

ЗАО “КИБЕРПЛАТ”



123610, г. Москва, ЦМТ-2, Краснопресненская наб.,
д.12 подъезд № 7
Телефон: (495) 967-02-20 Факс: (495) 967-02-08

CYBERPLAT

123610, Moscow, WTC-2, Krasnopresnenskaya
nab., 12, entrance # 7
Phone: (495) 967-02-20 Fax: (495) 967-02-08

Терминал сети CyberFT

Руководство администратора

1. Аннотация

В настоящем документе дано описание установки и настройки Терминала сети CyberFT.

2. Версии документа

Версия ПО	Дата	Изменения в Документе
2.2.1	05.01.2015	Начало отсчета версий документа.
2.2.1.7	10.02.2015	Добавлен раздел о безопасности, выделен подраздел «Настройка ключей перед началом работы», Описаны Настройки экспорта и меню «Участники», актуализированы снимки экрана.
2.3.1	26.03.2015	Добавлены и обновлены разделы в соответствии с новым функционалом
2.4.0	22.04.2015	Добавлены и обновлены разделы в соответствии с новым функционалом
2.5.2	05.06.2015	Обновлено в соответствии с новым функционалом: ДБО, FileAct

3. Содержание

1.	АННОТАЦИЯ	2
2.	ВЕРСИИ ДОКУМЕНТА	2
3.	СОДЕРЖАНИЕ	3
4.	ТЕРМИНЫ И СОКРАЩЕНИЯ.....	5
5.	ВВЕДЕНИЕ	9
5.1.	ОБЛАСТЬ ПРИМЕНЕНИЯ	9
5.2.	ОПИСАНИЕ ВОЗМОЖНОСТЕЙ	9
5.3.	УРОВЕНЬ ПОДГОТОВКИ ПОЛЬЗОВАТЕЛЕЙ	9
6.	НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ	10
6.1.	НАЗНАЧЕНИЕ ТЕРМИНАЛА.....	10
6.2.	ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ ТЕРМИНАЛА	10
6.2.1.	<i>Требования к программному обеспечению.....</i>	10
6.2.2.	<i>Требования к аппаратному обеспечению</i>	10
6.2.3.	<i>Требования к доступу в Интернет.....</i>	11
6.3.	СТРУКТУРА ДЕРЕВА КАТАЛОГОВ ТЕРМИНАЛА.....	11
7.	УСТАНОВКА И НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ.....	12
7.1.	УСТАНОВКА DEBIAN/LINUX	12
8.	УСТАНОВКА И НАСТРОЙКА ТЕРМИНАЛА.....	13
8.1.	СОСТАВ И СОДЕРЖАНИЕ ДИСТРИБУТИВА.....	13
8.2.	ИНСТАЛЛЯЦИЯ ТЕРМИНАЛА	13
8.3.	ОБНОВЛЕНИЕ ТЕРМИНАЛА	20
8.4.	РЕКОНФИГУРАЦИЯ ТЕРМИНАЛА	20
8.5.	ДЕИНСТАЛЛЯЦИЯ ТЕРМИНАЛА.....	21
8.6.	ОСОБЕННОСТИ КОНФИГУРАЦИИ ОКРУЖЕНИЯ	21
8.7.	ПОДКЛЮЧЕНИЕ КАТАЛОГОВ CYBERFT КАК СЕТЕВЫХ ДИСКОВ WINDOWS	22
8.8.	ВОЗМОЖНЫЕ ПРОБЛЕМЫ НА ТЕРМИНАЛЕ	23
9.	ВЕБ-ИНТЕРФЕЙС ГЛАВНОГО АДМИНИСТРАТОРА.....	23
9.1.	ДОСТУП К ВЕБ-ИНТЕРФЕЙСУ ТЕРМИНАЛА	23
9.2.	НАСТРОЙКА КЛЮЧЕЙ ПЕРЕД НАЧАЛОМ РАБОТЫ.....	24
9.2.1.	<i>Генерация ключа Автоподписанта</i>	24
9.2.2.	<i>Отправка сертификата открытого ключа</i>	27
9.2.3.	<i>Установка открытого ключа Процессинга CyberFT.....</i>	27
9.2.4.	<i>Обмен сертификатами со связанными Участниками</i>	27
9.2.5.	<i>Запуск обмена Терминала с сетью CyberFT.....</i>	29
9.3.	НАСТРОЙКИ И ФУНКЦИИ ВЕБ-ИНТЕРФЕЙСА АДМИНИСТРАТОРА	31
9.3.1.	<i>Замена ключа Автоподписанта.....</i>	31
9.3.2.	<i>Редактирование адреса Терминала.....</i>	32
9.3.3.	<i>Маршрутизация исходящих документов</i>	32
9.3.4.	<i>Активация экспорта документов и отчетов по статусу обработки документов.....</i>	34
9.3.5.	<i>Экспорт входящих документов на печать.....</i>	36
9.3.6.	<i>Управление пользователями</i>	37
9.3.7.	<i>Настройки подписания документов.....</i>	40
9.3.8.	<i>Журнал документов.....</i>	42

9.3.9.	<i>Главное меню Терминала</i>	44
10.	МОДУЛЬ ДБО	46
10.1.	НАСТРОЙКА ДБО РОЛЕЙ.....	46
10.2.	Доступ к ДБО-модулю для Главного Администратора	47
10.3.	ДБО-Справочники	47
10.3.1.	<i>Справочник Банки</i>	48
10.3.2.	<i>Справочник Контрагенты</i>	48
10.3.3.	<i>Справочник Назначения платежа</i>	50
11.	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	51
11.1.	ФАЙЛОВЫЙ ОБМЕН FILEACT	51
11.1.1.	<i>Порядок файлового обмена FileAct</i>	51
11.1.2.	<i>Правила формирования документов Терминалом</i>	51
11.2.	СТАТУСЫ ДОКУМЕНТОВ В CYBERFT	53
11.3.	ОПИСАНИЕ ОШИБОК.....	53
12.	РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ	54
12.1.	ВВЕДЕНИЕ.....	54
12.2.	ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ	55
12.3.	РЕКОМЕНДАЦИИ ПО РАЗМЕЩЕНИЮ И ЗАЩИТЕ ТЕРМИНАЛА CYBERFT	56
12.4.	ОБЩИЕ ТРЕБОВАНИЯ К ПЕРСОНАЛЬНОМУ КОМПЬЮТЕРУ, ИСПОЛЪЗУЕМОМУ ДЛЯ РАБОТЫ СО СРЕДСТВАМИ ЭЛЕКТРОННОЙ ПОДПИСИ	59
12.5.	ДЕЙСТВИЯ ПРИ НЕШТАТНЫХ СИТУАЦИЯХ	59

4. Термины и сокращения

Администрация – Юридическое лицо, привилегированный Участник «CyberFT», управляющий Единым справочником Сети. Администрация имеет в Сети CyberFT свой адрес.

Электронная подпись (ЭП) - Электронная подпись. В системе используются ключи, выпускаемые Системой, либо ключи усиленной (квалифицированной) цифровой подписи Участника.

Владелец ключей – физическое лицо, являющееся уполномоченным представителем Участника или Провайдера на отправку электронных документов от имени Участника через Сеть «CyberFT», создавшее Криптографические ключи, на имя которого Администрация зарегистрировала в Сети «CyberFT» соответствующий сертификат Открытого ключа, что позволяет Владельцу ключей создавать ЭП в электронных документах (подписывать Электронные документы ЭП) и использовать Электронный документооборот в Сети «CyberFT».

Закрытый (секретный) ключ – уникальная последовательность символов, предназначенная для создания ЭП и расшифровки информации с использованием Средств криптографической защиты информации и известная только Владельцу ключей.

Компрометация ключа – констатация лицом, владеющим Закрытым (секретным) ключом ЭП, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами.

Криптографические ключи – общее название Открытых и Закрытых (секретных) ключей.

Открытый ключ – уникальная последовательность символов, соответствующая Закрытому (секретному) ключу, общедоступная и предназначенная для подтверждения подлинности ЭП и зашифровки информации с использованием Средств криптографической защиты информации.

Участник – юридическое лицо (в том числе кредитная организация) или индивидуальный предприниматель, зарегистрированное(ый) в Сети «CyberFT» и участвующее в электронном документообороте.

Подключение Участника к Сети CyberFT – Технические, организационные и юридические действия по предоставлению Участнику возможности обмениваться Электронными документами с другими Участниками Сети CyberFT, выполняемые Провайдером. Перед Подключением Участник должен пройти Регистрацию в Сети CyberFT.

Процессинг «CyberFT» – программно-аппаратное решение, реализующее юридически значимый электронный документооборот в Сети CyberFT. Процессинг образует отдельный сегмент Сети CyberFT со своими Участниками. Каждый Процессинг в Сети CyberFT имеет свой адрес по адресу Провайдера, например CYBERUM@XXX.

Правила – Правила электронного документооборота Сети «CyberFT», установленные в Договоре об информационном и технологическом обслуживании.

Провайдер CyberFT – Юридическое лицо, привилегированный Участник «CyberFT», управляющий Процессингом. Каждый Провайдер, как Участник, имеет в Сети CyberFT свой адрес, например CYBERUM@XXX.

Регистрация Участника в Сети CyberFT – Назначение Участнику Уникального идентификатора в Сети CyberFT, осуществляемое Администрацией.

Сеть «CyberFT» – система электронного документооборота, представляющая собой совокупность программных и аппаратных средств, предназначенная для обмена юридически значимыми ЭД и обеспечивающая информационное и технологическое взаимодействие между Участниками.

Сегмент сети CyberFT – провайдер со своим Процессингом и пулом Участником образует сегмент Сети CyberFT.

Единый справочник Сети CyberFT – Справочник Участников, Провайдеров и пр. под управлением Администрации Сети CyberFT.

Средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, обеспечивающих применение ЭП и шифрования при организации Электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Терминал CyberFT – Программно-техническое средство, устанавливаемое у Участника и служащее для подключения Участника к Сети CyberFT.

Уникальный идентификатор Участника - уникальная последовательность символов, однозначно определяющая Участника Сети CyberFT. Уникальный идентификатор используется как адрес Участника при обмене Электронными документами в Сети CyberFT.

Установить связь с Участником сети - установление взаимного доверия между Участниками (RMA - Relationship Management Application). Без Установления связи разрешено отправлять только определенные типы документов другому Участнику.

Режим взаимного доверия – когда Участники обменялись сертификатами открытых ключей друг друга и признают ЭП друг друга.

Главный администратор (ГА) - сотрудник Участника уполномоченный производить настройки Терминала, влияющие на безопасность, а также предоставлять полномочия Подписантам подписывать документы от имени Участника.

Тип Электронного документа (Тип ЭД) - Допустимые в CyberFT форматы электронных документов, например MT***, ISO20022.

Электронный документ (ЭД) – Электронный документ.

Электронный документооборот (ЭДО) – Электронный документооборот.

Система ЭДО – Подсистема CyberFT, отвечающая за оборот определенного Типа ЭД.

Группа ЭД – Объединение Типов ЭД, например группа MT1**, группа MT2**.

Контрольное время ЭД - Время, указанное в ЭД до которого он должен быть доставлен до Получателя. Если ЭД не доставлен до указанного времени, он считается недоставленным и все дальнейшие попытки его доставки прекращаются.

Уведомление о доставке – Служебный Тип ЭД в формате XML CyberFT, используемый для отправки уведомления по факту доставки отправителю.

BICFT - Business Identification Code CyberFT. Код или адрес Участника в сети CyberFT. Если Участник уже имеет код BIC (адрес в SWIFT), то используется его BIC, если не имеет, то Участнику присваивается BICFT.

XML CyberFT - Формат электронного документа или XML конверта, который принят и поддерживается в Сети CyberFT. XML CyberFT может быть как самостоятельным документом, так и содержать ЭД других Типов. В большинстве случаев понятия XML CyberFT или XML конверт взаимозаменяемы.

XML конверт - Формат XML конверта, принятый и поддерживаемый в Сети CyberFT. Конверт может содержать как один, так и несколько ЭД одного Типа. В большинстве случаев понятия XML CyberFT или XML конверт взаимозаменяемы.

Сертификат - self-signed сертификат банка Участника, выпущенный на основании закрытого ключа; либо сертификат, выданный Удостоверяющим центром.

ОС - операционная система, установленная на ЭВМ.

БД - база данных.

Подписант - Сотрудник Участника, имеющий полномочия подписывать документы от имени Участника. Участник может установить режим «две подписи» для определенных типов ЭД. В этом случае роль Подписанта делится на две подроли:

- ▶ «1-я подпись» - Подписант, обладающий правом 1-й подписи;
- ▶ «2-я подпись» - Подписант, обладающий правом 2-й подписи.

Пользователь - Сотрудник Участника, имеющий доступ к Терминалу CyberFT.

Автоподписант – Автоматический Подписант.

УЦ - Удостоверяющий центр.

ДБО -Дистанционное Банковское Обслуживание.

5. Введение

5.1. Область применения

Система CyberFT предназначена для обеспечения юридически значимого обмена финансовыми сообщениями и электронными документами между Участниками системы. Участниками системы могут быть любые организации, которые участвуют в электронном обмене документами. Для получения статуса Участника необходимо зарегистрироваться в системе CyberFT.

Каждый Участник Сети имеет свой идентификатор (адрес в сети). В качестве адреса для Участника используется его BIC (адрес в системе SWIFT) или, если Участник не имеет BIC, ему присваивается BICFT.

5.2. Описание возможностей

Система обеспечивает юридически значимый обмен электронными документами между Участниками.

Основные функции Терминала:

- ▶ Регистрация документов в системе;
- ▶ Подписание документов ЭП Участника;
- ▶ Доставка исходящих документов до Процессинга;
- ▶ Загрузки входящих документов из Процессинга;
- ▶ Проверка ЭП входящих документов.

