GS LABS
GS GROUP

Публичный - L0

ПАК «Криптокипер»

Руководство администратора

Индекс	CryptoKeeper-AG
Конфиденциальность	Публичный - L0
Ревизия	1.2
Статус	Согласован

Содержание

1. Аннотация . . . 3
2. Термины и сокращения . . . 4
3. Введение . . . 6
3.1. Требования к квалификации администратора Cryptokeeper . . . 6
3.2. Системные требования . . . 6
4. Управление устройством на корпусе . . . 7
4.1. Меню текстового дисплея . . . 7
4.2. Управление устройством внутри корпуса . . . 10
5. Удаленное управление устройством . . . 12
5.1. Пользователи устройства . . . 12
5.2. Пользовательский скрипт . . . 13
5.2.1. Перед запуском . . . 13
5.2.2. Опции скрипта - справка . . . 14
5.2.3. Опции скрипта - подключение к устройству . . . 14
5.2.3.1. Обязательные опции . . . 14
5.2.3.2. Необязательные опции . . . 14
5.2.4. Опции скрипта - управление устройством . . . 15
5.2.5. Примеры запросов и ответов . . . 19
5.2.5.1. Сетевые настройки . . . 19
5.2.5.2. Список наборов ipkeys . . . 20
5.2.5.3. Версии ПО . . . 20
5.2.5.4. Клиенты рабочего протокола . . . 20
5.2.6. Коды, возвращаемые скриптом (Exit status) . . . 21
5.2.7. Сообщения об ошибках . . . 21
6. Начальная настройка устройства . . . 24
6.1. Начальные значения параметров . . . 24
7. Возможные проблемы и методы решения . . . 26
8. Обновление программного обеспечения . . . 27

1. Аннотация

Документ предназначен для сотрудников отдела мониторинга и инсталляции, а также для других технических специалистов, в обязанности которых входит настройка продукта ПАК "Криптокипер" (далее - устройство или CryptoKeeper) и поддержание его работоспособности.

2. Термины и сокращения

Термин	Определение
Активный набор IPkeys	Набор ipkeys, который используется на текущий момент в командах рабочего протокола.
Набор IPkeys	Набор промежуточных ключей, участвующих в шифровании данных с помощью Устройства. IPKeys используются для привязки к провайдерам (part type) чипа. IPkeys загружаются и хранятся на Устройстве в зашифрованном виде (с помощью корневых ключей из OTP чипа GS1.
Набор ключей по умолчанию	Файл (или несколько файлов) с наборами ключей (IPkeys), добавленные в прошивки в read-only подписанный/шифрованный раздел. Наборы по умолчанию являются нередактируемыми, и могут быть обновлены только вместе с прошивкой.
Оператор ТВ (TV Provider)	Организация, предоставляющая услуги просмотра цифрового телевидения и использования дополнительных сервисов.
ECM	Сообщение CAS, содержащее служебную информацию и зашифрованные ключи (CW), дескремблирующие транспортный поток.
ECMG	Функциональный компонент CAS в архитектуре DVB-Simulcrypt, генерирующий ECM сообщения, добавляемые в транспортный поток.
EMM	Сообщение CAS, содержащее служебные данные, информацию о правах доступа и специальные команды (активация карты, изменение подписки, обновление операционного ключа и другие).
EMMG	Функциональный компонент CAS в архитектуре DVB-Simulcrypt, генерирующий EMM сообщения, добавляемые в транспортный поток.
OTM	Способ обновления ПО через подключаемый носитель информации. Способ обновления ПО через сеть, также используемый на Устройстве, является частным случаем обновления OTM, при этом используется аналогичный файл обновления, помещаемый на удаленной управляющей рабочей станции.
CryptoKeeper	(ПАК "Криптокипер"). Используется для хранения и обработки секретных данных и ключей шифрования в продуктах "Программный комплекс "Система условного доступа DREGUARD" и "Система управления цифровыми правами DREPLUS".

Сокращение	Расшифровка
API	Application Programming Interface
BL	Bootloader
CAS	Conditional Access System
DRM	Digital Right Management

MW	Middleware
OTP	One-Time Programmable
WDT	Watchdog Timer

3. Введение

ПАК "Криптокипер" (далее - устройство или CryptoKeeper) представляет собой программно-аппаратное решение на базе чипа GS1, используемое для хранения и обработки секретных данных и ключей шифрования в системах CAS/DRM.

> ⚠ В связи с постоянным совершенствованием продукта, в т.ч. интерфейса на корпусе Устройства, могут иметь место незначительные несоответствия описания и фактического функционирования/внешнего вида интерфейса, НЕ ВЛИЯЮЩИЕ НА ОСНОВНОЙ ФУНКЦИОНАЛ ПРОДУКТА.

3.1. Требования к квалификации администратора Cryptokeeper

Администратор Системы должен обладать навыками:

- Работа со скриптами Python.
- Настройка сетевых подключений.

