

Терминал CyberFT

Руководство по установке и настройке

(для версии 3.2.1 и выше)

Установка Терминала CyberFT

Установка и настройка ОС Linux (Debian)

Загрузить ОС debian 7.8 можно с FTP:

`http://download.cyberft.ru/OS/debian-7.8.0-amd64-netinst.iso`

Во время установки, при выборе зеркал репозиториях укажите : `ftp.ru.debian.org`

При установке компонентов, выбираем только ssh-сервер + системные утилиты.

Проверите список репозиториях обновления debian:

`/etc/apt/sources.list`

Должны быть указаны следующие репозитории:

```
deb http://ftp.ru.debian.org/debian wheezy main contrib non-free
deb-src http://ftp.ru.debian.org/debian wheezy main contrib non-free
deb http://ftp.ru.debian.org/debian wheezy-updates main contrib non-free
deb http://ftp.ru.debian.org/debian-security wheezy/updates main contrib non-free
deb http://http.debian.net/debian wheezy-backports main
```

Для проверки версии версию ядра linux выполните команду:

```
uname -r
```

Получим примерно следующее:

```
3.2.0-0.bpo.4-amd64
```

Версия ядра Linux должна быть минимум 3.10

Обновить ядро:

```
apt-get install sudo
```

```
sudo apt-get update
```

В случае ошибки:

```
Ошибка GPG: http://http.debian.net wheezy-backports Release: Следующие подписи неверные:
BADSIG 8B48AD6246925553 Debian Archive Automatic Signing Key (7.0/wheezy)
<ftpmaster@debian.org>
```

Выполнить:

```
aptitude reinstall debian-archive-keyring
```

```
sudo apt-get install -t wheezy-backports linux-image-amd64
```

После обновления ядра, необходимо перезагрузить сервер.

Настройка окружения

```
apt-get -y install uuid nginx mysql-server redis-server cups lpr fail2ban samba stunnel4 openjdk-7-jre
openjdk-7-jdk build-essential libxml2-dev
```

Установка PHP

```
apt-get -y install software-properties-common python-software-properties
```

```
add-apt-repository 'deb http://packages.dotdeb.org wheezy-php56 all'
```

```
wget http://www.dotdeb.org/dotdeb.gpg
```

```
apt-key add dotdeb.gpg
```

```
apt-get update
```

```
apt-get -y install php5-fpm php5-common php5-cli php5-mcrypt php5-mysqlnd php5-curl php5-apcu
```

Установка Elasticsearch

```
wget https://download.elasticsearch.org/elasticsearch/release/org/elasticsearch/distribution/deb/elasticsearch/2.1.0/elasticsearch-2.1.0.deb
```

```
dpkg -i elasticsearch-2.1.0.deb
```

```
/etc/init.d/elasticsearch restart
```

Установка КриптоПРО CSP

```
apt-get -y install alien locales libc6-i386 lib32z1 libnss3-1d libnspr4-0d lsb-security lsb-core
```

Скачайте пакет КриптоПро CSP 3.9

```
tar -xf /linux-amd64.tgz
```

```
cd linux-amd64
```

```
alien -kci cprocsp-compat-altlinux-64-1.0.0-1.noarch.rpm
```

```
alien -kci lsb-cprocsp-base-3.9.0-4.noarch.rpm
```

```
alien -kci lsb-cprocsp-rdr-64-3.9.0-4.x86_64.rpm
```

```
alien -kci lsb-cprocsp-capilite-64-3.9.0-4.x86_64.rpm
```

```
alien -kci lsb-cprocsp-kc1-64-3.9.0-4.x86_64.rpm
```

```
alien -kci cprocsp-stunnel-64-3.9.0-4.x86_64.rpm
```

```
export PATH="$PATH:${ls -d /opt/cprocsp/{s,}bin/* | tr '\n' ':'}"
```

```
apt-get -y install pcscd pcsc-tools openct libusb-dev libccid
```

Создайте файл /etc/profile.d/cryptopro.sh с содержимым

```
export PATH="$PATH:${ls -d /opt/cprocsp/{s,}bin/* | tr '\n' ':'}"
```

Проверка корректной установки

```
cpconfig -license -view
```

Должно быть выведена информация о лицензии

Server license:

39390-Z0037-EA3YG-GRQED-E6LPZ

Expires: 3 month(s) 0 day(s)

Client license:

39390-Z0037-EA3YG-GRQED-E6LPZ

Expires: 3 month(s) 0 day(s)

Для установки лицензии выполните:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set далее-серийный-номер
```

Установка драйверов для работы с Токен

```
mkdir ../alladin
```

```
cd ../alladin
```

```
wget http://www.aladdin-rd.ru/support/downloads/get?ID=21493 -O alladin.zip
```

```
unzip alladin.zip
```

```
cd RPM\ 64/RPM/
```

```
alien pkiclient-5.00.28-0.x86_64.rpm
```

```
dpkg -i pkiclient_5.00.28-1_amd64.deb
```

```
cd /root/linux-amd64
```

```
alien -kci cproscsp-rdr-pcsc-64-3.9.0-4.x86_64.rpm
```

```
alien -kci cproscsp-rdr-jakarta-3.6.1-3.6.346-1.x86_64.rpm
```

Вставьте Токен

```
service pcscd start
```

```
list_pcsc
```

Должно отобразится подобное:

```
available reader: Aladdin eToken PRO USB 72K Java [Main Interface] 00 00
```

Установка Openssl xmlsec

```
mkdir /root/openssl/
```

```
cd /root/openssl/
```

```
wget http://openssl.org/source/openssl-1.0.2f.tar.gz
```

```
wget https://openssl.org/source/old/1.0.2/openssl-1.0.2f.tar.gz
```

```
wget --no-check-certificate http://www.aleksey.com/xmlsec/download/xmlsec1-1.2.20.tar.gz
```