Основные функции Процессинга:

- ▶ Проверка документов на соответствие форматам MT, ISO, ЦБР;
- ▶ Проверка ЭП документов;
- ▶ Маршрутизация документов;
- ▶ Отслеживание статусов документов.

5.3. Уровень подготовки пользователей

Для администрирования Терминала необходимы базовые знания в области администрирования Linux-систем и БД MySQL.

Пользователи Терминала должны обладать базовыми навыками работы с ПК.

6. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

6.1. Назначение Терминала

Терминал представляет собой серверное программное обеспечение, устанавливаемое на стороне Участника CyberFT и предназначенное для подписания, отправки и получения электронных документов при обмене с другим Участником. Терминал поставляется как deb-пакет и управляется через веб-интерфейс.

Файловая система Терминала представляет собой дерево каталогов (подробнее см. п. 6.3 Структура дерева каталогов Терминала), где, в частности, содержатся папки для исходящих и входящих документов: **In** и **Out**.

Терминал периодически сканирует папку **Import** на наличие новых файлов. В случае их появления передает на подписание секретным ключом Участника.

После подписания документы по транспортному протоколу передаются в Процессинг системы CyberFT. Взаимодействие Терминала с Процессингом осуществляется через интернет с использованием криптографического протокола TLSv1.

В случае наличия соответствующей настройки, Терминал дополнительно передает входящие документы в папку **Export** (для АБС), и/или на принтер (для ручной обработки).

Помимо документов, передаются также квитанции о текущем статусе отправленных документов (**statusreport**). Они тоже подписываются передающей стороной.

Информация о статусе доставки документов доступна в Журнале Терминала. Кроме того, квитанции могут быть настроены на экспорт в папку **cyberxml** (для АБС).

Основная обработка документа – прием, контроль и доставка электронных документов – происходит в Процессинге.

6.2. Требования к видам обеспечения Терминала

6.2.1. Требования к программному обеспечению

Debian GNU/Linux 7.8 (wheezy) Release: 7.8

Файловая система ext3 или ext4.

6.2.2. Требования к аппаратному обеспечению

- ▶ Архитектура процессора x86-64;
- ▶ Объем ОЗУ не менее 4Gb;
- ▶ Многоядерный ЦП уровня Intel Core 2 Duo 3.0 Ghz и выше;
- ▶ Объем жесткого диска не менее 40 Gb.

6.2.3. Требования к доступу в Интернет

Компьютер, на котором устанавливается Терминал, должен иметь доступ в Интернет к репозиторию Debian и к Процессингу по адресу `tcp://service.cyberft.ru`:

- ▶ для тестовой эксплуатации
`tcp://service.cyberft.ru:50090`
- ▶ для коммерческой эксплуатации
`tcp://service.cyberft.ru:50091`

А также к следующим ресурсам:

- ▶ `download.cyberplat.ru` (109.72.129.138, TCP/443, 80)
- ▶ используемые репозитории ОС Debian (HTTP, FTP).

Компьютер оператора должен иметь доступ к веб-интерфейсу Терминала (порт 443, 80).

6.3. Структура дерева каталогов Терминала

В рабочей директории Терминала `/var/www/cyberswift/` содержатся следующие файлы и директории:

- **storage** Хранилище документов, ключей и сертификатов внутри Терминала
 - **documents** Хранилище документов
 - **in** Хранилище входящих документов
 - **origins** Хранилище всех входящих документов без каких-либо преобразований*
 - **containers** Хранилище расшифрованных контейнеров входящих документов, порождаемых из фреймов*
 - **sources** Хранилище экстрактированных из контейнеров входящих документов*
 - **invalid** Хранилище "битых" входных документов, которые нельзя никак зарегистрировать*
 - **out** Хранилище исходящих документов
 - **containers** Хранилище контейнеров исходящих документов, порождаемых из исходных документов*
 - **sources** Хранилище исходных документов*
 - **invalid** Хранилище исходных документов, которые не удалось зарегистрировать в БД Терминала и отправить*

Например, если UUID документа уже присутствует в БД, то документ не регистрируется, а попадает в `invalid`.

- **temp** Каталог для временных файлов*
- **keys** Каталог для ключей автобота
- **import** Папка для импорта внутрь Терминала
- **export** Хранилище входящих документов, экспортированных из Терминала
 - **swift** Хранилище экспортированных swift-документов
 - **cyberxml** Хранилище экспортированных CyberXML-документов формата StatusReport
 - **documents** Хранилище экспортированных CyberXML-документов формата Statement (выписка) и ProvCSV.
- **config** конфигурация для клиентов

* Каталог имеет динамически создаваемую вложенную структуру. Это означает, что в нем создаются каталоги, каждый из которых содержит указанные документы числом не более 10000. При переполнении каталога создается новый каталог. Таким образом происходит защита от переполнения файловой системы.

Согласно приведенной структуре, адреса некоторых директорий, которые могут понадобиться для настройки, выглядят следующим образом:

/var/www/cyberswift/import - директория для исходящих файлов (отправка в Процессинг из АБС);

/var/www/cyberswift/export/swift - используется для **экспорта** документов во внешнюю систему (АБС).

/var/www/cyberswift/export/cyberxml - используется для **экспорта** статусов обработки документов, проходящих через обмен в сети CyberFT, во внешнюю систему (АБС).

Входящие документы, имеющие недоверенные подписи, в обработку не передаются, хранятся вместе с остальными входящими контейнерами по адресу:

/var/www/cyberswift/storage/documents/in/containers

7. УСТАНОВКА И НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ

7.1. Установка Debian/Linux

Рекомендации по установке ОС: Debian GNU/Linux 7.8 (wheezy) Release: 7.8

Стабильно совместимый с CyberFT образ ОС доступен по ссылке <http://download.cyberft.ru/OS/>, рекомендуется использовать его.

Если планируется самостоятельно скачивать ОС с официального зеркала, при установке должны использоваться следующие параметры:

- ▶ При выборе образа для загрузки выбрать сборку amd64
- ▶ В диалоге выбора варианта установки рекомендуется выбрать пункт "64 bit Install"
- ▶ В диалоге выбора зеркала для закичивания обновлений выбрать страну "Russian Federation" и зеркало "mirror.yandex.ru":
- ▶ В диалоге выбора устанавливаемого ПО стоит отключить установку: "Debian desktop environment", "Print Server".

8. УСТАНОВКА И НАСТРОЙКА ТЕРМИНАЛА

8.1. Состав и содержание дистрибутива

Дистрибутив Терминала поставляется в формате **deb** пакета. Состав дистрибутива:

- ▶ Исполняемые файлы Терминала;
- ▶ Конфигурация окружения;
- ▶ Исполняемые файлы веб-интерфейса.

8.2. Инсталляция Терминала

До установки получите адрес Терминала Участника у менеджера по интеграции.

Рекомендуется производить установку пакета на «свежую» систему.

Возврат к предыдущим экранам для исправления введенных данных доступен в диалогах по команде Cancel.

Для установки Терминала необходимо загрузить DEB пакет на сервер. Дистрибутивы располагаются по адресу <http://download.cyberft.ru/>.

Установка должна производиться через консоль из-под пользователя **root**.

- ▶ Перед запуском установки желательно обновить списки пакетов из репозиториев командой **apt-get update**
- ▶ Для запуска установки выполните команду **dpkg -i {\$packageName}.deb**

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Dec 19 15:15:27 2014 from karazhas.cyberplat.com
root@cyberswift-rp:~# dpkg -i /root/cyberft_2.1_amd64.deb
```

Рисунок 1. Пример выполнения команды `dpkg -i`

- ▶ В случае, если в системе будут найдены недостающие пакеты, менеджер пакетов сообщит об этом. В таком случае необходимо выполнить команду `apt-get -f install`

```
dpkg: ошибка при обработке параметра cyberft:amd64 (--install):
проблемы зависимостей – оставляем не настроенным
При обработке следующих пакетов произошли ошибки:
cyberft:amd64
root@cyberswift-deb:~# apt-get -f install
```

Рисунок 2. Пример выполнения команды `apt-get -f install`

Будут установлены недостающие зависимости и сам пакет.

- ▶ В процессе установки установщик задаст вопросы, в соответствии с ответами на которые будет произведена настройка окружения и основных компонентов.
- ▶ В процессе установки может потребоваться дополнительное место для пакетов. Установщик спросит разрешение на продолжение установки