3.2. Системные требования

Рабочая станция, с которой будет осуществляться управление Устройством, должна обладать следующими характеристиками:

- Наличие сетевого интерфейса Ethernet.
- Операционная система: *Microsoft Windows* или *Linux* (для управления с помощью скрипта).
- Установленный *Python 3.7* или выше.
- Установленная библиотека *requests* для *Python*. Версия - не ниже 2.25.1.

  > ⓘ Установить библиотеку можно, выполнив команду: pip install requests

4. Управление устройством на корпусе

В одном корпусе стандартного серверного размера 1U помещаются два полностью независимых устройства Cryptokeeper. Далее следует описание для одного устройства, при этом подразумевается, что в каждом корпусе присутствует 2 комплекта соответствующих органов коммутации, индикации и управления.

На задней панели расположен разъем для подключения кабеля питания устройства (220В).

На передней панели расположены органы управления и индикации. Внешний вид передней панели представлен на рисунке:

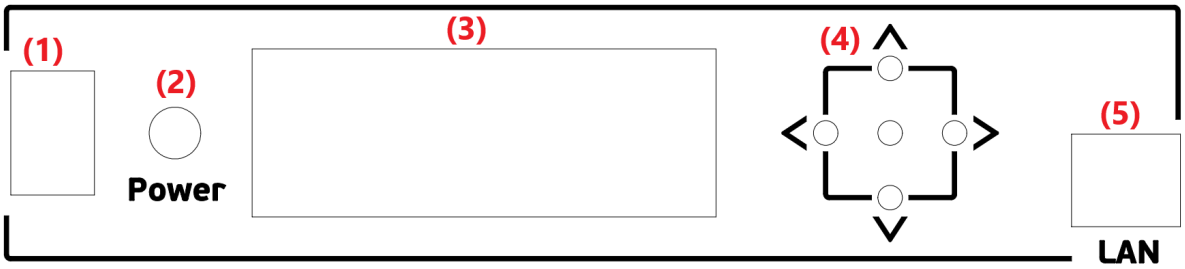

Рис. 2.1. Передняя панель Устройства.

Цифрами на рисунке 2.2 обозначены:

- Выключатель питания (поз. 1) - механический, отключающий питание 220В.
- Светодиодный индикатор включения и статуса (поз. 2) - светится зеленым светом, если Устройство включено и функционирует нормально, светится желтым светом, если в процессе обновления ПО Устройства произошел сбой.
- Двухстрочный текстовый дисплей для отображения основных параметров работы Устройства (поз. 3) - включается при включении питания, а также после нажатия любой из кнопок навигации. Далее, если в течении 15сек. не нажималась ни одна кнопка навигации, изображение с дисплея исчезает, подсветка остается включенной.
- Кнопки для навигации по меню параметров и перезагрузки Устройства (поз. 4) - с помощью кнопок Вверх (/\), Вниз (\/), Влево(<), Вправо(>) выбираются разделы и экраны внутри разделов меню. Средняя кнопка (OK, без обозначения) служит для подтверждения выбора при работе с разделом перезагрузки.
- Разъем RJ-45 (поз. 5) - служит для подсоединения Устройства к LAN. Через сетевой интерфейс происходит связь Устройства с клиентами, а также удаленное управление Устройством.

4.1. Меню текстового дисплея

С помощью текстового дисплея на корпусе Устройства возможны:

- Просмотр текущего IP-адреса и статуса Устройства.
- Просмотр текущих параметров подключения Устройства к сети обмена данными (IP, маска подсети, шлюз, номера портов для работы и управления).
- Просмотр доступных на Устройстве наборов ключей и их параметров.
- Просмотр номеров версий ПО и параметров запуска Устройства.
- Просмотр количества и параметров подключения (IP-адрес + порт) клиентов Устройства.
- Управление перезагрузкой Устройства.

Отображение основных параметров работы Устройства на двухстрочном текстовом дисплее разбито на разделы, каждый из которых может включать несколько переключаемых экранов (см. далее).

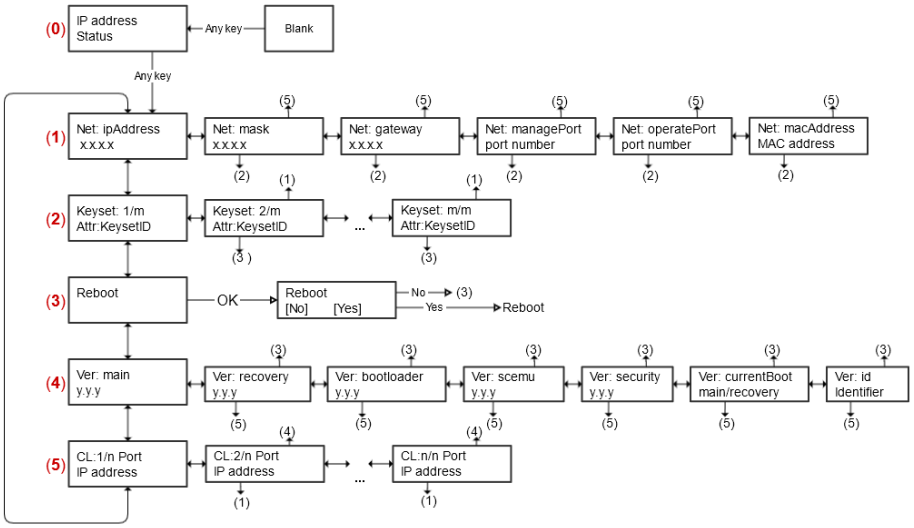

Рис. 2.2. Схема разделов меню дисплея.

