошибок, которые произошли в ходе работы с *Криптосервисом* в ходе текущей сессии АРМа. При закрытии АРМа лог не сохраняется.

Рисунок 17 Экран "Лог"



5 Распространенные проблемы

5.1 Нет соединения

Стоит проверить, что к Криптосервису никто не подключен по тому же интерфейсу что и АРМ, так как поддерживается только одно подключение в каждый момент времени.

5.2 Пропали клиента

Возможно применен фильтр, стоит проверить информационную зону над списком клиентов.

Ссылки на документы

1. «ПАК Звезда - Техническое описание криптобиблиотеки», НИИМЭ, ПАК Звезда - Техническое описание криптобиблиотеки.docx