```
tar xvzf openssl-1.0.2f.tar.gz
```

```
tar xvzf xmlsec1-1.2.20.tar.gz
```

```
cd openssl-1.0.2f
```

```
./config --prefix=/usr/local/openssl-1.0.2 shared
```

```
make
```

```
make install
```

Добавить строки в файл /usr/local/openssl-1.0.2/ssl/openssl.cnf:

В начало:

```
openssl_conf = openssl_def
```

В конец:

```
[openssl_def]
```

```
engines = engine_section
```

```
[engine_section]  
gost = gost_section
```

```
[gost_section]  
engine_id = gost  
dynamic_path = /usr/local/openssl-1.0.2/lib/engines/libgost.so  
default_algorithms = ALL  
CRYPT_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
```

```
cd ../xmlsec1-1.2.20  
./configure --prefix=/usr/local/xmlsec1-1.2.20 --enable-gost --disable-crypto-dl --with-  
openssl=/usr/local/openssl-1.0.2 --without-gcrypt --without-gnutls --without-libxslt  
make  
make install  
mv /usr/lib/ssl/openssl.cnf /usr/lib/ssl/openssl.cnf_bak  
mv /usr/bin/openssl /usr/bin/openssl_bak
```

Установка Терминала CyberFT

Загрузите архив с актуальной версией Терминала на FTP: <http://download.cyberft.ru/>

Сохраните архив в ОС Debian в каталог /home/

Создайте каталог, в который будет распакован архив. Например, /cyberft/.

В /etc/default/stunnel4 прописать ENABLED=1

Распакуйте архив с дистрибутивом, командой:

```
tar -zxvf /home/cyberft-v3.2.1.7.tar.tar.gz -C /home/cyberft/
```

Для запуска установки выполните:

```
/home/cyberft/distr/install.sh
```

Установка терминала осуществляется без использования docker

После установки прописать в /etc/rc.local

```
nano /etc/rc.local
```

добавить строчку */home/cyberft/app/service.sh start*

```
ln -s /usr/local/openssl-1.0.2/bin/openssl /usr/bin/openssl
```

```
ln -s /usr/local/openssl-1.0.2/ssl/openssl.cnf /usr/lib/ssl/openssl.cnf
```

```
ln -s /home/cyberft/app/src/bin/cyberft-crypt /usr/local/bin/cyberft-crypt
```

```
echo "/usr/local/xmlsec1-1.2.20/lib/" >> /etc/ld.so.conf.d/xmlsec.conf
```

```
ldconfig
```

```
export PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}"
```

в */etc/php5/fpm/php.ini* изменить *upload_max_filesize = 200M*

пропишите в */etc/environment*

```
export OPENSSL_CONF="/usr/local/openssl-1.0.2/ssl/openssl.cnf"
```

```
service stunnel4 restart
```

```
service nginx restart
```

```
service php5-fpm restart
```

```
/home/cyberft/app/service.sh restart (stop, start)
```

Генерация локальных ключей КриптоПРО

Все действия с КриптоПро осуществляются из под пользователя `www-data`

Создадим криптохранилище и файл запроса сертификата.

Создайте в каталоге `/home/` файлы для записи запроса на ключ в количестве необходимых ключей.

```
cd /home/
```

```
touch req1
```

```
chown www-data:www-data req1
```

```
touch req2
```

```
chown www-data:www-data req2
```

```
touch req3
```

```
chown www-data:www-data req3
```

.....

В запросе, в реквизитах ключа, укажите свои реквизиты

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" cryptcp -creatrst -dn "C=RU,L=Moscow,O=Cyberplat Ltd,OU=IT,E=ivanov@cyberplat.com,CN=Ivanov Ivan" -cont '\\.\hdimage\ivanov' req1
```

в данном примере *Ivanov* это название криптохранилища.

req1 – название файла с запросом на сертификат ключа

После генерации открываем полученный файл в редакторе

```
nano req1
```

Открываем в браузере страницу Тестового УЦ [КриптоПро](#), копируем туда содержимое файла *req1* и нажимаем выбрать.

Скачиваем полученный сертификат в формате DER и сохраняем в каталог `/home/` на сервере Linux и сохраним под именем *Ivanov.cer*

Полученные сертификаты устанавливаем в хранилище КриптоПро командой:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" cryptcp -instcert -cont '\\.\hdimage\ivanov' Ivanov.cer
```

Проверяем установленный сертификат командой

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" certmgr -list
```

Импорт ключевого контейнера и сертификата КриптоПРО с Токена

Создайте (запишите) ключи и сертификат на Токен.

Важно: Ключи на Токене должны быть экспортируемыми

Вставьте Токен в сервер Терминала

Выясним название ключевого контейнера на Токен:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" csptest -keyset -enum_cont -verifycontext -fqcn
```

Получим список всех доступных контейнеров ключей КриптоПРО:

```
root@TestEvraz:~# sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" csptest -keyset -enum_cont -verifycontext -fqcn
CSP (Type:75) v3.9.8001 KC1 Release Ver:3.9.8227 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 31534755
\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\ca0ef16d-c2f0-41ca-9d01-50658436bbaa
\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\1891a450-f9e1-44dd-882f-3fedd173d20d
\\.\HDIMAGE\IvanovII
\\.\HDIMAGE\BondarAA
OK.
Total:
[ErrorCode: 0x00000000]
root@TestEvraz:~#
```

Название нужного контейнера:

```
\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\ca0ef16d-c2f0-41ca-9d01-50658436bbaa
```

Для экспорта ключевого контейнера с Токена в локальное хранилище сервера Терминала выполните:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" csptest -keycopy -src '\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\ca0ef16d-c2f0-41ca-9d01-50658436bbaa' -dest '\\.\HDIMAGE\IvanPetrov'
```

Введите Pin-code **от Токена** и далее укажите пароль для ключевого контейнера.