Особенности использования меню дисплея:

1. Переход между разделами производится кнопками *Вверх*, *Вниз*. Движение происходит по кольцу.
2. Переход между экранами раздела производится кнопками *Вправо*, *Влево*. При этом:
    - Переход не закольцован.
    - Нажатие кнопки *Вверх* или *Вниз* при нахождении на любом из экранов раздела приводит к переходу к первому экрану предыдущего или следующего раздела меню.
      На рис. 2.2 первые экраны разделов меню пронумерованы. Стрелки, указывающие на цифры, обозначают переход к соответствующему экрану при нажатии кнопок *Вверх*, *Вниз*.
3. После включения Устройства, на дисплее показывается экран статуса (рис. 2.2, поз.0). При нахождении на данном экране, нажатие любой кнопки навигации переводит к первому экрану раздела Net (рис. 2.2, поз.1). В дальнейшем, при перемещении по меню, экран статуса не показывается.
4. Таймауты:
    a. При нахождении на любом экране меню, кроме экрана статуса, в отсутствие нажатий на кнопки навигации в течение 120 сек., происходит переход к экрану статуса.
    b. При нахождении на экране статуса, в отсутствие нажатий на кнопки навигации в течение 15 сек., изображение с дисплея исчезает. В режиме отсутствия изображения (показан на рис. 2.2 как 'Blank'), нажатие на любую из кнопок навигации вызывает показ экрана статуса.

⚠ В некоторых ситуациях возможна задержка реакции устройства на нажатие кнопок навигации. Длительность такой задержки может достигать 1сек., что не является неисправностью. В течение периода задержки, команды нажатий кнопок не "накапливаются" - следует дождаться реакции устройства на предыдущее нажатие, а затем производить последующие.

Экран статуса (IP address/Status) отображает:

- 1я строка - текущий IP-адрес Устройства.
- 2я строка - текущий статус устройства: *No alarm* - ошибок в работе нет, *(код ошибки)* - в процессе обновления ПО устройства произошла ошибка, код которой показывается на дисплее.

Экраны раздела Net отображают текущие значения параметров сетевого подключения Устройства. 1я строка - название параметра, 2я строка - значение параметра:

- *Net:ipAddress* - текущий IP-адрес Устройства.
- *Net:mask* - текущую маску подсети Устройства.
- *Net:gateway* - текущий IP-адрес шлюза.
- *Net:managePort* - номер порта для управления Устройством через управляющий протокол.
- *Net:operatePort* - номер порта для работы клиентов с Устройством через рабочий протокол.
- *Net:macAddress* - MAC-адрес Устройства.

Экраны раздела Keyset отображают количество и свойства наборов IP-ключей на Устройстве:

- Один экран соответствует одному набору IP-ключей.
- В 1й строке отображается порядковый номер набора ключей/общее количество наборов ключей.
- Во 2й строке отображаются свойства набора ключей и его идентификатор (keysetID) в формате:
  - первый символ - признак активности набора (прочерк - неактивный, A(ctive) - активный);
  - второй символ - признак, показывающий, является ли набор нередактируемым (прочерк - редактируемый, R(ead only) - только для чтения). Нередактируемыми (только для чтения) являются наборы, загруженные при прошивке Устройства;
  - после двоеточия отображается идентификатор набора (keysetID).

> Примеры отображения:
>
> **AR:48** - набор 48 является активным и нередактируемым.
>
> **--:50** - набор 50 является неактивным и редактируемым.

Экраны раздела Reboot служат для перезагрузки Устройства, которая производится следующим образом:

1. Нажатием средней кнопки (OK) перейдите к экрану выбора решения.
2. Кнопками Влево/Вправо выберите решение: *No* - не выполнять перезагрузку (по умолчанию), *Yes* - перезагрузить Устройство.
3. Подтвердите выбор средней кнопкой (OK).
4. Если было выбрано *Yes*, Устройство перезагрузится, после чего будет показан экран статуса (см. выше). Если было выбрано *No*, показывается начальный экран раздела Reboot, от которого возможен переход к другим разделам меню.

Экраны раздела Ver (версия) отображают номера версий компонентов ПО, а также название раздела памяти, из которого произошла загрузка устройства. 1я строка - название параметра, 2я строка - значение параметра:

- Ver: main - версия ПО в основном разделе Linux/RootFS.
- Ver: recovery - версия ПО вспомогательного (аварийного) раздела Linux/RootFS.
- Ver: bootloader - версия ПО загрузчика.
- Ver: scemu - версия ПО компонента SCEMU.
- Ver: security - т.н. "защитная версия ПО": версия системы безопасности для защиты Устройства от "отката прошивки".