```
incron libdbd-mysql-perl libmysqlclient18 mysql-client-5.5 mysql-common
mysql-server mysql-server-5.5 mysql-server-core-5.5 nginx openssl php-apc
php5-cli php5-common php5-fpm php5-mcrypt php5-mysqlnd redis-server
обновлено 0, установлено 17 новых пакетов, для удаления отмечено 0 пакетов, и 0
пакетов не обновлено.
не установлено до конца или удалено 1 пакетов.
Необходимо скачать 15,6 МБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 115 МБ
.
Хотите продолжить [Д/н]? д
```

Рисунок 3. Запрос на установку дополнительных пакетов.

- ▶ При установке MySQL Server система попросит ввести пароль административного пользователя MySQL «root».

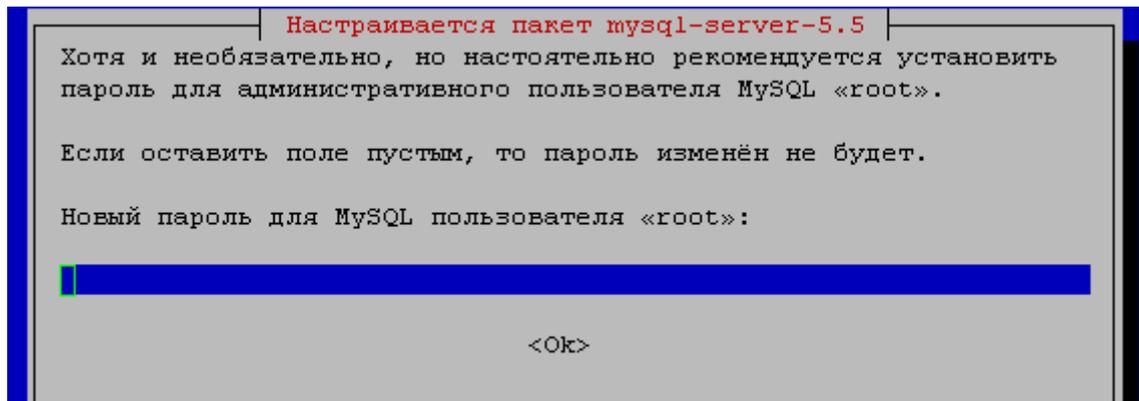


Рисунок 4. Регистрация пароля администратора БД MySQL для пользователя «root».

- ▶ Подтвердите пароль

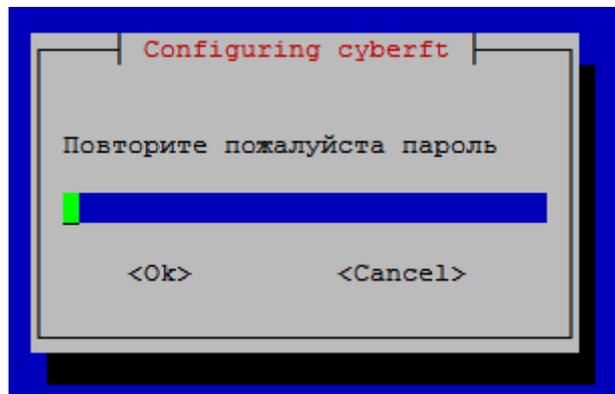


Рисунок 5. Подтверждение пароля.

- ▶ Укажите введенный на предыдущем экране пароль к БД для пользователя root (нужен для подключения deb-пакета к БД).

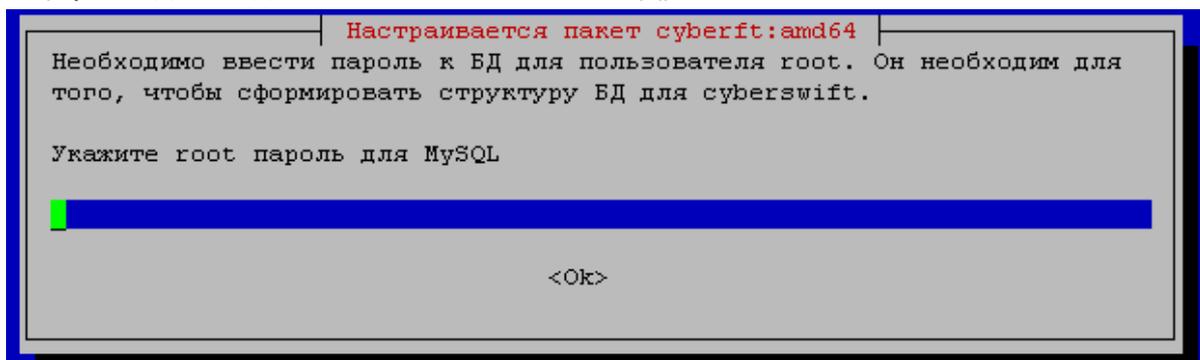


Рисунок 6. Ввод пароля к БД MySQL для пользователя «root».

- ▶ Укажите название БД

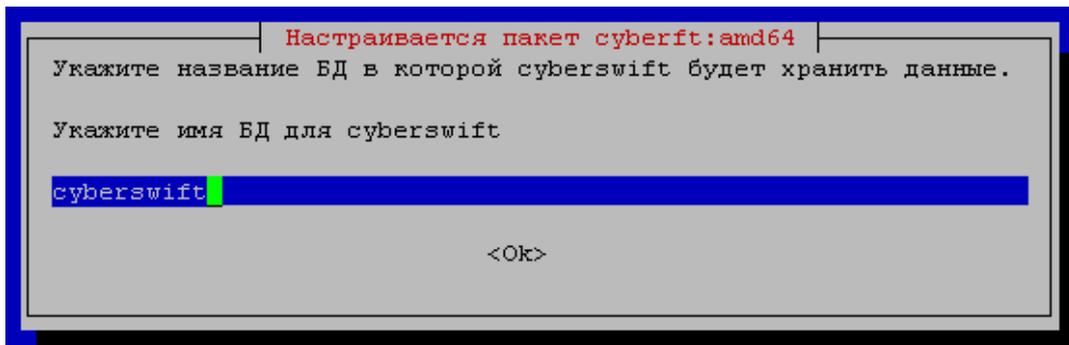


Рисунок 7. Ввод названия БД.

- ▶ Укажите пароль нового пользователя БД для cyberswift

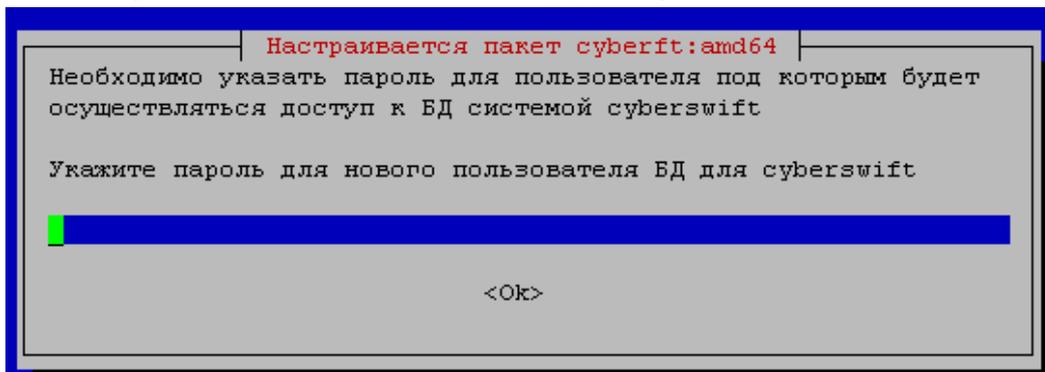


Рисунок 8. Ввод пароля пользователя ДБ.

- ▶ Подтвердите пароль

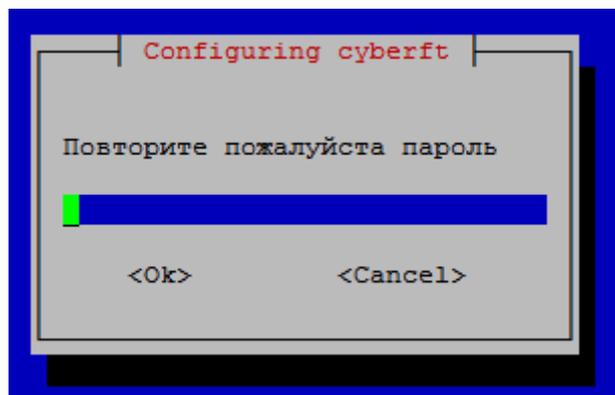


Рисунок 9. Подтверждение пароля.

- ▶ Укажите временную зону сервера

Временная зона указывается в соответствии с форматом для Linux систем. Список поддерживаемых timezones доступен по ссылке:

<http://php.net/manual/ru/timezones.php>

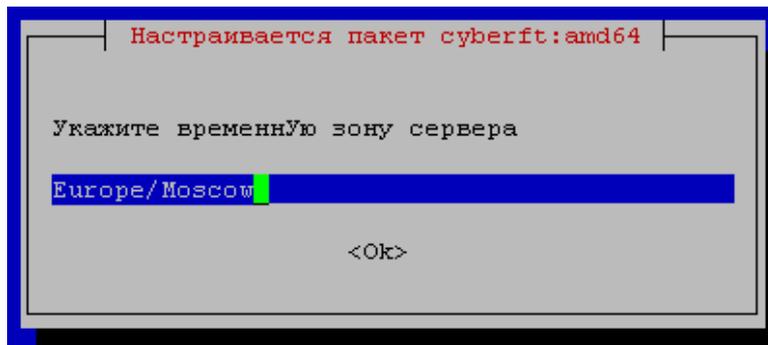


Рисунок 10. Ввод временной зоны сервера.

- ▶ Укажите servername для конфигурации nginx

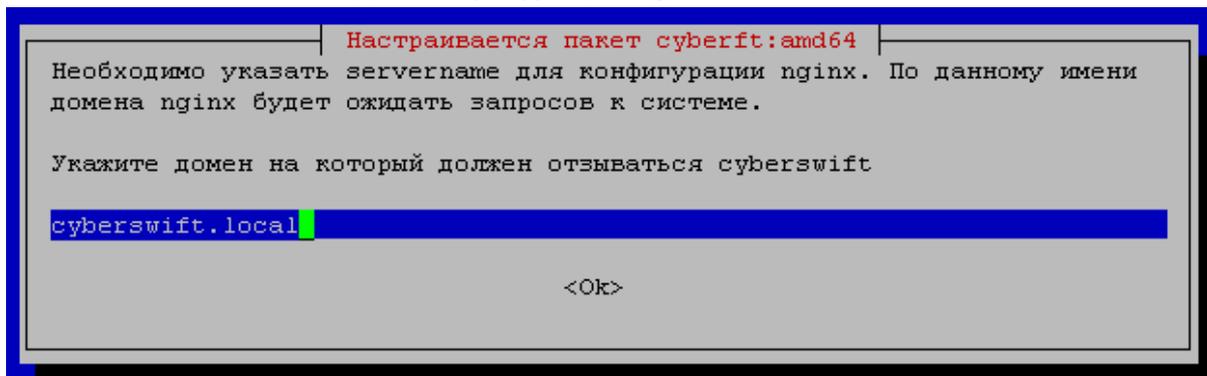


Рисунок 11. Ввод servername для конфигурации nginx.

- ▶ Укажите название Вашей компании

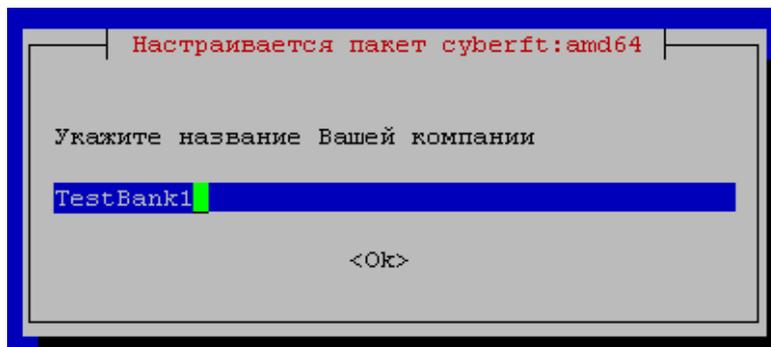


Рисунок 12. Ввод названия компании.

- ▶ Укажите адрес Терминала в системе CyberFT

Адрес Терминала необходимо предварительно получить у вашего менеджера по интеграции в «Киберплат». Если Вы не знаете адрес вашего Терминала, то необходимо написать запрос по адресу support@cyberft.ru.

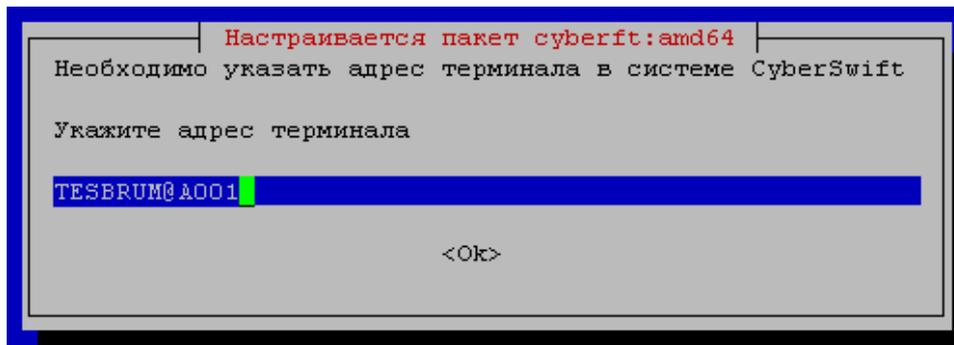


Рисунок 13. Ввод адреса Терминала.

- ▶ Подтвердите активацию Samba.

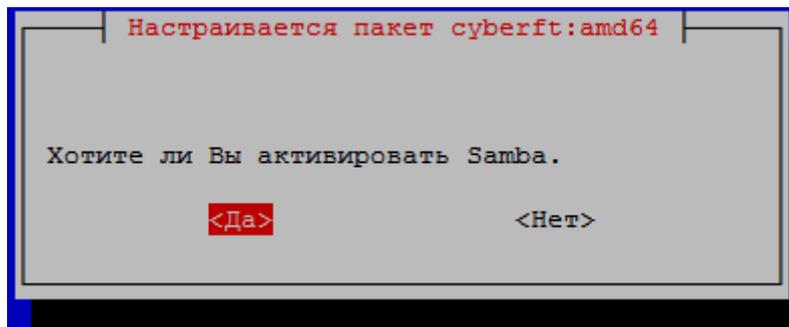


Рисунок 14. Активация Samba.

- ▶ Укажите пароль монтирования Samba на внешней системе (применение см. в разделе 8.7 «Подключение каталогов CyberFT как сетевых дисков Windows» данного Руководства).

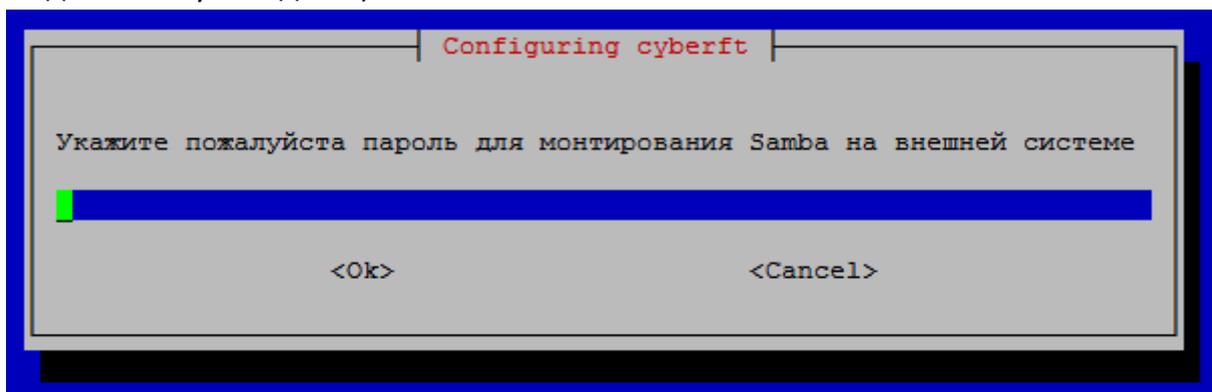


Рисунок 15. Ввод пароля Samba.

- ▶ Подтвердите пароль

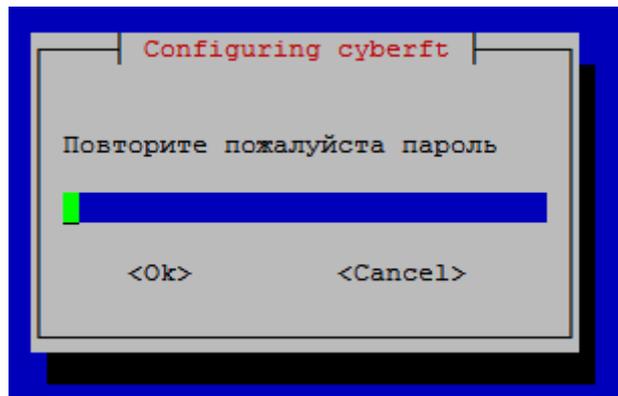


Рисунок 16. Подтверждение пароля.

- ▶ Укажите логин Главного администратора (ГА).
Связка логин/пароль используется для доступа к веб интерфейсу терминала. По умолчанию используется логин admin@cyberft.com

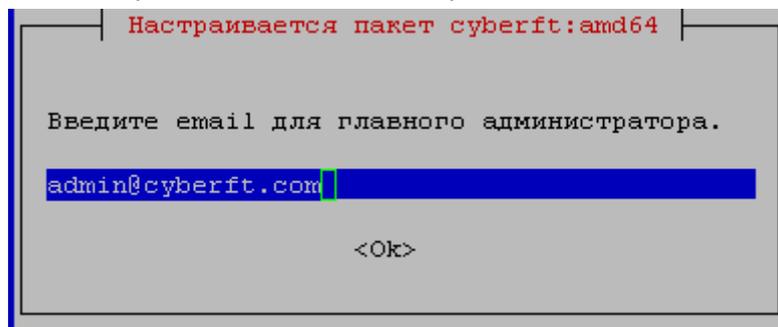


Рисунок 17. Регистрация логина ГА.

- ▶ Укажите пароль ГА.

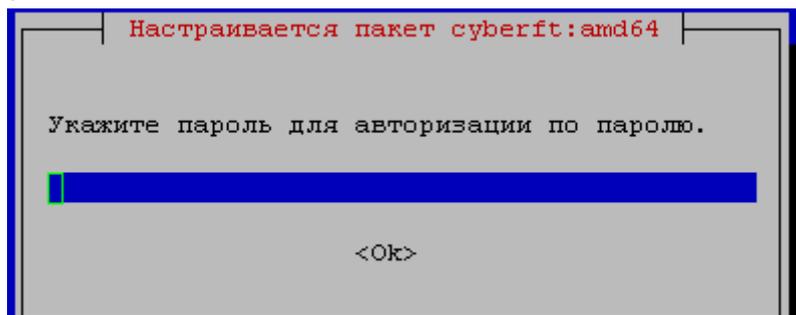


Рисунок 18. Регистрация пароля ГА.

- ▶ Укажите пароль для сертификата ГА

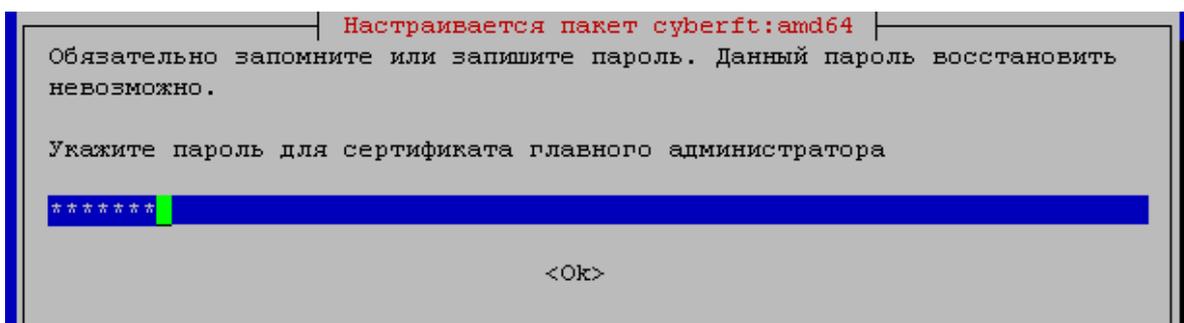


Рисунок 19. Ввод пароля для сертификата ГА.

ВНИМАНИЕ!

Если в вашей системе открыта авторизация из-под root пользователя, то установщик выдаст предупреждающее сообщение:

```
# На вашей системе открыта авторизация из под root пользователя. Безопасность терминала под угрозой!  
# Скорректируйте файл /etc/ssh/sshd_config. Установите значение параметра PermitRootLogin no  
# Выполните перезапуск службы /etc/init.d/sshd restart
```

Рисунок 20. Предупреждение об открытой авторизации из-под root.

Для обеспечения необходимого уровня безопасности рекомендуем запретить авторизацию из-под root пользователя выполнив указанные действия.

Инсталляция Терминала завершена!

8.3. Обновление Терминала

Компания CyberPlat периодически выпускает новые релизы Терминала CyberFT. Для установки новой версии нет необходимости деинсталлировать прежнюю версию. Новые версии устанавливаются поверх прежней.

Для обновления версии Терминала необходимо скачать новый DEB пакет по ссылке <http://download.cyberft.ru/>, загрузить его на сервер Терминала и выполнить в консоли команду `dpkg -i {$packageName}.deb`. Система установит необходимые обновления, не затирая прежние каталоги и находящиеся в них данные.

8.4. Реконфигурация Терминала

Параметры, заданные при установке Терминала, доступны для редактирования.

Если установка еще не завершена – редактирование заданных параметров доступно через последовательное нажатие кнопки **Cancel**.

Если установка уже была пройдена, для реконфигурации нужно остановить обмен с сетью CyberFT (см.п.9.2.5 данного Руководства), и вызвать консольную команду:

dpkg-reconfigure cyberft

Для редактирования будут последовательно выведены все те же окна конфигурации, которые были доступны при установке (описаны в разделе 8.2 Инсталляция Терминала данного Руководства).

8.5. Деинсталляция Терминала

Для деинсталляции Терминала могут использоваться консольные команды:

apt-get purge cyberft – полностью удалить Терминал и все связанные данные,

apt-get remove cyberft – полностью удалить Терминал с сохранением данных,

/var/www/cyberswift/www/yii document/purge – Команда очищает БД и директории для документов.

Для аварийного удаления пакета Терминала со всеми данными используется скрипт **emergencyRemove.sh**. Скрипт находится в папке Utilities:

<http://download.cyberft.ru/Utilities/emergencyRemove.zip>

Необходимо перенести файл на сервер, где установлен Терминал (например, в папку root) и запустить скрипт emergencyRemove.sh через консоль командой sh:

sh /root/emergencyRemove.sh либо **../root/emergencyRemove.sh**

Может потребоваться прописать права на выполнение данной операции для файла.

Для этого необходимо до запуска скрипта выполнить команду:

chmod 0700 emergencyRemove.sh

8.6. Особенности конфигурации окружения

Вместе с пакетом устанавливаются следующие компоненты:

gcc(>= 4.7.1); uuid-dev(>=2.20.1); uuid(>=1.6.2); nginx(>=1.2.0); mysql-server (>=5.5.30); redis-server (>=2.4.14); openssl (>=1.0.1); php5-fpm, php5-common, php5-cli, php5-mcrypt, php5-mysqlnd, php-apc (версия >=5.4.x) php5-curl; incron; cups; lpr; pecl; pecl/stomp, sudo, less, fail2ban, samba, task-spooler

В процессе установки будут выполнены следующие операции:

- ▶ Для **mysql** будет добавлен файл конфигурации **/etc/mysql/conf.d/cyberswift.conf**. Устанавливаются оптимизированные показатели для лучшей работы БД. Опционально можно удалить данный файл, но настоятельно рекомендуется

активировать в основном конфиге опцию **innodb_file_per_table**. На базовых настройках со временем вероятно снижение производительности.

- ▶ Для nginx будет добавлен файл конфигурации **/etc/nginx/sites-available/cyberswift.conf** и ссылка **/etc/nginx/sites-enabled/cyberswift.conf**. Создается отдельный виртуал-хост и указывается в качестве хоста по умолчанию (default).
- ▶ Для php будет добавлен файл конфигурации **/etc/php5/fpm/pool.d/cyberswift.conf**. Создается отдельный пул процессов.

В качестве демонов работают следующие компоненты:

- ▶ php-fpm
- ▶ nginx
- ▶ fail2ban: `/usr/bin/python /usr/bin/fail2ban-server -b -s /var/run/fail2ban/fail2ban.sock`
- ▶ samba: `/usr/sbin/smbd`
- ▶ redis: `/usr/bin/redis-server /etc/redis/redis.conf`
- ▶ task-spooler: `/usr/bin/tsp`
- ▶ mysql: `/usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306`
- ▶ mysql: `/bin/sh /usr/bin/mysqld_safe`

8.7. Подключение каталогов CyberFT как сетевых дисков Windows

1. На терминале в файле **/etc/samba/cyberswift.conf** расположена конфигурация подключения, при необходимости редактируете параметры:

```
[cyberswift_import]
path = /var/www/cyberswift/import
valid users = @www-data
guest ok = no
writable = yes
browsable = no
create mask = 0755
directory mask = 0755

[cyberswift_export_swt]
path = /var/www/cyberswift/export/swift
valid users = @www-data
guest ok = no
writable = yes
browsable = no
create mask = 0755
directory mask = 0755

[cyberswift_export_xml]
path = /var/www/cyberswift/export/cyberxml
valid users = @www-data
```