Проверим, что ключевой контейнер экспортировался в хранилище сервера:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" csptest -keyset -enum_cont -verifycontext -fqcn
```

```
root@TestEvraz:~# sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" csptest -keyset -enum_cont -verifycontext -fqcn
CSP (Type:75) v3.9.8001 KC1 Release Ver:3.9.8227 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 26349219
\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\ca0ef16d-c2f0-41ca-9d01-50658436bbaa
\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\1891a450-f9e1-44dd-882f-3fedd173d20d
\\.\HDIMAGE\IvanovII
\\.\HDIMAGE\IvanPetrov
\\.\HDIMAGE\BondarAA
```

Скопируем сертификат с Токена в хранилище:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" certmgr -inst -cont '\\.\Aladdin eToken PRO USB 72K Java [Main Interface] 00 00\ca0ef16d-c2f0-41ca-9d01-50658436bbaa' -cont '\\.\HDIMAGE\IvanPetrov'
```

Проверим что сертификат успешно установлен и прилинкован к соответствующему контейнеру ключа:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/*|tr '\n' ':'}" certmgr -list
```

Импорт ключевого контейнера и сертификата КриптоПРО с Флешки

Создайте (запишите) ключи и сертификат на Флешку.

Важно: Ключи должны быть экспортируемыми

Вставьте Флешку в сервер Терминала

Скопируйте ключевой контейнер с флешки на сервер в директорию

```
/var/opt/cproscsp/keys/www-data/
```

Выставьте права на каталог контейнера 700 для пользователя www-data

Уточним название ключевого контейнера:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cproscsp/{s,}bin/*|tr '\n ':'}'" csptest -keyset -enum_cont -verifycontext -fqcn
```

Получим список всех доступных контейнеров ключей КриптоПРО:

```
root@TestEvraz:~# sudo -u www-data env PATH="$PATH:${ls -d /opt/cproscsp/{s,}bin/*|tr '\n ':'}'" csptest -keyset -fqcn
CSP (Type:75) v3.9.8001 KC1 Release Ver:3.9.8227 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 29859491
\\.\HDIMAGE\ChivanovAA
\\.\HDIMAGE\IvanovII
\\.\HDIMAGE\IvanPetrov
\\.\HDIMAGE\BondarAA
OK.
```

Скопируйте сертификат подписанта в директорию на сервер Терминала (напримр /home/certs/)

Установим сертификат ключа в хранилище:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cproscsp/{s,}bin/*|tr '\n ':'}'" certmgr -inst -file /home/certs/ChivanovAA.cer -cont '\\.\HDIMAGE\ChivanovAA'
```

Проверим что сертификат успешно установлен и прилинкован к соответствующему контейнеру ключа:

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cproscsp/{s,}bin/*|tr '\n ':'}'" certmgr -list
```

```
=====
1-----
Issuer       : C=RU, L=Moscow, O=Cyberplat, CN=Chivanov Aleksandr
Subject      : C=RU, L=Moscow, O=Cyberplat, CN=Chivanov Aleksandr
Serial       : 0x4BF8D75F11FD3CD1
SHA1 Hash    : 0xd6191bff7609b098d7ea6c400a1eb30bb43d8eb3
Not valid before : 19/05/2016 12:11:23 UTC
Not valid after  : 19/05/2017 12:11:23 UTC
PrivateKey Link : Yes. Container : HDIMAGE\\.\Chivanov.000\1992
```

Импорт сертификатов пользователя в хранилище сервера Терминала CyberFT

Для добавления сертификата проверки подписи для документов типа **ISO20022** выполнить

```
cd /home/cyberft/app/src
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" ./yii cryptopro/add-certificates-from-terminal iso20022
```

Для добавления сертификата проверки подписи для документов типа **FileACT** выполнить

```
cd /home/cyberft/app/src
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" ./yii cryptopro/add-certificates-from-terminal fileact
```

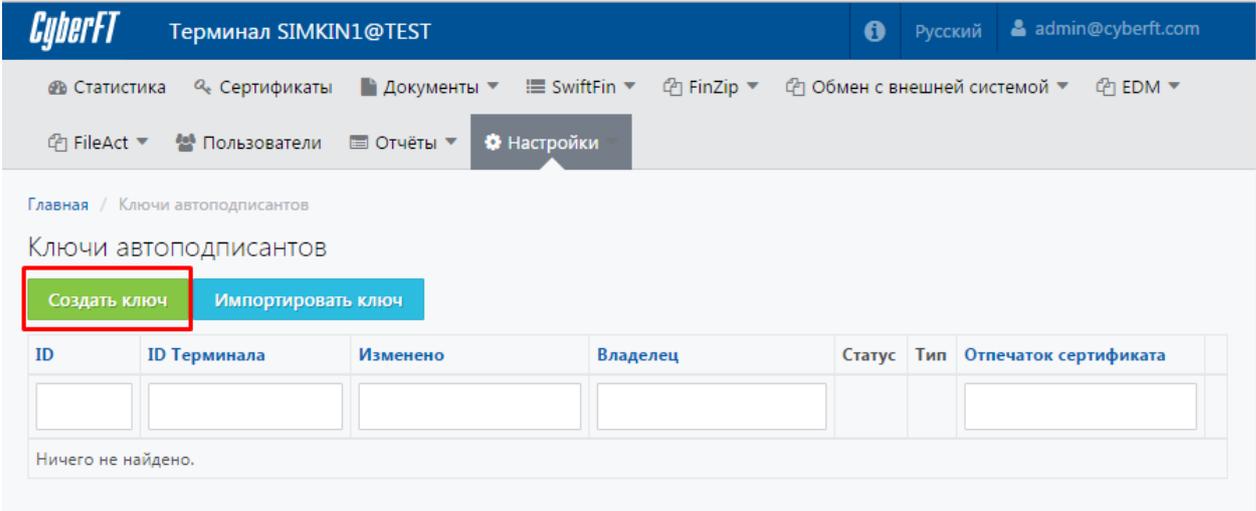
Добавьте сертификат из локального хранилища в терминал.

```
cd /home/cyberft/app/src
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" ./yii cryptopro/install-certificate-from-container (название контейнера Ivanov, user1, user2, user3 и т.д.)
```

Настройка Терминала CyberFT через веб интерфейс

Генерация ключей автоматического подписанта.