- Ver: currentBoot - название раздела памяти, из которого произведена загрузка устройства. *main* - загрузка произведена из основного раздела, нормальная работа; *recovery* - загрузка произведена из вспомогательного раздела.

⚠ При загрузке из вспомогательного раздела работа устройства с клиентами по рабочему протоколу невозможна. Такой режим предназначен только для возможности обновления ПО.

- Ver: id - значение идентификатора чипа в формате HEX (4 байта). Значение идентификатора записывается при производстве чипа и уникально для каждого экземпляра Устройства.

  ⓘ Для справки: является аналогом идентификатора CAS ID для приемников на базе чипа GS1, берутся последние 4 байта.

Экраны раздела CL (Client) отображают количество, порты и IP-адреса подключения клиентов, работающих с Устройством:

- Один экран соответствует одному клиенту.
- В 1й строке отображается порядковый номер клиента/общее количество подключенных клиентов, а далее - номер порта подключения на стороне клиента.
- Во 2й строке отображается IP-адрес клиента.
  Пример отображения:
  CL:2/38 45464 - клиент с порядковым номером 2 из 38 подключенных, номер порта клиента 45464.
  192.168.217.136 - IP-адрес клиента.

⚠ Максимальное число одновременно подключенных клиентов равно 100. Попытки установки 101-го подключения будут проигнорированы Устройством.

4.2. Управление устройством внутри корпуса

При необходимости, возможна перезагрузка Устройства или сброс к заводским настройкам с помощью кнопок внутри корпуса. Также внутри корпуса расположен разъем USB, через который, используя флеш-накопитель, можно обновить ПО устройства.

Для доступа к кнопкам и порту USB, откройте корпус, сняв верхнюю крышку. Внешний вид платы Устройства со снятой верхней крышкой показан на рисунке:

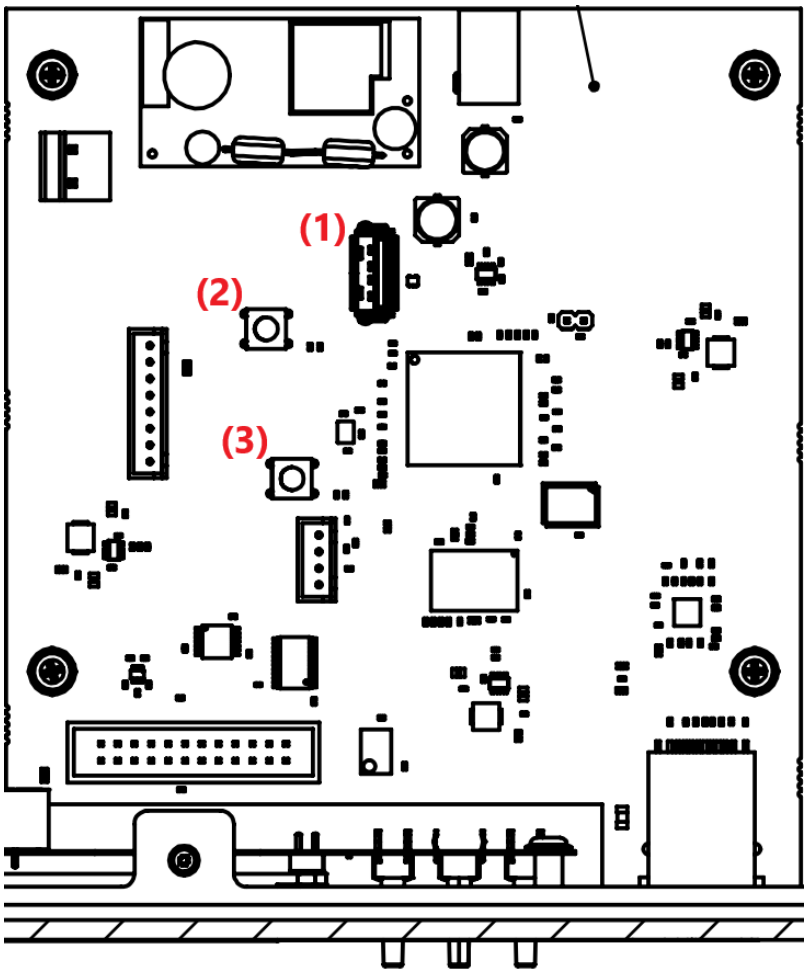

Рис. 2.3. Внешний вид основной платы Устройства со снятой верхней крышкой.