```
guest ok = no
writable = yes
browsable = no
create mask = 0755
directory mask = 0755
```

2. В Windows подключаете сетевые диски:

\\IP терминала\cyberswift_import

\\IP терминала\cyberswift_export_swf

\\IP терминала\cyberswift_export_xml

3. При подключении указываете логин/пароль:

User: www-data

Password: пароль Samba, указанный при установке/реконфигурации, см. рисунок «Ввод пароля Samba.».

4. Перезапускаете на Терминале incron консольной командой

/etc/init.d/incron restart

После успешной настройки в сетевых дисках Windows должны быть видны файлы из соответствующих каталогов Linux

При импорте корректного файла сообщения в сетевой диск **cyberswift_import** в Терминале должно зарегистрироваться сообщение (или маршрутизироваться в папку swift).

8.8. Возможные проблемы на Терминале

Команды проверки incron:

su www-data -c "incrontab -e" проверка параметров incron

/etc/init.d/incron restart перезапуск incron

В каких случаях применяется: из каталога import файлы не импортируются в Терминал.

9. ВЕБ-ИНТЕРФЕЙС ГЛАВНОГО АДМИНИСТРАТОРА

9.1. Доступ к веб-интерфейсу Терминала

Доступ к веб-интерфейсу управления Терминалом осуществляется по IP сервера, где развернут Терминал. Авторизация осуществляется по логину/паролю администратора.

Для авторизации по логину/паролю необходимо нажать на кнопку **«Вход в систему с паролем»**.

Кнопка «Войти в систему» служит для аутентификации по ключу. Данная функция

может использоваться только в браузере IE>9 версии, при этом необходимо установить SDK CAPICOM и ключи в хранилище windows.

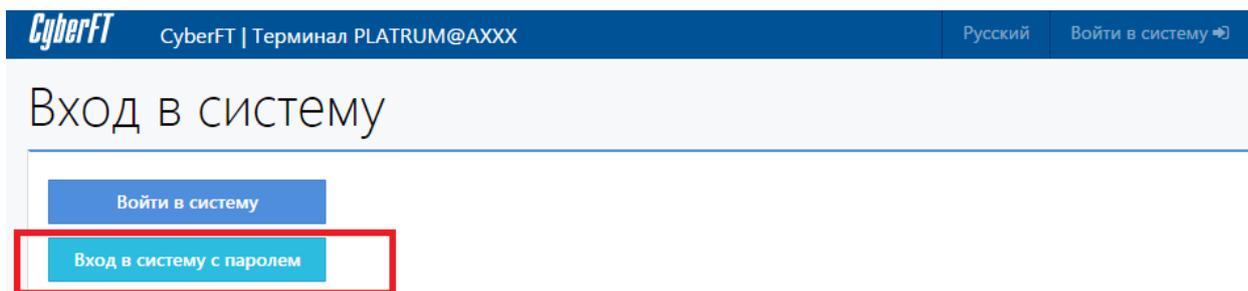


Рисунок 21. Подключение к интерфейсу Терминала.

Следующим экраном отобразится форма авторизации. Необходимо ввести логин (регистрационный Email) и пароль. После чего нажать кнопку **«Войти в систему»**:

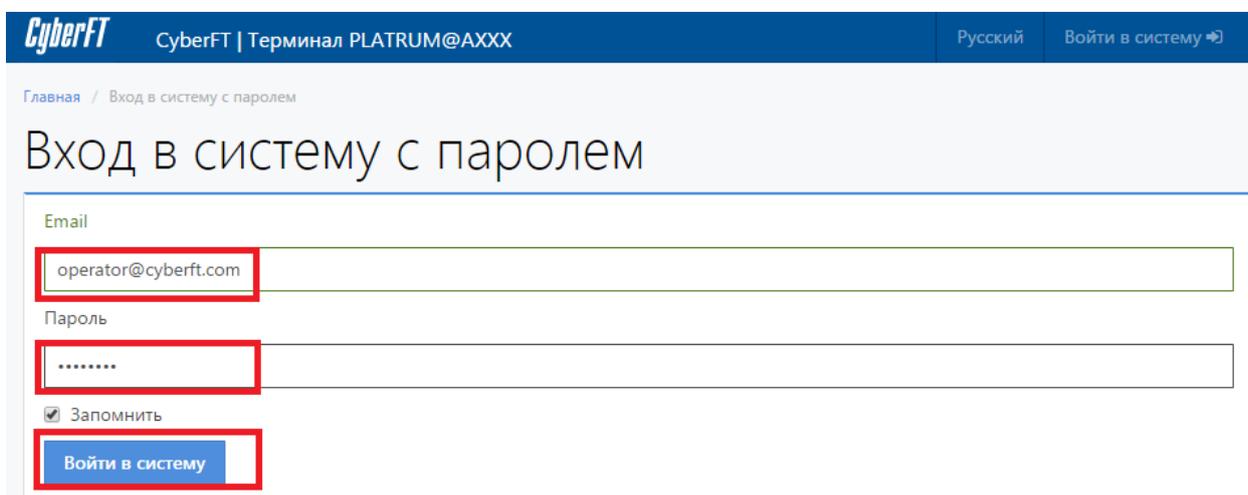


Рисунок 22. Вход в систему по логину/паролю.

9.2. Настройка ключей перед началом работы

После установки терминала необходимо настроить ключи, а именно:

1. Сгенерировать ключ Автоподписанта.
2. Отправить сертификат открытого ключа Автоподписанта в Cyberplat для регистрации в Процессинге CyberFT по адресу support@cyberft.ru.
3. Обменяться сертификатами открытых ключей со связанными участниками.

Далее в этом разделе последовательность работы с ключами описана подробно.

9.2.1. Генерация ключа Автоподписанта

Для того, чтобы сгенерировать ключ Автоподписанта, заходим в меню «Автоподписант» и нажимаем «Генерировать ключи»:

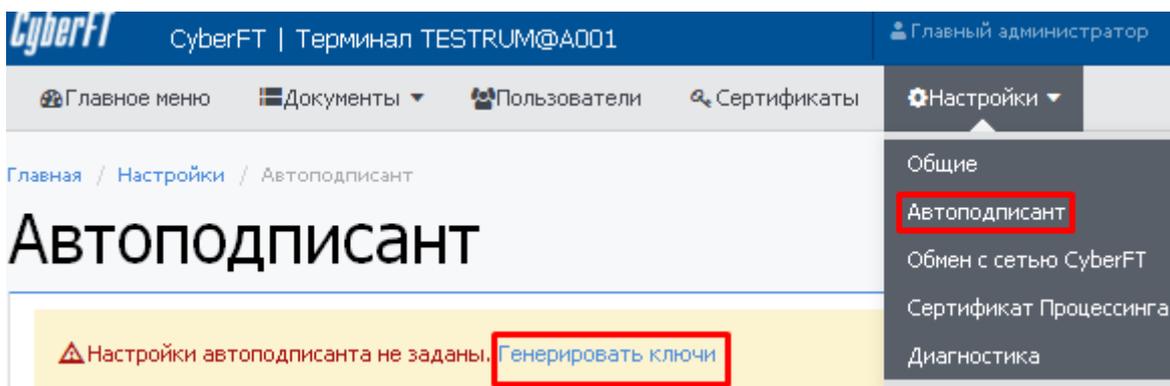


Рисунок 23. Генерация ключа Автоподписанта.

Перед изменением ключей Автоподписанта система выдаст предупреждающее сообщение.

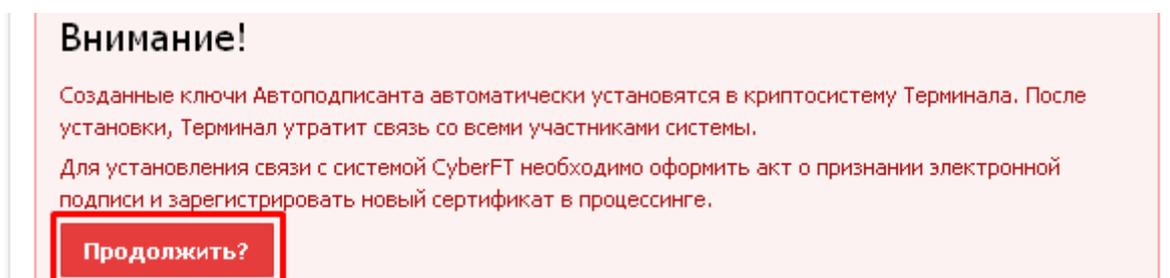


Рисунок 24. Предупреждающее сообщение при изменении ключей Автоподписанта.

Данное сообщение говорит о том, что в случае изменения ранее созданного и зарегистрированного ключа Автоподписанта дальнейший файловый обмен со старым ключом становится невозможен. Для возобновления работы будет необходимо зарегистрировать новый сертификат открытого ключа Автоподписанта в Процессинге CyberFT и передать его всем связанным партнерам по сети CyberFT для установки в Терминалы.

Далее нужно придумать безопасный пароль для секретного ключа (рекомендуемый формат: от 8 символов, с использованием цифр, букв и спец.символов), ввести его в оба текстовых поля, и нажать кнопку **«Генерировать ключи»**.

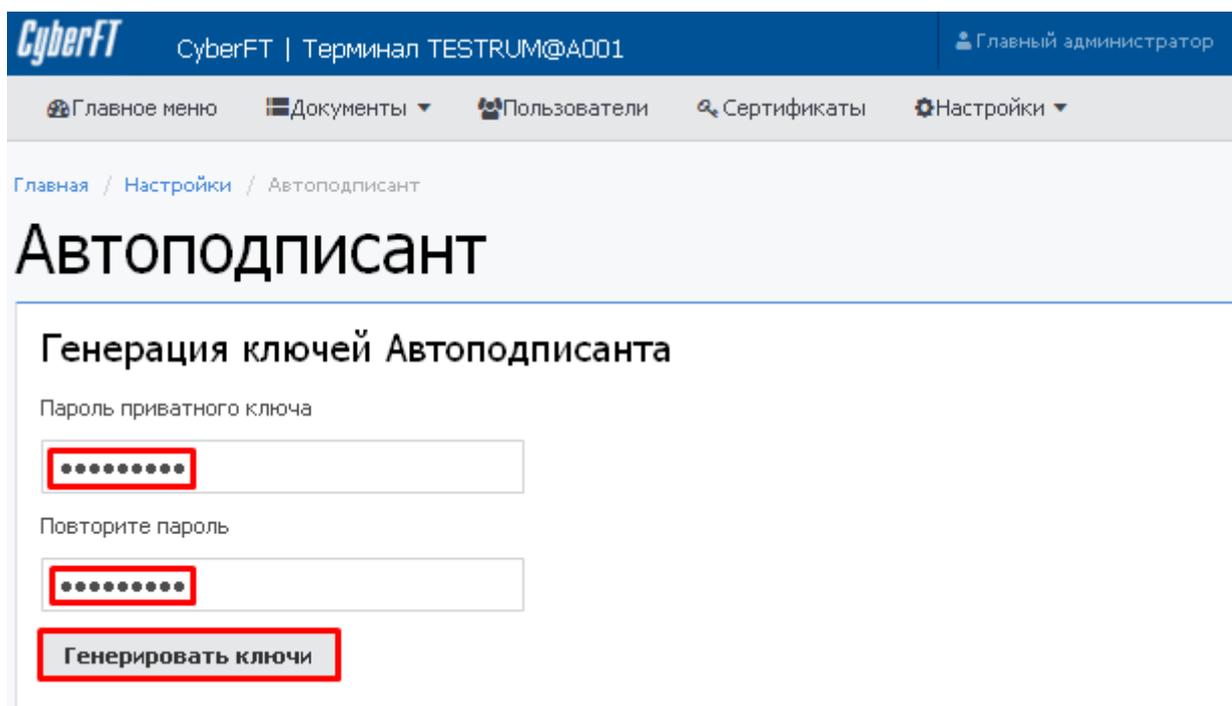


Рисунок 25. Задание пароля для генерации ключей Автоподписанта.

В случае успеха будет выведено сообщение «Настройки автоподписанта обновлены».

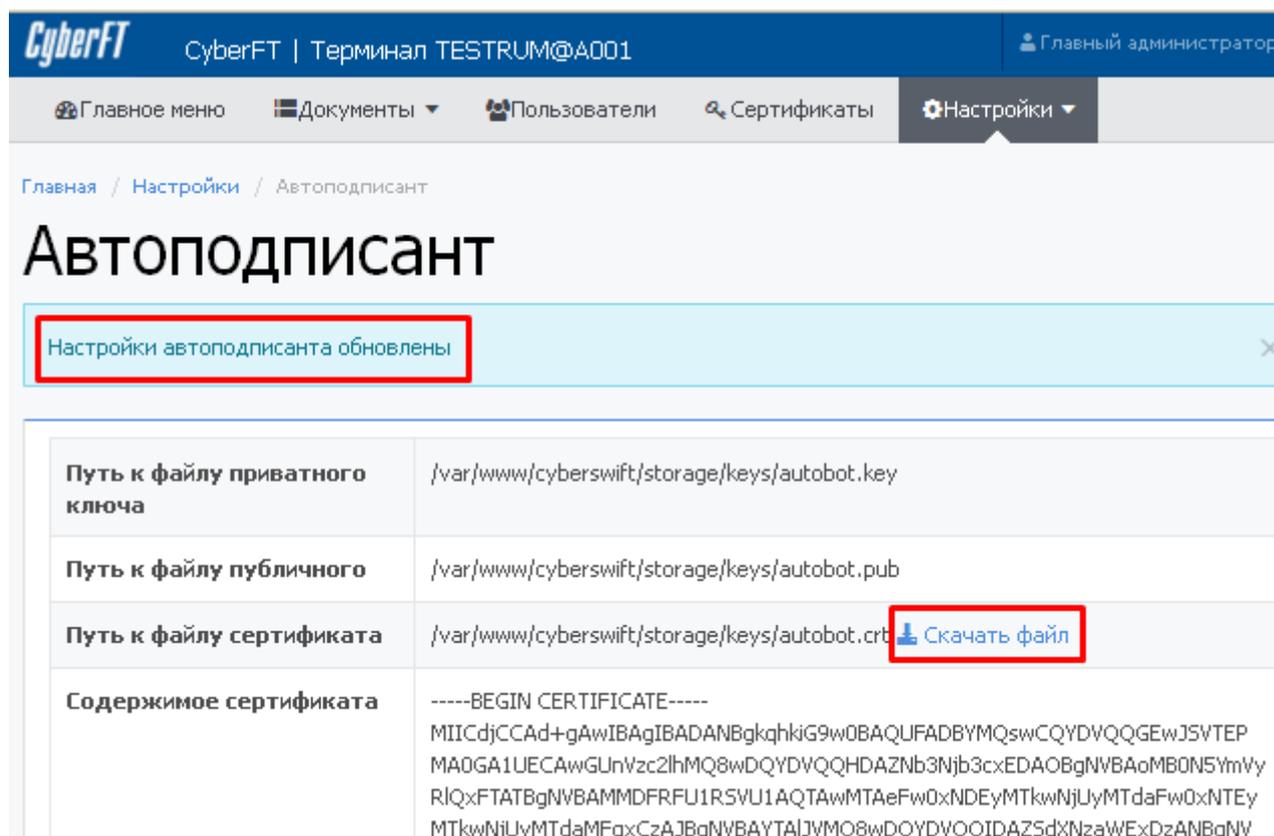


Рисунок 26. Данные сертификата Автоподписанта.

Для выполнения дальнейших шагов по настройке ключей, на этом экране необходимо получить файл вашего сертификата, нажав кнопку «Скачать файл». В дальнейшем доступ к этому экрану осуществляется из меню «Настройки / Автоподписант».