Входим в Настройки -> Ключи автоподписантов

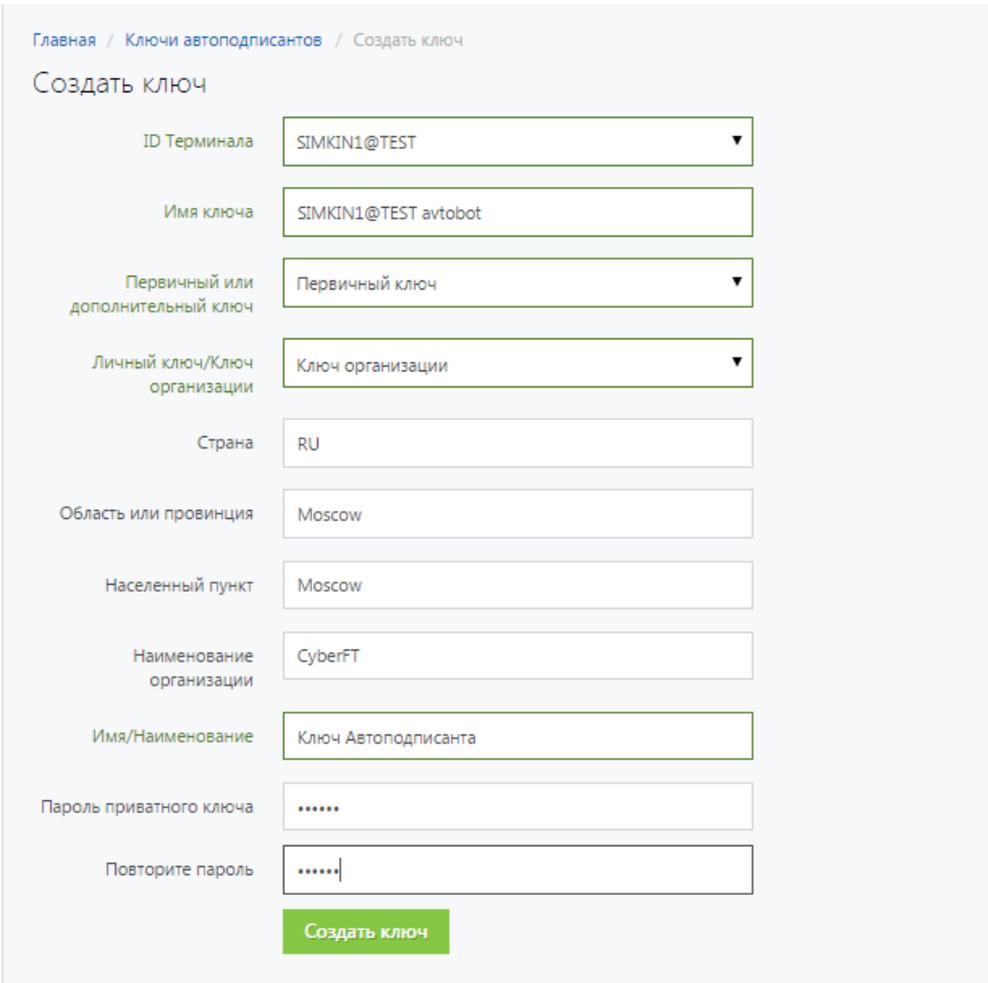


The screenshot shows the CyberFT web interface. The top navigation bar includes the CyberFT logo, the terminal ID 'SIMKIN1@TEST', and user information 'admin@cyberft.com'. Below the navigation bar, there are several menu items: 'Статистика', 'Сертификаты', 'Документы', 'SwiftFin', 'FinZip', 'Обмен с внешней системой', and 'EDM'. A secondary menu includes 'FileAct', 'Пользователи', 'Отчёты', and 'Настройки'. The main content area is titled 'Ключи автоподписантов' and contains two buttons: 'Создать ключ' (highlighted with a red box) and 'Импортировать ключ'. Below the buttons is a table with columns: ID, ID Терминала, Изменено, Владелец, Статус, Тип, and Отпечаток сертификата. The table is currently empty, and a message below it says 'Ничего не найдено.'

Заполняем реквизиты ключа.

Владелец ключа вводит пароль приватного ключа.

Нажимаем «Создать ключ».



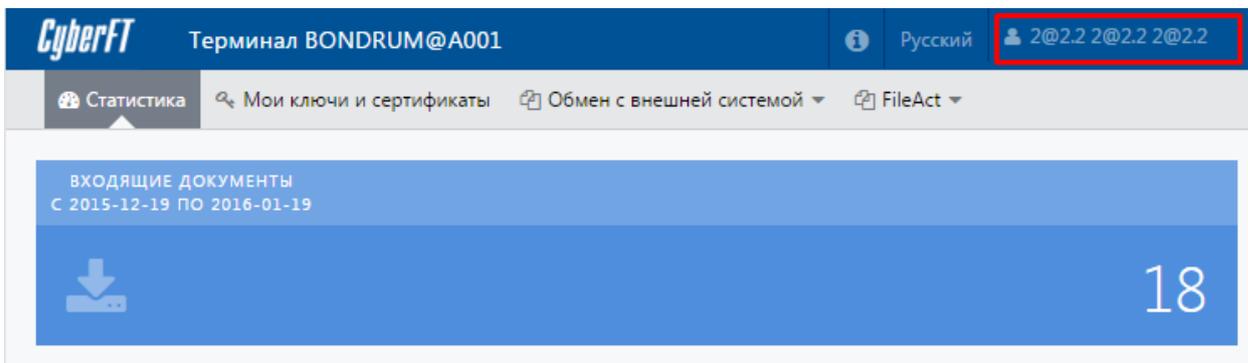
The screenshot shows the 'Создать ключ' form. The breadcrumb trail is 'Главная / Ключи автоподписантов / Создать ключ'. The form fields are: 'ID Терминала' (dropdown menu with 'SIMKIN1@TEST'), 'Имя ключа' (text input with 'SIMKIN1@TEST avtobot'), 'Первичный или дополнительный ключ' (dropdown menu with 'Первичный ключ'), 'Личный ключ/Ключ организации' (dropdown menu with 'Ключ организации'), 'Страна' (text input with 'RU'), 'Область или провинция' (text input with 'Moscow'), 'Населенный пункт' (text input with 'Moscow'), 'Наименование организации' (text input with 'CyberFT'), 'Имя/Наименование' (text input with 'Ключ Автоподписанта'), 'Пароль приватного ключа' (password input with '*****'), and 'Повторите пароль' (password input with '*****'). A green 'Создать ключ' button is located at the bottom of the form.