Выполните нужную операцию:

1. Перезагрузите Устройство кратковременным нажатием на кнопку *Reset* (на рис. 2.3, поз. 3), расположенную на печатной плате. При этом на дисплее Устройства в течение нескольких секунд могут сохраняться данные, отображенные перед процедурой сброса, однако после этого будет отображен экран статуса.
2. Выполните сброс Устройства к заводским настройкам. Для этого:
    a. нажмите кнопку *FactReset* (рис. 2.3,поз. 2) на печатной плате Устройства;
    b. кнопками Влево/Вправо на передней панели Устройства выберите решение, отображаемое на дисплее передней панели: *No* - не производить сброс к заводским настройкам (по умолчанию), *Yes* - произвести сброс к заводским настройкам;
    c. подтвердите выбор средней кнопкой (OK);
    d. если было выбрано *Yes*, настройки будут сброшены к заводским, Устройство перезагрузится, после чего будет показан экран статуса (см. выше). Если было выбрано *No*, на дисплее показывается экран статуса (см. выше). Также экран статуса будет отображен, если в течение 15 секунд не было выбрано ни одно из решений.
3. Произведите обновление ПО Устройства, подключив флеш-накопитель с файлом обновления к порту USB (рис. 2.3, поз. 1). Подробнее см. в документе "ПАК "Криптокипер. Руководство по установке ПО".

5. Удаленное управление устройством

Управление всеми параметрами Устройства осуществляется удаленно через REST API на базе протокола HTTPS.

⚠ Перед началом работы с Устройством проверьте наличие файлов (предоставляются заказчику при поставке устройства):

1. Пользовательского скрипта: *ck3_user.py* (описание работы с пользовательским скриптом приводится ниже в настоящем документе).
2. Цепочки публичных SSL сертификатов: *client_ca_chain.pem*.

5.1. Пользователи устройства

Управление Устройством возможно от лица пользователей, имеющих фиксированные логины и уникальные пароли. При этом различаются полномочия каждого из пользователей на доступ к определенным функциям управления. Ниже приводится описание пользователей и их доступа к функциям управления.

Роли (пользователи):

- *keyholder*: управление наборами ключей.
- *configure*: управление настройками (кроме изменения наборов ключей).
- *monitor*: чтение некоторых параметров, просмотр статистики.

Легенда:

	доступ закрыт
	доступ открыт

	Команды	**логин "keyholder"**	**логин "configure"**	**логин "monitor"**
1	Получить сетевые настройки			
2	Установить сетевые настройки			
3	Получить порт для рабочего протокола			
4	Установить порт для рабочего протокола			
5	Получить порт для управляющего протокола			
6	Установить порт для управляющего протокола			

7	Получить список IP-адресов подключенных клиентов			
8	Получить список наборов ключей			
9	Установить активный набор ключей ipkeys			
10	Добавить набор ключей			
11	Удалить набор ключей			
12	Получить версии ПО			
13	Обновить ПО			
14	Получить прогресс обновления			
15	Перезагрузить устройство			
16	Установить пароль пользователя			
18	Сбросить настройки на заводские			
19	Включить экран статуса на дисплее для быстрого нахождения Устройства в стойке			
20	Сменить пароль рабочего протокола			

⚠ Логины пользователей фиксированы, не подлежат изменению.

5.2. Пользовательский скрипт

Для упрощения работы пользователей с управляющим протоколом Устройства, разработан python-скрипт, описываемый ниже. Скрипт запускается на рабочей станции, с которой осуществляется управление Устройством. Скрипт предоставляется при поставке устройства заказчику.

5.2.1. Перед запуском

Для работы скрипта необходимо:

- Убедиться, что на рабочую станцию, с которой запускается скрипт, установлен Python3 (3.7 или выше).
- Убедиться что установлена библиотека requests.

  ⚠ Если библиотека не установлена, это можно сделать выполнив команду: *pip install requests*

- Убедиться, что файл скрипта *ck3_user.py* присутствует на управляющей рабочей станции.
- Убедиться, что в одной директории с файлом скрипта находится файл цепочки публичных SSL сертификатов: *client_ca_chain.pem*.

⚠

- Файл должен иметь расширение ".pem".
  Если файл отсутствует, то запуск скрипта завершится с ошибкой: *Couldn't find a certificate matching the mask ".pem"*

  Если файлов с таким расширением в директории будет несколько - скрипт будет использовать первый найденный, с выдачей сообщения: *File "FILENAME" will be used as a client certificate*.

5.2.2. Опции скрипта - справка

Скрипт может быть вызван со специальными справочными опциями, без каких-либо других опций и команд, в т.ч. обязательных.

Опция	Описание
`--help` `-h`	Показывает справку по скрипту
`--version`	Показывает версию пользовательского скрипта

5.2.3. Опции скрипта - подключение к устройству

⚠ Значение опции задаётся через пробел.

5.2.3.1. Обязательные опции

Следующие опции должны быть в каждом вызове скрипта для управления Устройством или получения информации об Устройстве:

Опция	Значение	Описание	Примечание
`--user` `-u`	CK_USER	Имя пользователя для подключения к Устройству	Доступные значения CK_USER: `keyholder, configure, monitor`

5.2.3.2. Необязательные опции

Если опции, описанные ниже, не заданы, используются значения по умолчанию.