На Терминале ключи Автоподписанта хранятся по адресу

`/var/www/cyberswift/storage/keys`

9.2.2. Отправка сертификата открытого ключа

После нажатия кнопки «Скачать файл» будет сформирован файл открытого ключа связанного участника, имеющий следующий вид:

cyberft-terminal-[ID терминала участника].[расширение «crt»] Например:

cyberft-terminal-MRBBRUMMAXXX.crt.

Данный файл необходимо отправить по адресу support@cyberft.ru для регистрации в Процессинге CyberFT. Этот же файл необходимо будет в дальнейшем высылать другим Участникам при обмене сертификатами.

9.2.3. Установка открытого ключа Процессинга CyberFT

Далее необходимо зарегистрировать сертификат открытого ключа Процессинга.

Открытый ключ для подключения к тестовому процессингу доступен по ссылке <http://download.cyberft.ru/Testcert/>, пройдя по которой, нужно сохранить файл с локально (в браузере «Сохранить объект как» или аналог):

CYBERUM@TEST-900924C49EC6EC8488180F92A0E35EC7A0AB59AD.pem

Далее сертификат загружается через меню «Сертификаты», аналогично сертификатам других Участников (экраны данного процесса приведены в разделе 9.2.4 «Обмен сертификатами со связанными Участниками» данного Руководства).

Id Терминала тестового процессинга – **CYBERUM@TEST**

Открытый ключ для подключения к боевому процессингу уточняйте у вашего менеджера в CyberFT. Id Терминала боевого процессинга – **CYBERUM@AFTX**

9.2.4. Обмен сертификатами со связанными Участниками

При установлении связи участники CyberFT должны обмениваться друг с другом открытыми ключами автоподписанта и персональными ключей сотрудников (когда они будут сгенерированы пользователем). Файлы сертификатов ключей имеют вид:

Для автоподписанта:

[ID терминала участника]-[отпечаток сертификата].[расширение «crt»], например:

TESTZZZ@Z001-85E9A9BE7A9335CE16D2C990EDFD7EF703A50B61.crt

Для подписанта:

user[id]- [отпечаток сертификата].[расширение «crt»], например:

user4-2A82E7EE83E32FC460D26D11E715C035904FBFA5.crt

Файлы ключей сертификатов доступны:

Для автоподписанта – из меню «Настройки / Автоподписант», кнопка «скачать файл».

Для персонального ключа – из-под учётки данного сотрудника, в меню «Мои ключи и сертификаты».

Для добавления Сертификата другого участника нужно зайти в пункт меню «Сертификаты» и нажать кнопку «Добавить сертификат»

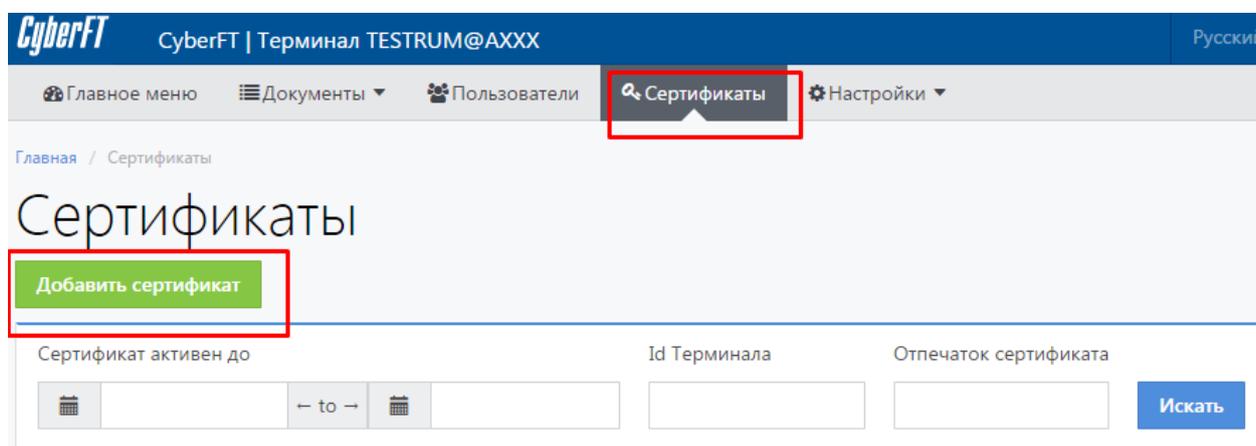


Рисунок 27. Регистрация ключа связанного Участника.

Указать идентификатор терминала добавляемого Участника в поле «ID Терминала» другого Участника, в поле «Сертификат» - путь до файла сертификата, выбрать соответствующую «Роль» в выпадающем списке и нажать кнопку «Создать».

Добавить сертификат

Сертификат	<input type="text"/>	<input type="button" value="Выбрать файл"/>
Id Терминала	<input type="text"/>	Необходимо заполнить «Id Терминала».
Активен до	<input type="text"/>	Необходимо заполнить «Активен до».
Роль	<input type="text" value="Undefined"/>	
Имя владельца	<input type="text"/>	
Должность	<input type="text"/>	
Email	<input type="text"/>	
Телефон	<input type="text"/>	
		<input type="button" value="Добавить"/>

Рисунок 28. Регистрация ключа связанного Участника.

На Терминале сертификаты участников хранятся по адресу
`/var/www/cyberswift/storage/certs`

9.2.5. Запуск обмена Терминала с сетью CyberFT

Автоматический обмен запускается из меню «Настройки».

Для запуска обмена необходимо перейти в п. меню «Настройки/ Обмен с сетью CyberFT», и ввести пароль приватного ключа Автоподписанта:

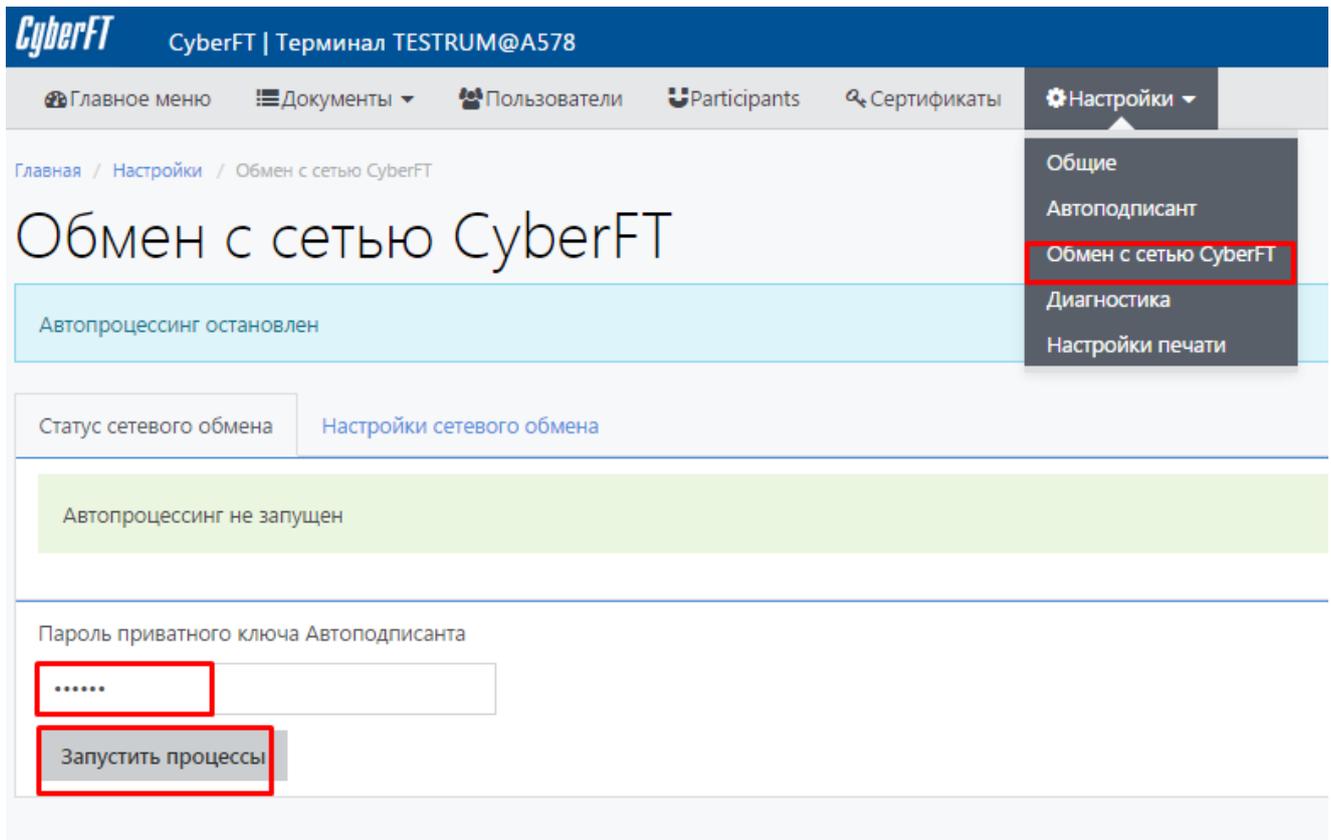


Рисунок 29. Запуск автоматического обмена сообщениями.

После запуска обмена должно появиться сообщение: **«Автоматические процессы запущены {дата время}»**.

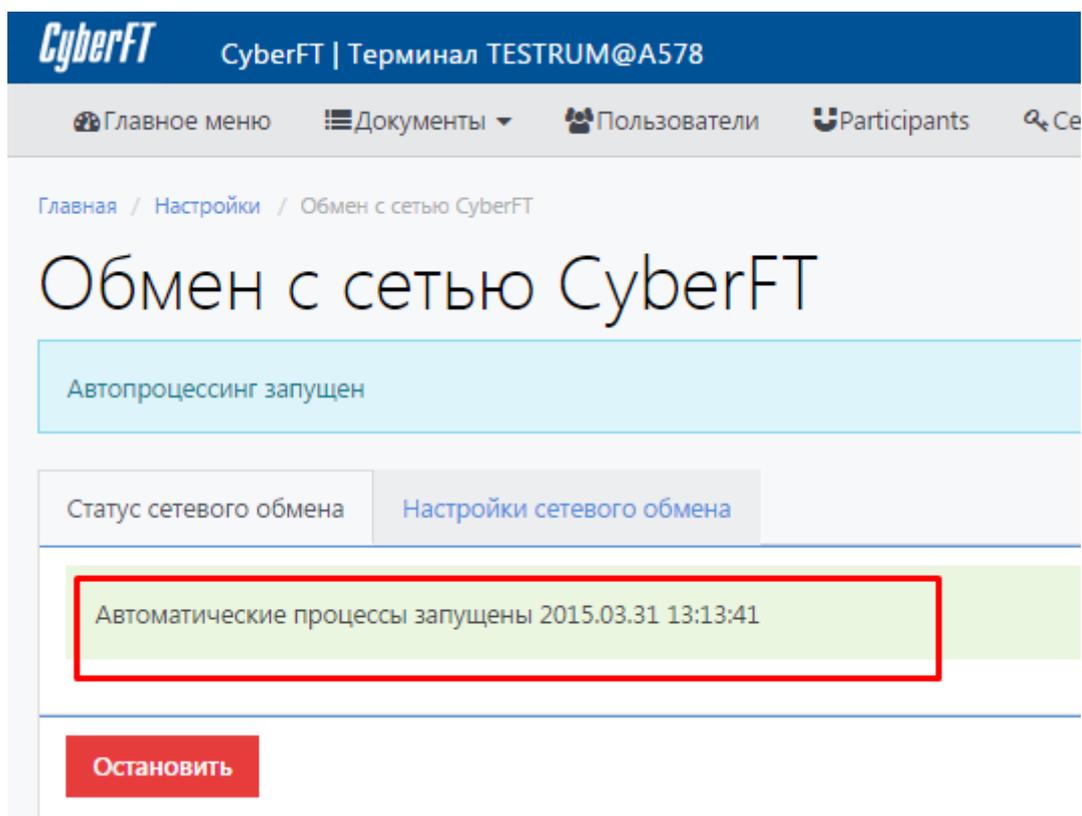


Рисунок 30. Запуск автоматических процессов.

Для остановки обмена, необходимо в этой же вкладке нажать кнопку **«Остановить»**.