Сгенерится комплект ключей.

По нажатию кнопки «Скачать файл» можно выгрузить сертификат открытого ключа.

Активация ключей подписантом.

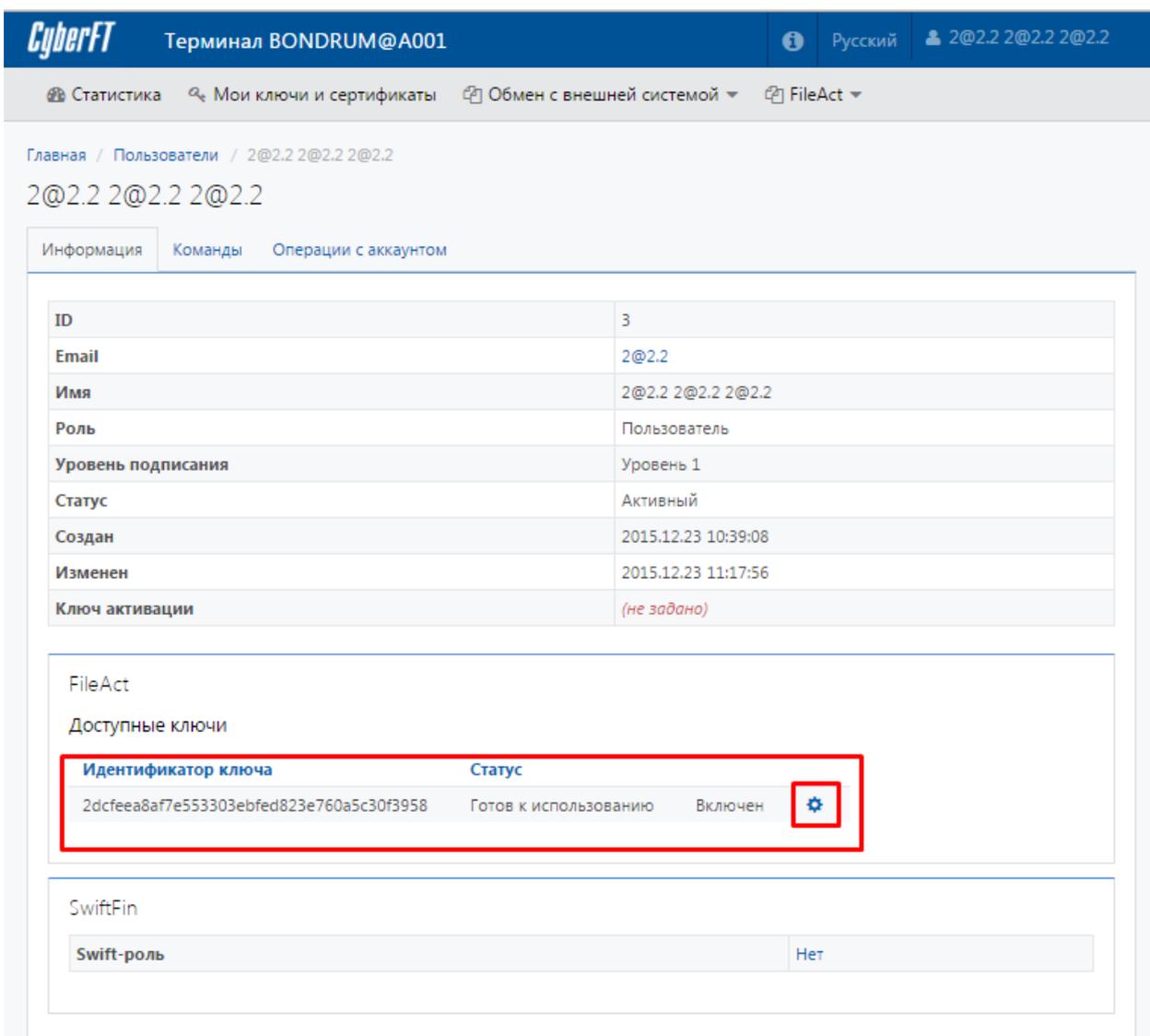
- 1) Входим в Терминал под пользователем владельцем ключа
- 2) Входим в свойства учетной записи пользователя (отмечено красным)



The screenshot shows the CyberFT terminal interface. At the top, the user is logged in as 'Терминал BONDRUM@A001' in Russian. The user's email '2@2.2 2@2.2 2@2.2' is highlighted with a red box. Below the navigation bar, there is a section for 'ВХОДЯЩИЕ ДОКУМЕНТЫ' (Incoming Documents) for the period 'С 2015-12-19 ПО 2016-01-19'. A large blue box displays the number '18' with a download icon.

В Блоке **FileAct** отображаются привязанные к пользователю ключи.

- 3) Для активации ключа входим в «Настройки» соответствующего ключа.