Опция	Значение	Описание	Примечание

`--address`
 	
`-a`
	`CK_HOSTNAME[:PORT]`	Имя хоста для подключения к Устройству
		
		Через двоеточие можно задать управляющий порт для подключения
			`CK_HOSTNAME` можно задать как с префиксом "https://" так и без него
			
			Если задать префикс "http://", то скрипт завершится с ошибкой: `Only HTTPS is supported`
			
			Если `PORT` не задан, то будет использовано значение по-умолчанию - ":443"
			
			По умолчанию, в качестве доменного имени используется IP адрес: 192.168.2.2
			
			Можно использовать доменное имя, соответствующее шаблону "*.ck3.device". Например, "default.ck3.device".
			
			Для подключения к Устройству по доменному имени, необходимо указать это имя в системном файле "hosts" на ПК пользователя.

5.2.4. Опции скрипта - управление устройством

⚠

1. Значение опции задаётся через пробел.
2. Для полноценного удаленного управления Устройством должна быть произведена его начальная настройка, как описано в главе "Начальная настройка" настоящего документа.

Только одна опция из таблицы ниже может быть передана за один вызов скрипта

Опция	Значение	Описание	Примечание	Пользователи, которым доступна команда*

`--network`
 	
`-n`
		Показывает текущие сетевые настройки Устройства		keyholder
				configure
				monitor

`--set-network`	`[IP]:[MASK]:[GW]`	Меняет "ipAddress", "mask", "gateway" Устройства на переданные `IP:MASK:GW`	Если нужно поменять меньше настроек, то можно передать только значения изменяемых настроек, оставив значения неизменяемых пустыми. Например, чтобы поменять только "ipAddress" и "gateway", не меняя "mask", следует передать: `IP::GW` Каждое значение (`IP, MASK, GW`) должно соответствовать формату: xxx.xxx.xxx.xxx , где xxx - десятичное число от 0 до 255.	configure
`--set-manage-port`	`PORT`	Меняет "managePort" (порт управляющего протокола) Устройства на `PORT`	`PORT` должен быть десятичным числом от 0 до 65535.	configure
`--set-operate-port`	`PORT`	Меняет "operatePort" (порт рабочего протокола) Устройства на `PORT`	`PORT` должен быть десятичным числом от 0 до 65535.	configure

`--keysets`
 	
`-k`
		Показывает текущие наборы ключей ipkeys на Устройстве		keyholder configure

`--add`	`KEYFILE[:SIGNFILE]`	Добавляет набор ключей Через двоеточие можно задать файл, содержащий подпись для набора. **Примечание.** Добавление набора ключей приведет к закрытию всех соединений рабочего протокола.	`KEYFILE` не должен иметь расширение ".sig" Если `SIGNFILE` не задан, скрипт будет искать его по шаблону `KEYFILE + '.sig'` Например, если передан только `KEYFILE` с именем "ipkeys1.txt", то скрипт будет в той же директории искать `SIGNFILE` сначала по имени "ipkeys1.txt.sig", затем по имени "ipkeys1.sig"	keyholder

`--delete`	`ID`	Удаляет набор по ID. **Примечание.** Удаление набора ключей повлечет за собой закрытие всех соединений рабочего протокола.	Id набора ключей ipkeys, должен быть десятичным числом	keyholder
`--activate`	`ID`	Активирует набор по ID. **Примечание.** Смена активного набора повлечет за собой закрытие всех соединений рабочего протокола.	Id набора ключей ipkeys, должен быть десятичным числом	keyholder
`--update`	`UPDATE_FILE`	Начинает обновление ПО Устройства	После передачи файла, начинается процесс обновления ПО Устройства. Прогресс обновления выводится в консоль, выполнение других команд будет заблокировано. Если во время обновления произойдет ошибка (неверная подпись файла обновления, и т. п.), то обновление прервётся, в консоль будет выведен текст ошибки и её код. Если во время обновления прервать выполнение скрипта обновление не прервётся. Статус обновления можно будет узнать командой `--update-status`	configure
`--update-status`		Показывает статус обновления	Если попытки обновления не было, возвращает "Update not started" Если происходит обновление, показывает стадию обновления и процент Если последняя попытка обновления завершилась с ошибкой, показывает текст и код ошибки	configure

`--versions`
 	
`-v`
		Показывает версии ПО Устройства, и раздел с которого была произведена загрузка		keyholder
				configure
				monitor

`--clients`
 	
`-c`
		Показывает список клиентов рабочего протокола Устройства. По каждому клиенту возвращается информация в формате: IP-адрес: порт.		keyholder
				configure
				monitor

`--reboot`
 	
`-r`
		Перезагружает Устройство		keyholder
				configure
				monitor

`--factory-reset`		Сбрасывает Устройство к заводским настройкам	После вызова команды и ввода пароля, пользователь получит предупреждение и место для ввода ответа:
			
			`Caution! Can't be undone! Are you sure you want to restore factory settings? (yes - continue)`
			`Answer:`
			
			Ответ `"yes"` - произойдет сброс к заводским настройкам.
			