При остановленном обмене, работает только процесс регистрации документов в Журнале документов, запросы к процессингу не выполняются.

9.3. Настройки и функции веб-интерфейса администратора

9.3.1. Замена ключа Автоподписанта

Для замены ключа Автоподписанта необходимо зайти в п. меню «Настройки / Автоподписант» и нажать кнопку **«Сбросить ключи автоподписанта»**.

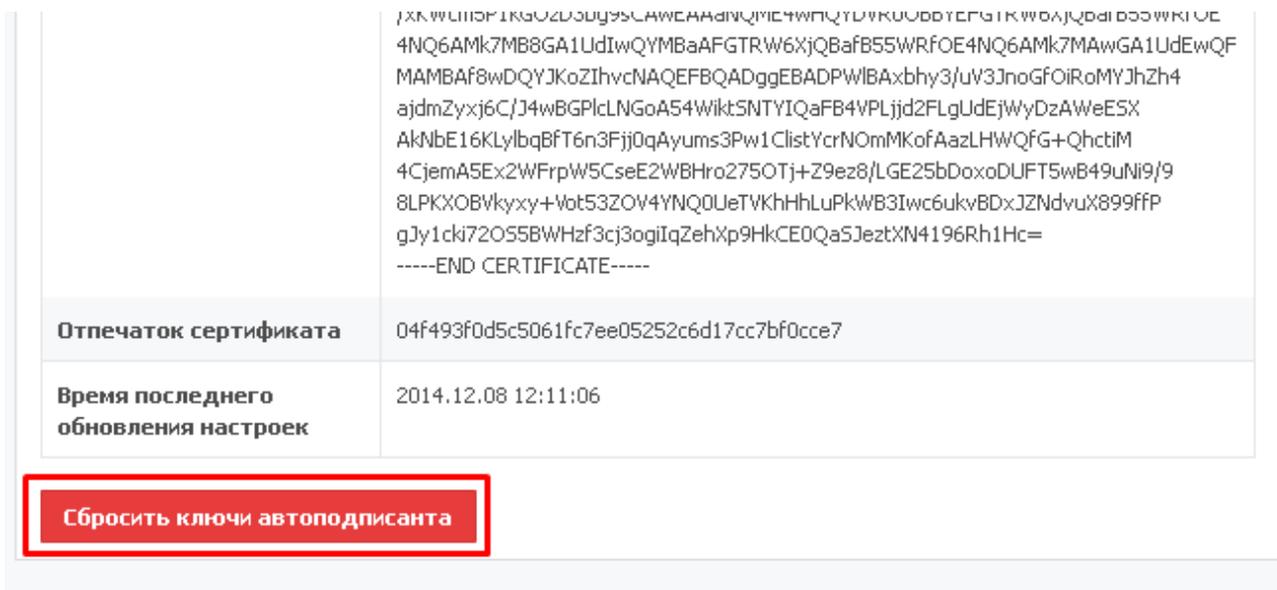


Рисунок 31. Сброс ключа Автоподписанта.

9.3.2. Редактирование адреса Терминала

Редактирование адреса Терминала не доступно через интерфейс администратора, и осуществляется в общем порядке реконфигурации (см. раздел 8.4 Реконфигурация Терминала).

9.3.3. Маршрутизация исходящих документов

В настройках Терминала CyberFT опционально может быть определена рабочая папка для экспорта документов из АБС в SWIFT следующим образом.

При загрузке документов (в папку **/var/www/cyberswift/import** либо через интерфейс из меню «Документ из файла») Терминал автоматически определяет принадлежность адреса получателя сети CyberFT.

Если Получатель является Участником CyberFT (критерий – наличие символа «@» в адресе Получателя), Терминал направляет ему документ по сети CyberFT. Если не является, то Терминал выгружает документ в папку для импорта в SWIFT (как задать см. ниже). Таким образом, Участникам CyberFT документы автоматически будут доставляться через CyberFT, а остальным организациям через SWIFT.

Для активации автоматической маршрутизации документов нужно зайти в меню Настройки/Общие, установить флаг в пункте «Активировать маршрутизацию swift документов», указать новую директорию для перенаправления документов через SWIFT и сохранить данные настройки.

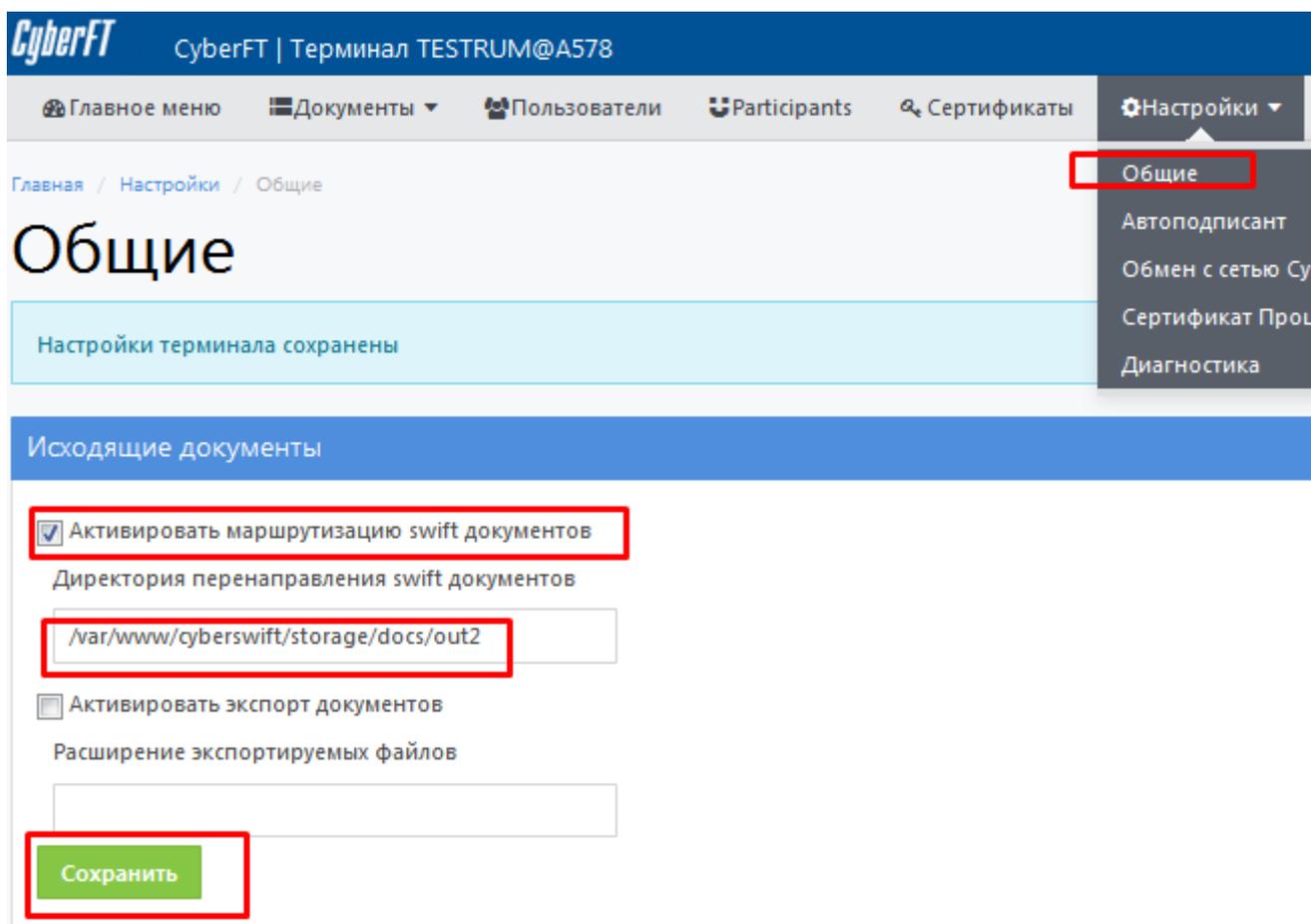


Рисунок 32. Настройка автоматической маршрутизации документов.

При этом, могут быть заданы исключения из общего правила маршрутизации swift «в зависимости от наличия символа @ в адресе Участника». А именно, если адрес Участника имеет SWIFT-формат (не содержит @), но при этом необходимо отправить документ через CyberFT, данный адрес должен быть прописан в таблице участников (меню «Участники»):

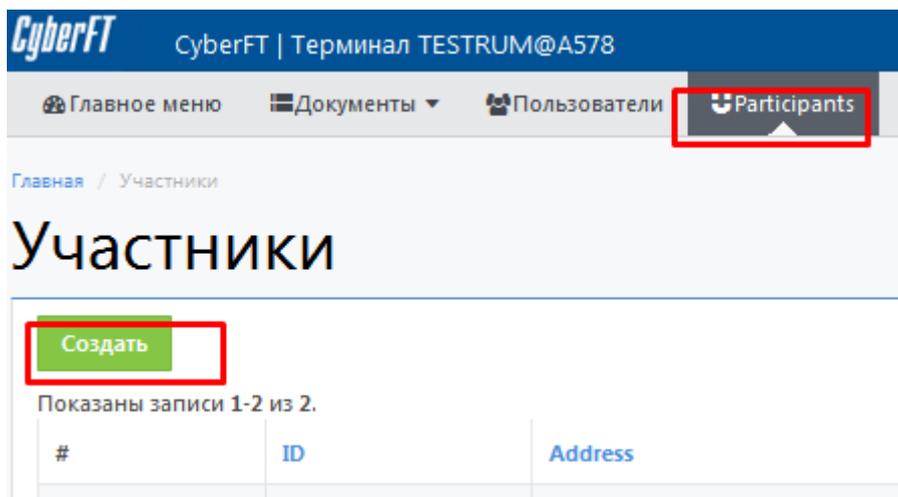


Рисунок 33. Управление исключениями из правила маршрутизации по SWIFT-адресам.

9.3.4. Активация экспорта документов и отчетов по статусу обработки документов

В настройках Терминала CyberFT могут быть определены правила экспорта документов для АБС. Для активации данной функции нужно зайти в меню Настройки/Общие, установить флаг в пункте «Активировать экспорт документов», указать расширение файлов документов, на которое настроена АБС и сохранить данные настройки.

В этом случае корректные входящие документы после проверки будут переименовываться и направляться в каталог **`/var/www/cyberswift/export/swift`**

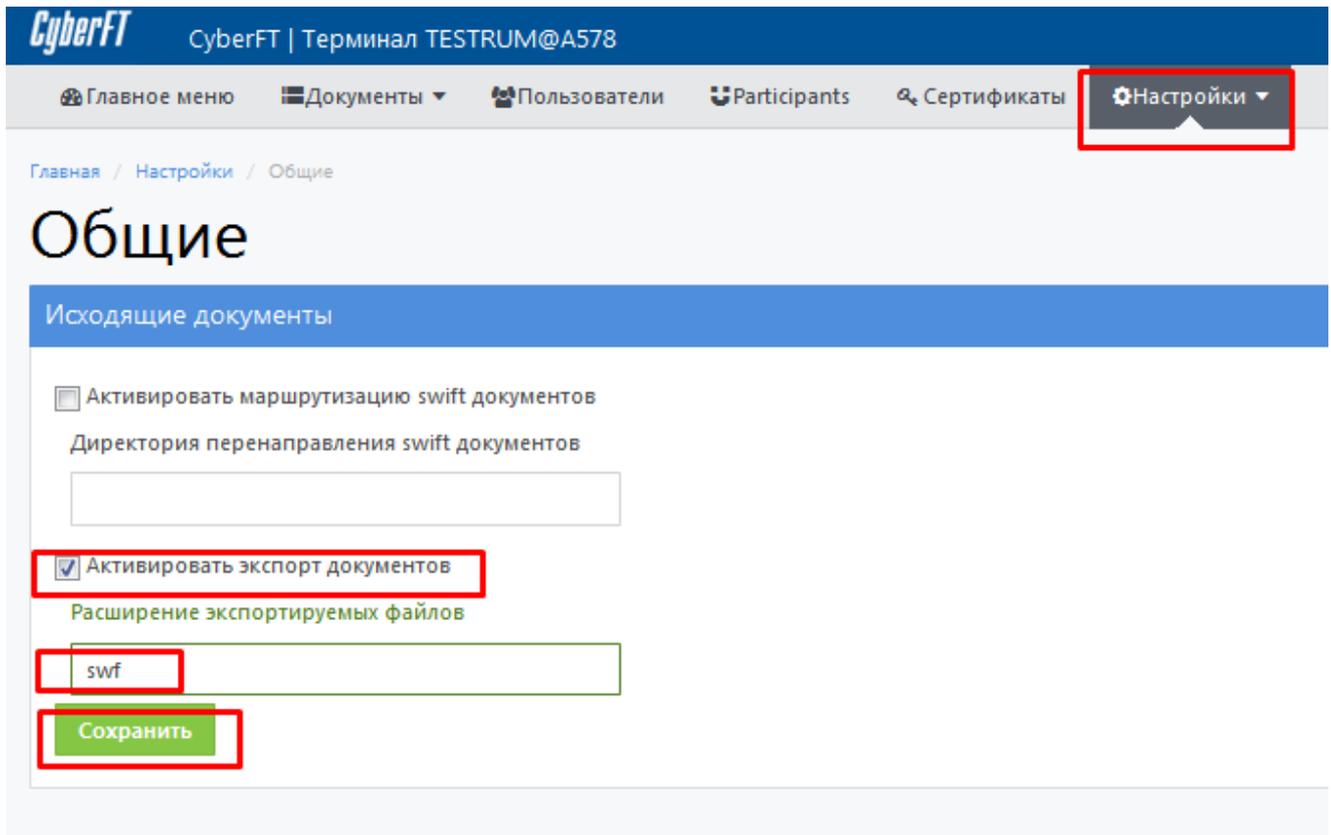


Рисунок 34. Активация экспорта входящих документов.

Также в настройках Терминала CyberFT для АБС могут быть определены правила экспорта отчетов по статусу обработки документов. Для активации данной функции нужно зайти в меню Настройки/Общие, установить флаг в пункте «Активировать экспорт документов в формате CyberXML» и сохранить данные настройки.

В этом случае отчеты по статусу будут направляться в каталог **`/var/www/cyberswift/export/cyberxml`**

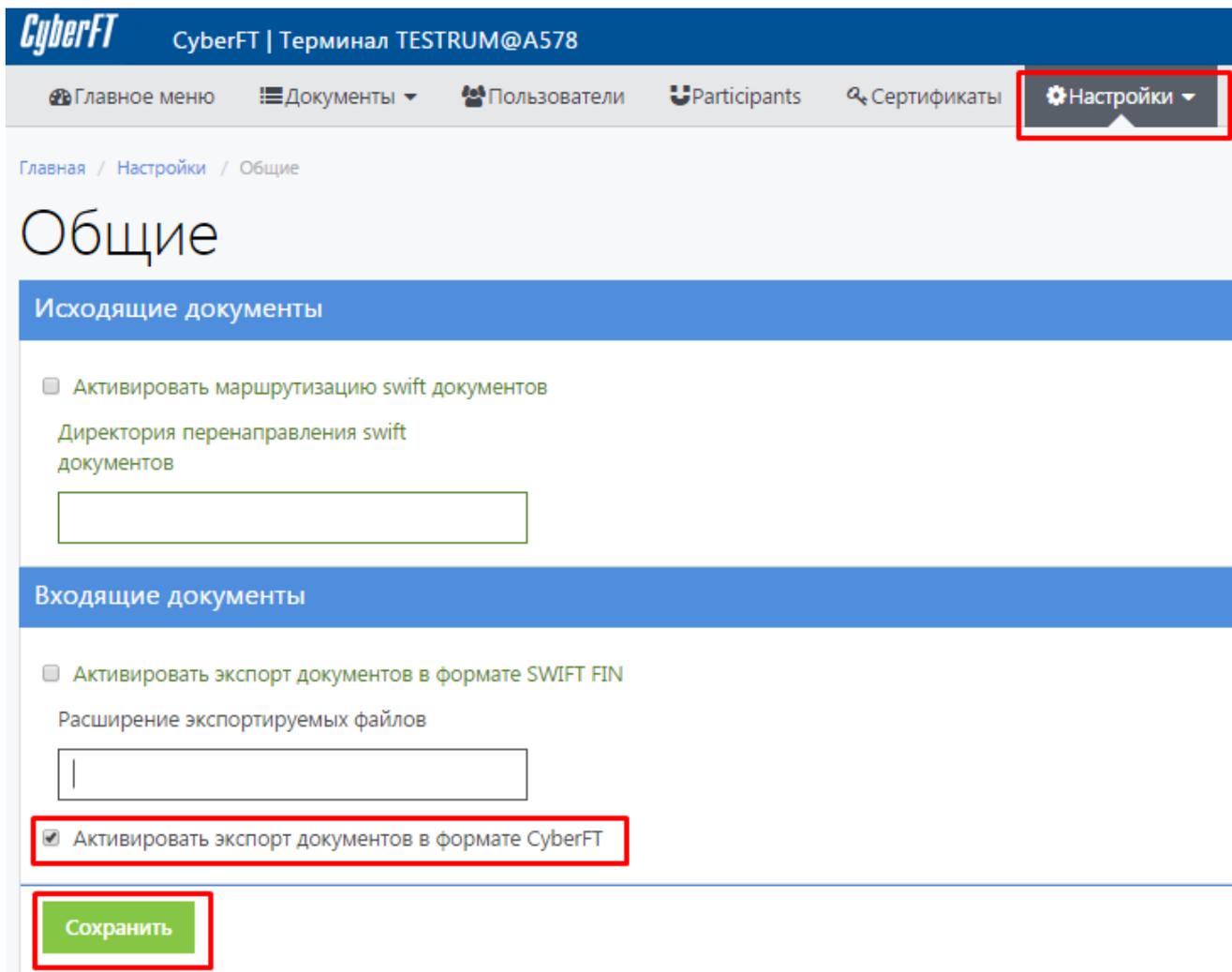


Рисунок 35. Активация экспорта отчетов по статусу.

9.3.5. Экспорт входящих документов на печать

Для входящих документов доступна настройка автоматической маршрутизации на принтер, в зависимости от типа. Для этого нужно зайти в главное меню в п. «Настройки», п.п. «Настройки печати», выбрать типы документов, и нажать кнопку сохранить.

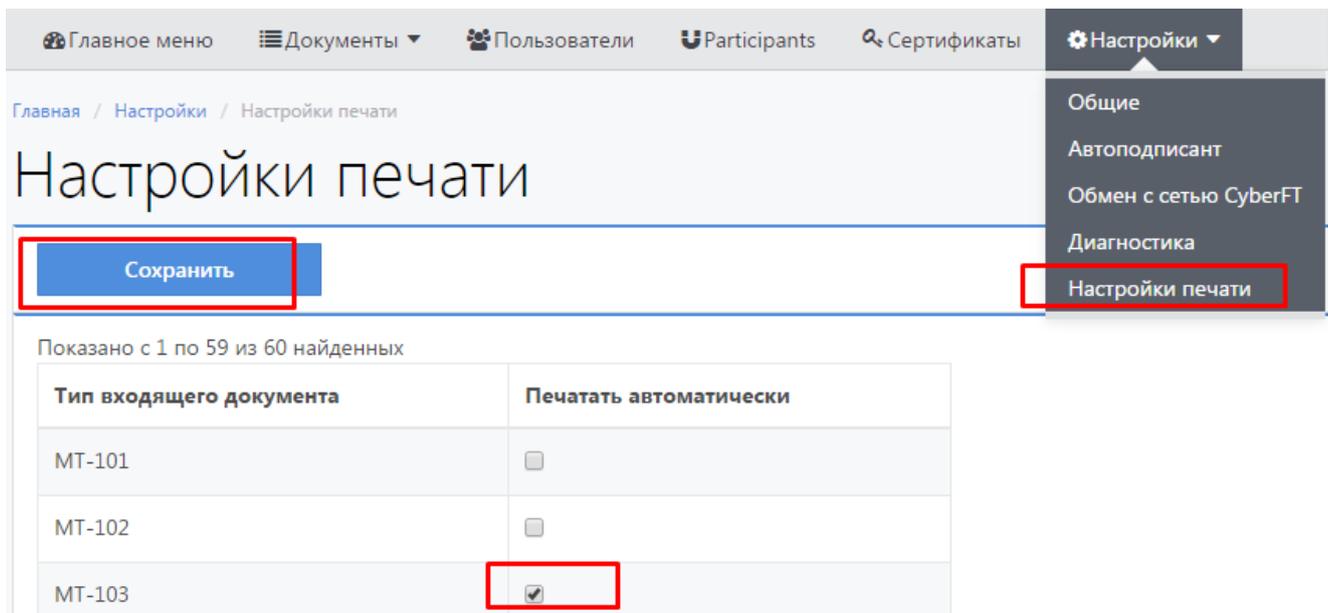


Рисунок 36. Активация экспорта документов на принтер.

9.3.6. Управление пользователями

Для создания учетной записи нового пользователя необходимо зайти в меню Пользователи и нажать кнопку «Создать».

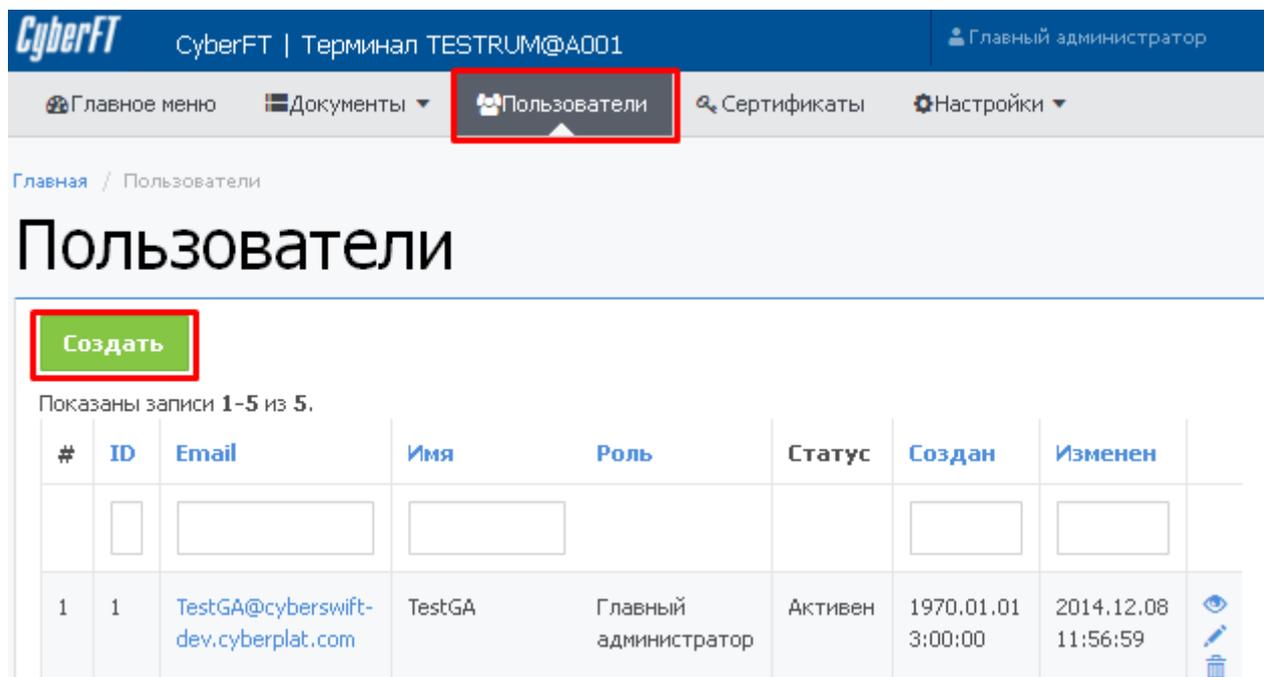