The screenshot shows the 'Пользователи' (Users) section for the user '2@2.2 2@2.2 2@2.2'. The 'Информация' (Information) tab is selected. A table displays user details:

ID	3
Email	2@2.2
Имя	2@2.2 2@2.2 2@2.2
Роль	Пользователь
Уровень подписания	Уровень 1
Статус	Активный
Создан	2015.12.23 10:39:08
Изменен	2015.12.23 11:17:56
Ключ активации	(не задано)

Below the table, the 'FileAct' section shows 'Доступные ключи' (Available keys). A table lists a key with its identifier and status:

Идентификатор ключа	Статус
2dcf6ea8af7e553303ebfed823e760a5c30f3958	Готов к использованию

The 'Включен' (Enabled) button and the gear icon for settings are highlighted with a red box.

The 'SwiftFin' section shows the 'Swift-роль' (Swift role) as 'Нет' (None).

- 4) Владелец ключа собственноручно вводит пароль от ключа, ставит галочку в чекбокс Activate, нажимает «Изменить»

CyberFT Терминал TESTPDV@X001

Статистика | Мои ключи и сертификаты | Документы | SwiftFin | Обмен с внешней системой | **FileAct** | FinZip

Главная / FileAct / Ключи КриптоПро / Ключ №4

Ключ №4

Сертификат

Организация: ООО КиберПлат
Подразделение: SUPPORT
CN: Test Cyber User1
Email: support@cyberplat.com

Статус: Готов к использованию

Пароль от eToken

.....

Разрешить автоподписание

Изменить

Ключ активирован и добавлен в процесс автоматического подписания исходящих сообщений FileAct.

Настройка верификации входящих сообщений

Для настройки верификации входящих сообщений заходим в FileAct -> Настройки
Настройки КриптоПро

В блоке Верификация входящих необходимо добавить сертификаты ключей участников, которыми должны быть в обязательном порядке подписаны все входящие сообщения от соответствующего участника.

Скриншот веб-интерфейса CyberFT. Вкладка: Терминал TESTPDV@X001. Меню: Статистика, Сертификаты, Документы, SwiftFin, EDM, Обмен с внешней системой, FileAct, FinZip. Адрес: Главная / FileAct / Настройки КриптоПро. Заголовок: Настройки КриптоПро.

Подпись

Активировать подписание КриптоПро

Сохранить

Доступные ключи

Идентификатор ключа	Статус
91886be1d6809bf579d919a7bde0daf07863d181	Готов к использованию Включен Скачать ⚙️

Верификация входящих

Доступные сертификаты

ID терминала	Идентификатор ключа	Статус
TESTPDV@X001	91886be1d6809bf579d919a7bde0daf07863d181	Готов к использованию Скачать ⚙️
SIMKIN1@TEST	498bd5bccf07e1831d0f4fd5535db22048ae1133	Готов к использованию Скачать ⚙️

Добавить сертификат

Для добавления сертификата проверки подписи для документов типа **ISO20022** выполнить
`cd /home/cyberft/app/src`
`sudo -u www-data env PATH="$PATH:$(ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':')". /yii cryptopro/add-certificates-from-terminal iso20022`

Для добавления сертификата проверки подписи для документов типа **FileACT** выполнить
`cd /home/cyberft/app/src`
`sudo -u www-data env PATH="$PATH:$(ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':')". /yii cryptopro/add-certificates-from-terminal fileact`

Статус сертификата должен измениться на «Готов к использованию»

Настройка почтового сервера для рассылки уведомлений

Заходим в Настройки -> Настройки почтовых оповещений
Указываем реквизиты почтового сервера и нажимаем «Сохранить»

The screenshot shows the CyberFT interface for the terminal 'SIMKIN1@TEST'. The 'Настройки' (Settings) menu item is highlighted with a red box. The page title is 'Настройки почтовых оповещений' (SMTP server settings). The form contains the following fields:

- SMTP хост: smtp.mail.ru
- SMTP порт: 25
- Логин: bond008@inbox.ru
- Пароль:
- Шифрование: Нет

Buttons: Сохранить (Save), Тестовый адрес (Test address), Проверить (Check).

Настройка рассылки уведомлений

Заходим в Настройки -> Список рассылки оповещений
Добавляем пользователей в список рассылки.
Сообщения будут рассылаться на указанный email пользователя.

The screenshot shows the CyberFT interface for the terminal 'PHPTTEST@A001'. The page title is 'Список рассылки оповещений' (List of notification distribution). A notification message is displayed: 'Настройки пользовательского оповещения сохранены' (User notification settings saved).

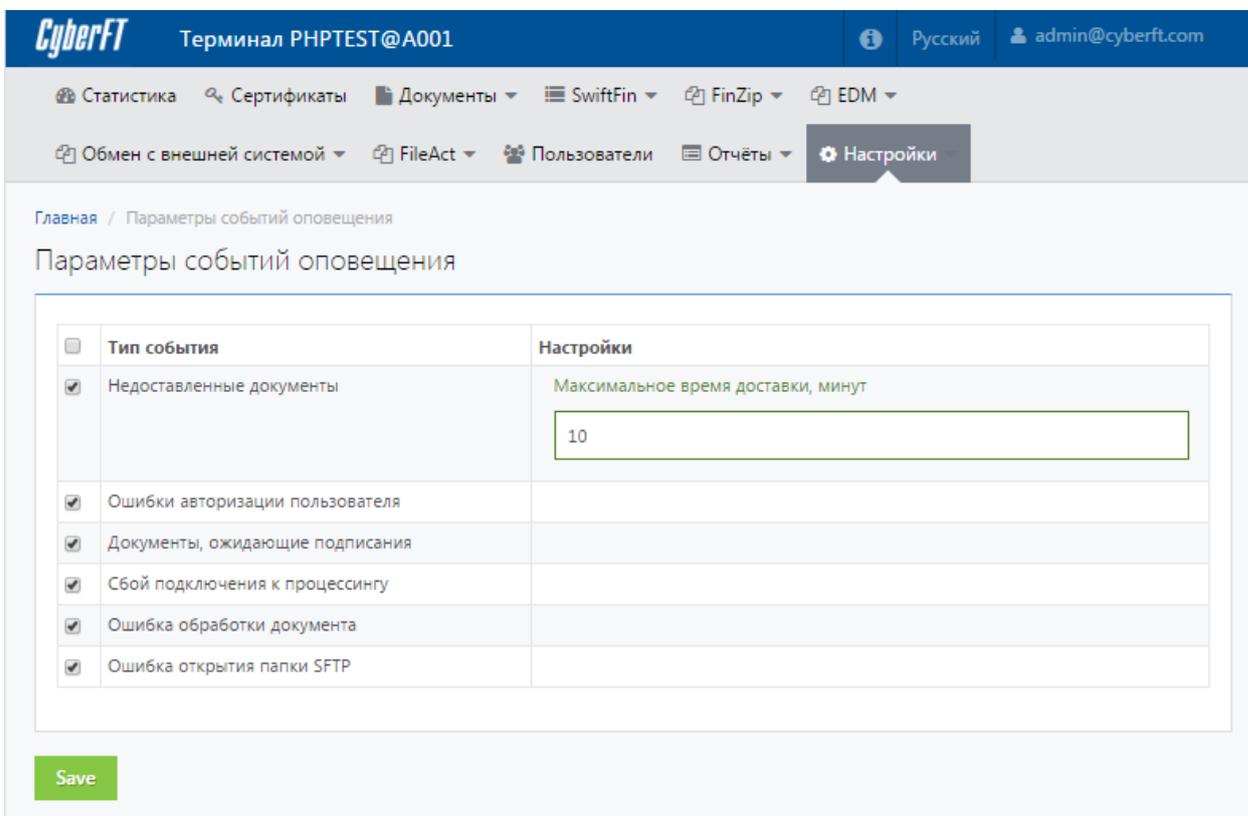
The table shows the list of users receiving notifications:

Id	Name	Email	
10	a.bondar	a.bondar@cyberplat.ru	🗑️
1	admin@cyberft.com	admin@cyberft.com	🗑️

Below the table, there is a section 'Добавить нового пользователя' (Add new user) with a dropdown menu showing 'Iso@cyberft.com' and a 'Добавить' (Add) button.

Настройка оповещений по событиям

Заходим в Настройки -> Параметры событий оповещения
Активируем рассылку уведомлений в соответствии с событиями, настраиваем соответствующие параметры и сохраняем.



The screenshot shows the CyberFT web interface. The header includes the logo, terminal name (Терминал РНРТЕСТ@A001), language (Русский), and user (admin@cyberft.com). The navigation menu contains: Статистика, Сертификаты, Документы, SwiftFin, FinZip, EDM, Обмен с внешней системой, FileAct, Пользователи, Отчёты, and Настройки. The breadcrumb trail is: Главная / Параметры событий оповещения. The main heading is: Параметры событий оповещения. Below it is a table with two columns: Тип события and Настройки.

<input type="checkbox"/>	Тип события	Настройки
<input checked="" type="checkbox"/>	Недоставленные документы	Максимальное время доставки, минут <input type="text" value="10"/>
<input checked="" type="checkbox"/>	Ошибки авторизации пользователя	
<input checked="" type="checkbox"/>	Документы, ожидающие подписания	
<input checked="" type="checkbox"/>	Сбой подключения к процессингу	
<input checked="" type="checkbox"/>	Ошибка обработки документа	
<input checked="" type="checkbox"/>	Ошибка открытия папки SFTP	

Save

Подключение сетевых дисков

При подключении сетевого диска указываем:

Папка для импорта: \\192.168.72.128\cyberft_import

Папка для экспорта: \\192.168.72.128\cyberft_export

Пользователь: cyberft-samba

Пароль указывается при установке samba

Удаление ключей КриптоПРО

Удаление ключей КриптоПРО с сервера Терминала CyberFT

Выясним какие сертификаты имеются в хранилище

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" certmgr -list
```

Получим

```
=====
1-----
Issuer      : E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CRYPTO-PRO Test
Center 2
Subject     : C=RU, S=Moscow, L=Moscow, O=Cyberplat Ltd, OU=IT, E=test@cyberplat.com, CN=test
Serial      : 0x12000DD1340FD2D6F58BC6CC9B000000DD134
SHA1 Hash   : 0xd1758c577fb9c9b83ca7b1e5257f2d5e0af44900
Not valid before : 16/02/2016 10:12:44 UTC
Not valid after  : 16/05/2016 10:22:44 UTC
PrivateKey Link : Yes. Container : HDIMAGE\\Chivanov.000\1992
```

Удалим сертификат

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" certmgr -delete
1
```