			Любой другой ответ - пользователь получит сообщение: `Factory reset canceled!`
				configure

`--set-password`		Меняет пароль пользователя	После вызова команды, пользователь должен будет сначала ввести текущий пароль (чтобы запрос был принят Устройством), после этого дважды ввести новый пароль для пользователя CK_USER Пароль должен отвечать следующим требованиям: • длина пароля: от 8 до 15 символов, в пароле должны быть 1 заглавная буква, 1 цифра, 1 символ. • допустимые символы: латинские строчные и прописные буквы (a-z, A-Z), цифры 0-9, символы !@#$%&*()-=_+	keyholder configure monitor
`--wakeup` `-w`		Включает отображение экрана статуса на дисплее Устройства	Опция должна облегчить поиск конкретного Устройства в стойке	keyholder configure monitor
`--set-authkey`		Меняет пароль рабочего протокола (auth-ключ для протокола 0xCF)	Опция не принимает значений, после вызова опции появляется место для ввода auth-ключа. Формат auth-ключа: hex-строка, 16 байт	keyholder configure

* *Примечание:* пользователи, которым закрыт доступ, могут вызвать команду, но получат ошибку: `"No user permission for call this command"`

5.2.5. Примеры запросов и ответов

5.2.5.1. Сетевые настройки

Запрос:

```
./ck3_user.py --user configure --network
```

Ответ:

```
ipAddress: 192.168.2.2
mask: 255.255.255.0
gateway: 192.168.2.0
managePort: 443
operatePort: 49999
macAddress: 00:23:7c:f5:c4:99
```

5.2.5.2. Список наборов ipkeys

Запрос:

```
./ck3_user.py --user keyholder --keysets
```

Ответ:

```
23 readOnly active
48 readOnly
52
53
```

5.2.5.3. Версии ПО

Запрос:

```
./ck3_user.py --user monitor --versions
```

Ответ:

```
bootloader: 1.0.3
currentBoot: main
id: 2F000011
main: 0.1.9
recovery: 0.0.1
scemu: 1.0.0
security: 0
```

5.2.5.4. Клиенты рабочего протокола

Запрос:

```
./ck3_user.py -u monitor --clients
```

Ответ:

```
192.168.2.3:57830
192.168.2.3:57836
192.168.2.3:57350
192.168.2.3:57366
```

5.2.6. Коды, возвращаемые скриптом (Exit status)

При завершении работы скрипт возвращает следующие коды:

- 0 - операция выполнена успешно;
- 1 - ошибка на стороне скрипта (неправильный вызов параметра, ошибка во вводимых значениях и т.п.);
- 2 - ошибка на стороне Устройства (недопустимое действие для пользователя, неверный пароль и т.п.).

5.2.7. Сообщения об ошибках

Если скрипт завершает свою работу с кодом 1 (ошибка в вызове скрипта, см. выше), на экране показывается одно из следующих сообщений об ошибках:

Сообщение	Описание
Only one command is allowed at a time	Скрипт вызван с более чем одной опцией - командой управления
Couldn't find a certificate matching the mask '.pem'	Скрипт не может найти файл с ca-chain. Требуется чтобы файл был в одной директории со скриптом и имел расширение '.pem'
Only HTTPS is supported	В опцию --address передано CK_HOSTNAME, начинающееся с префикса 'http:'. Устройство поддерживает только 'https'
Incorrect hostname in address: {ADDRESS}	В опцию --address передано пустое значение CK_HOSTNAME
The password contains unsupported characters	Введенный пароль содержит недопустимые символы
No ping to host {HOSTNAME}	В текущий момент устройство не доступно по адреccу HOSTNAME
Incorrect data: {DATA} You must submit three parameters separated by colon. If you want to submit fewer parameters, leave the unnecessary fields blank. For example, you want to change only 'gateway', then the line should be like "::GATEWAY"	В опцию --set-network передано [IP]:[MASK]:[GW] с неправильным количеством разделителей ":". Разделителей должно быть два, даже если необходимо передать меньше значений.
Nothing to change	В опцию --set-network передано [IP]:[MASK]:[GW] не содержащее самих значений, только разделители - "::"

The '{DATA}' parameter is invalid	В опцию --set-network передано [IP]:[MASK]:[GW] с неправильным параметром. Каждый из параметров IP, MASK и GW должен либо отсуствовать, либо содержать три точки и состоять из чисел от 0 до 255.
Incorrect data: {DATA} The port number must be in range from 0 to 65535	В опцию --set-manage-port или --set-operate-port передано недопустимое значение PORT. PORT должен быть числом от 0 до 65535
Incorrect data: {DATA} Keyfile name can't be empty.	В опцию --add передано KEYFILE[:SIGNFILE], в котором KEYFILE - пустое значение
Incorrect data: {DATA} Keyfile name can't end with '.sig'.	В опцию --add передано KEYFILE[:SIGNFILE], в котором KEYFILE имеет недопустимое расширение '.sig'
Incorrect data: {DATA} If you want to submit only keyfile, then there must be only it (without colon). For example --add KEYFILE_NAME If you want to submit both keyfile and signfile, then the keyfile must go first, then colon, and then signfile. For example --add KEYFILE_NAME:SIGNFILE_NAME	В опцию --add неверно передано значение KEYFILE[:SIGNFILE]. Например вот так: ck3_user.py -u keyholder --add keyfile.json::
Keyfile "{KEYFILE}" not found.	В опцию --add передано имя файла с набром ключей KEYFILE , но файл с таким именем не найден.
SignFile "{SIGNFILE}" not found.	В опцию --add передано имя файла подписи SIGNFILE, но файл с таким именем не найден, либо не удалось найти файл подписи по шаблону.
Incorrect data: {DATA} KeysetID must be a positive number.	В опцию --delete или --activate передано значение keysetID , не являющееся положительным числом.
Update file "{FILE}" not found.	В опцию --update передано значение UPDATE_FILE, не являющееся существующим файлом
Update error: {TEXT} (code {CODE})	В опцию --update передан UPDATE_FILE, являющийся невалидным для обновления ПО. Причина невалидности указана в {TEXT}