Где 1 это ID сертификата в хранилище

Выясним какие имеются контейнеры ключей

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" csptest -keyset -
enum_cont -verifycontext -fqcn
```

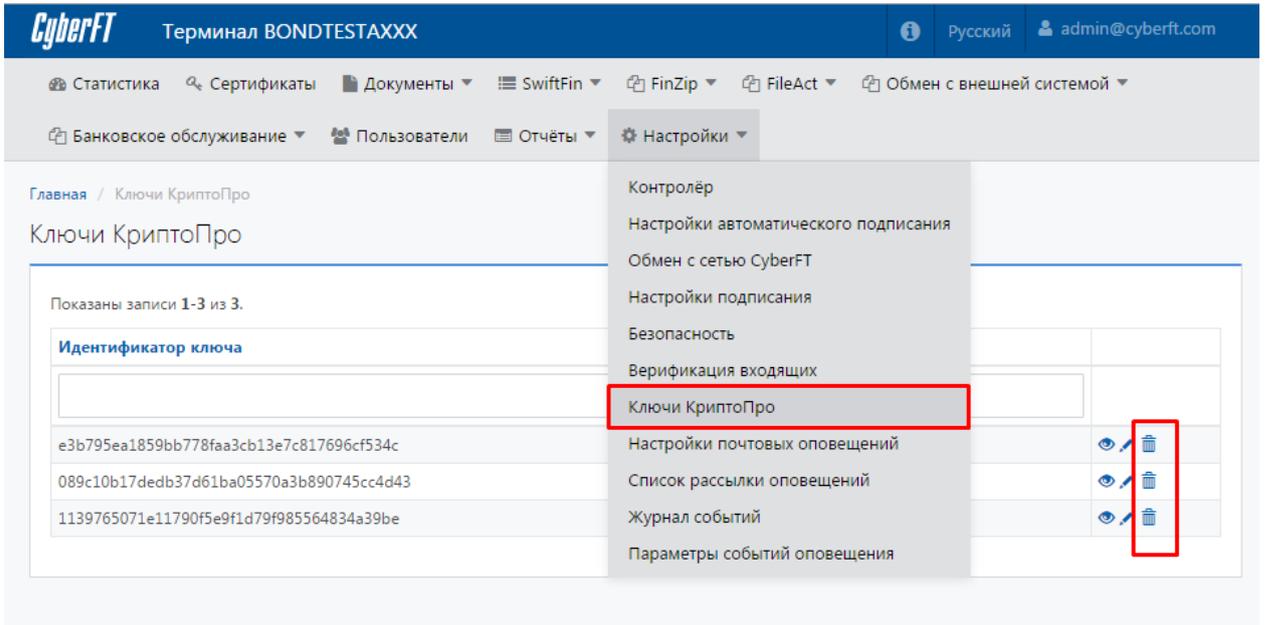
```
root@TestEvraz:~# sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" csptest -keys
et -enum_cont -verifycontext -fqcn
CSP (Type:75) v3.9.8001 KC1 Release Ver:3.9.8227 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 23158435
\\.HDIMAGE\ChivanovAA
\\.HDIMAGE\IvanovII
\\.HDIMAGE\BondarAA
OK.
```

Удалим хранилище ChivanovAA

```
sudo -u www-data env PATH="$PATH:${ls -d /opt/cprosp/{s,}bin/* | tr '\n' ':'}" certmgr -delete -cont
'\\.hdimage\ChivanovAA'
```

Удаление сертификатов КриптоПРО из базы данных Терминала CyberFT

Для удаления записей о сертификатах в веб интерфейсе Терминала CyberFT зайдите в Настройки → Ключи КриптоПро и удалите нужные сертификаты

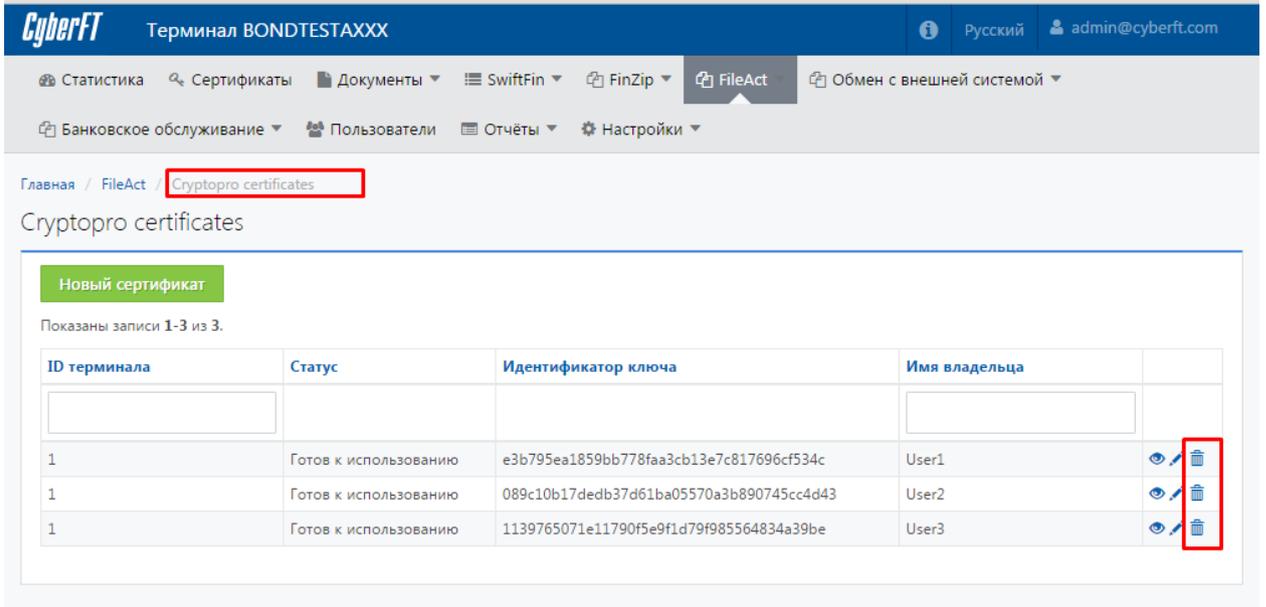


Скриншот веб-интерфейса терминала CyberFT. В меню «Настройки» пункт «Ключи КриптоПро» выделен красной рамкой. В таблице ниже выделены красными рамками значки удаления для трех записей.

Идентификатор ключа			
е3b795ea1859bb778faa3cb13e7c817696cf534c			
089c10b17dedb37d61ba05570a3b890745cc4d43			
1139765071e11790f5e9f1d79f985564834a39be			

Для удаления сертификатов верификации входящих сообщений зайдите в меню Cryptopro certificates по ссылке: <https://XXX.XXX.XX.XXX/ru/ISO20022/cryptopro-cert/index>

Далее можно удалить не нужные сертификаты.



Скриншот веб-интерфейса терминала CyberFT. В меню «FileAct» пункт «Cryptopro certificates» выделен красной рамкой. В таблице ниже выделены красными рамками значки удаления для трех записей.

ID терминала	Статус	Идентификатор ключа	Имя владельца	
1	Готов к использованию	е3b795ea1859bb778faa3cb13e7c817696cf534c	User1	
1	Готов к использованию	089c10b17dedb37d61ba05570a3b890745cc4d43	User2	
1	Готов к использованию	1139765071e11790f5e9f1d79f985564834a39be	User3	