Factory reset cancelled!	После вызова опции --factory-reset, пользователь получил предупреждение о необратимости операции а так же вопрос об уверенности в своих действиях. На этот вопрос пользователь дал ответ отличный от 'yes'
The entered passwords do not match!	После вызова опции --set-password, пользователь вводит сначала свой текущий пароль, затем два раза вводит новый пароль. Если новые пароли не совпадают, пользователь увидит это сообщение.
Impossible combination!	Недопустимая комбинация параметров. Если сообщение повторяется, обратитесь к разработчику скрипта, приведя пример запуска или комбинацию опций и значений, после которого появилось это сообщение.

6. Начальная настройка устройства

Перед использованием Устройства необходимо выполнить его начальную настройку. В противном случае работа Устройства будет невозможна. Необходимые для настройки шаги описаны ниже.

1. Через ethernet соединить Устройство с рабочей станцией, с которой будет производиться настройка.
2. Настроить сетевое подключение рабочей станции к Устройству с использованием IP-адреса Устройства, отображаемого на экране статуса (см. также раздел "Начальные значения параметров" в настоящем документе).
3. Поместить на рабочей станции файлы пользовательского скрипта и сертификатов. См. раздел "Пользовательский скрипт" настоящего документа.
4. С помощью пользовательского скрипта получить значения версий ПО Устройства. Этим проверяется связь рабочей станции с Устройством.
5. С помощью пользовательского скрипта сменить пароли всех пользователей.

   ⚠
   - Пароль должен отвечать следующим требованиям:
     - длина пароля: от 8 до 15 символов, в пароле должны быть 1 заглавная буква, 1 цифра, 1 символ.
     - допустимые символы: латинские строчные и прописные буквы (a-z, A-Z), цифры 0-9, символы !@#$%&*()-=_+
   - До смены паролей всех пользователей, работа Устройства с клиентами и настройка остальных параметров невозможны.
   - После смены паролей всех пользователей Устройство готово к работе и изменению настроек, перезагрузка не требуется.
   - Пароли пользователей Устройства должны быть уникальными.
   - В целях безопасности, рекомендуется также устанавливать уникальные пароли пользователей для разных экземпляров Устройства.

6. При необходимости, с помощью пользовательского скрипта изменить сетевые настройки Устройства, добавить наборы ключей и изменить их параметры.

Описание настроек Устройства см. в разделе "Пользовательский скрипт" настоящего документа.

6.1. Начальные значения параметров

По умолчанию, в ПО Устройства заданы следующие значения параметров:

1. Сетевые настройки:
   a. IP-address: 192.168.2.2
   b. Netmask: 255.255.255.0
   c. Gateway: not used
      - означает, что шлюз по умолчанию не установлен / не используется
   d. Port для рабочего протокола 49999
   e. Port для управляющего протокола: 443
2. Наборы ключей:
   a. по умолчанию в rootfs добавляется 1 набор (согласуется с заказчиком перед поставкой устройства).

   b. по умолчанию, активным является набор с меньшим значением KeysetID (если в прошивку добавлено несколько наборов)
3. Пользователи и пароли управляющего протокола:
   a. login: "keyholder", password: "keyholder";
   b. login: "configure", password: "configure";
   c. login: "monitor", password: "monitor".
4. Пароль для рабочего протокола (hex-строка): "22222222222222222222222222222222"

7. Возможные проблемы и методы решения

Проблема	Возможные причины и решение
Появление признаков нестабильной или некорректной работы Устройства	Произведите перезагрузку Устройства.
При попытке установки нового соединения с Устройством, на стороне клиента показывается ошибка вида 'connection reset by peer'.	Вероятно, достигнуто максимальное число одновременных клиентских подключений к Устройству, равное 100. Разорвите ненужные соединения и повторите попытку установки нового соединения.

8. Обновление программного обеспечения

Штатно, обновление ПО устройства возможно двумя способами:

1. Основной способ - через сетевой интерфейс.
2. Вспомогательный способ - через интерфейс USB, расположенный внутри корпуса устройства.

Способы и процедуры обновления ПО устройства описаны в документе "ПАК "Криптокипер. Руководство по установке ПО"