Рисунок 37. Создание нового пользователя.

Указываем Email, Имя, Роль и Статус нового пользователя и нажимаем «Создать».

Главное меню | Документы | Пользователи | Участники

Главная / Пользователи / Создать

Создать

Email

Имя

Роль

Уровень подписания

Статус

Создать

Рисунок 38. Данные нового пользователя.

Пароль нового пользователя выводится на экран, изменить его в дальнейшем может тоже только ГА. Для внесения изменений в данные пользователя нажмите кнопку **«Изменить»**, для изменения пароля при этом дополнительно поставьте флажок **«Сбросить пароль»**.

CyberFT | Терминал TESTRUM@A001 Главный администратор

Главное меню | Документы | Пользователи | Сертификаты | Настройки

Главная / Пользователи / test2

test2

Создан новый пользователь с паролем "YJOB134orDR5"

Изменить
Удалить

ID	8
Email	test2@test.test
Имя	test2
Роль	Подписант
Статус	Активен
Создан	2014.12.15 17:59:39
Изменен	2014.12.15 17:59:39

Рисунок 39. Информация о новом пользователе и пароль пользователя.

Новый пользователь отображается в реестре пользователей. Для просмотра дополнительной информации по пользователю необходимо нажать в крайней правой колонке таблицы пользователей на значок «Просмотр», для редактирования данных пользователя на значок «Редактировать», для удаления на значок «Удалить».

Пользователи

Создать

Показаны записи 1-6 из 6.

#	ID	Email	Имя	Роль	Статус	Создан	Изменен	
1	1	TestGA@cyberswift-dev.cyberplat.com	TestGA	Главный администратор	Активен	1970.01.01 3:00:00	2014.12.08 11:56:59	  

Рисунок 40. Реестр пользователей. Просмотр данных пользователя.

При переходе в режим редактирования пользователя отобразится форма с доступными для редактирования полями: Email, Имя, Роль и Статус. Для изменения пароля поставьте флажок «Сбросить пароль».

The screenshot shows the user editing interface in CyberFT. The page title is "Редактировать пользователя: test@". The form contains the following fields:

- Email: test@test.test
- Имя: test@test.test
- Роль: Подписант (dropdown menu)
- Статус: Активен (dropdown menu)
- Сбросить пароль: (checkbox, highlighted with a red box)
- Редактировать: (blue button, highlighted with a red box)

Рисунок 41. Форма редактирования учетных данных пользователя.

Для применения внесенных изменений нажмите кнопку «Редактировать».

После сброса пароля новый пароль будет выведен на экран ГА (как и при заведении нового пользователя).

9.3.7. Настройки подписания документов

Все исходящие документы Терминала подписываются Автоподписантом. Дополнительно к этому может производиться подписание исходящих документов персональной электронной подписью Подписанта.

Для этого у Подписанта должен быть установлен Тонкий клиент CyberFT. Для установки Тонкого клиента необходимо скачать на ПК установочный exe-файл. Дистрибутивы и

руководство пользователя располагаются по адресу <http://download.cyberft.ru/>, в каталоге Client CyberFT.

Чтобы исходящие документы не отправлялись без персональных подписей, в интерфейсе администратора необходимо изменить дефолтные настройки следующих параметров подписания:

1. Настройка подписания

Здесь необходимо установить флажки к тем видам документов, которые требуют персональной подписи (по умолчанию флажки не установлены):

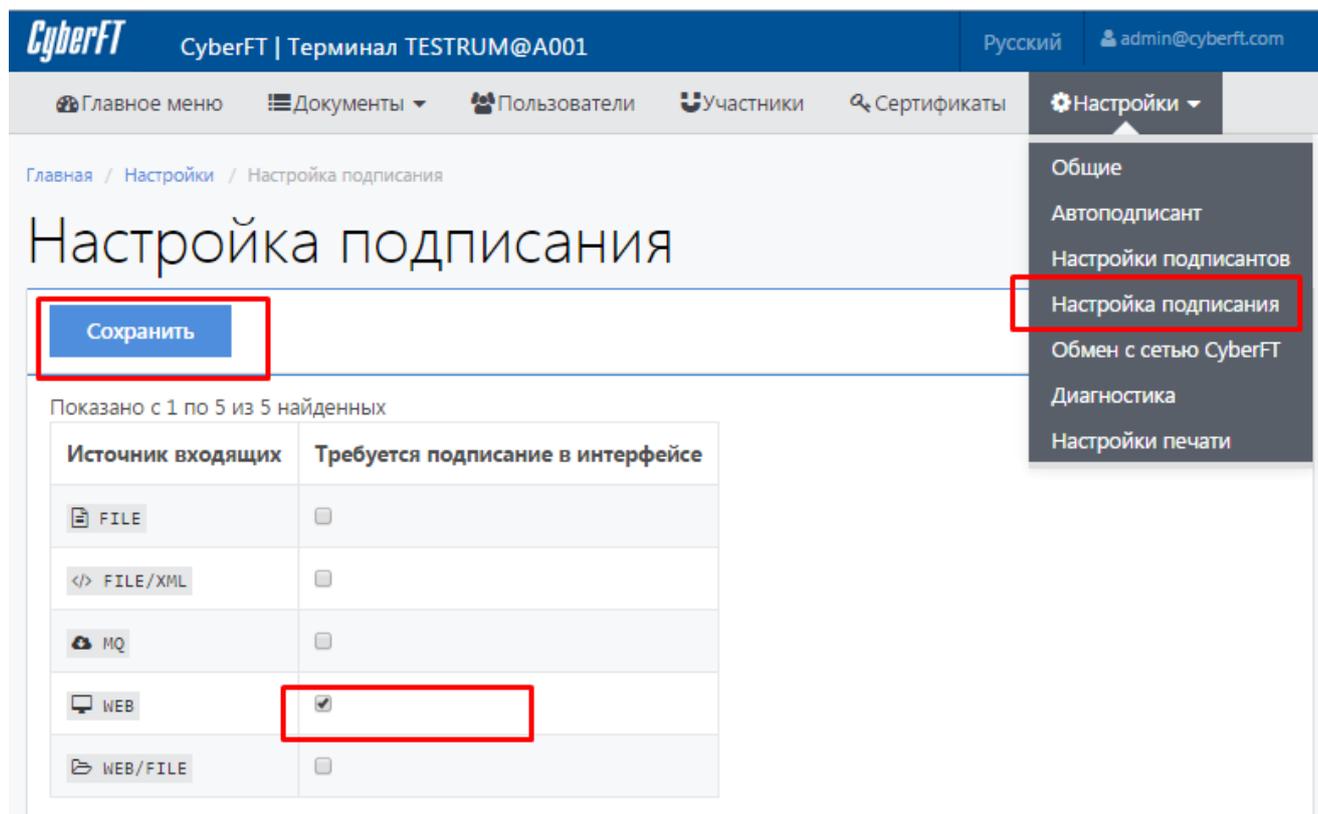


Рисунок 42. Настройки подписания.

2. Настройки подписантов

Здесь необходимо установить количество подписей, которые должны содержать исходящие документы, требующие персонального подписания (значение по умолчанию – «Не требуется, только Автобот»):

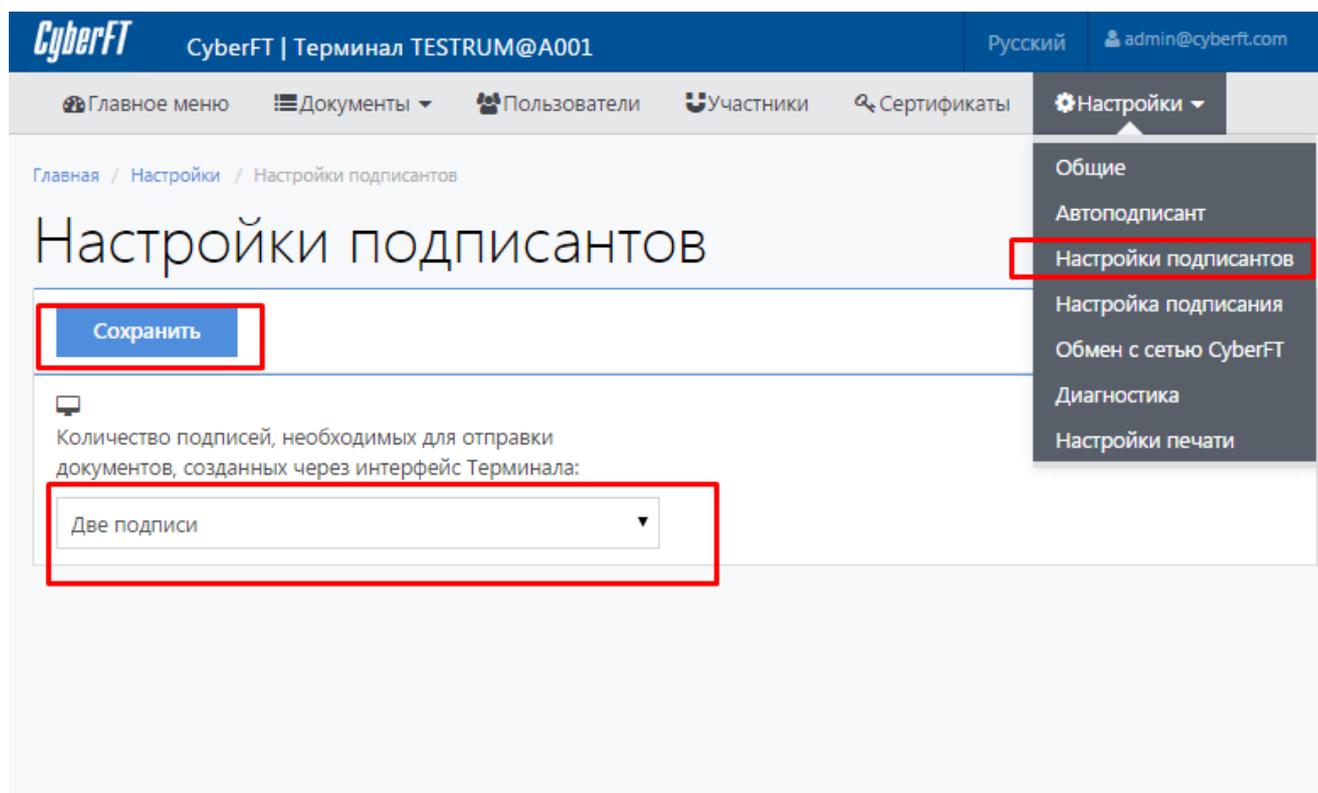


Рисунок 43. Настройки подписантов.

9.3.8. Журнал документов

Журналы документов доступны в меню «Документы». Для просмотра доступны отдельно разделы Журнала документов: Входящие, Исходящие и Ошибочные документы; а также общий Журнал документов, содержащий все перечисленные категории плюс служебные сообщения от сети CyberFT.

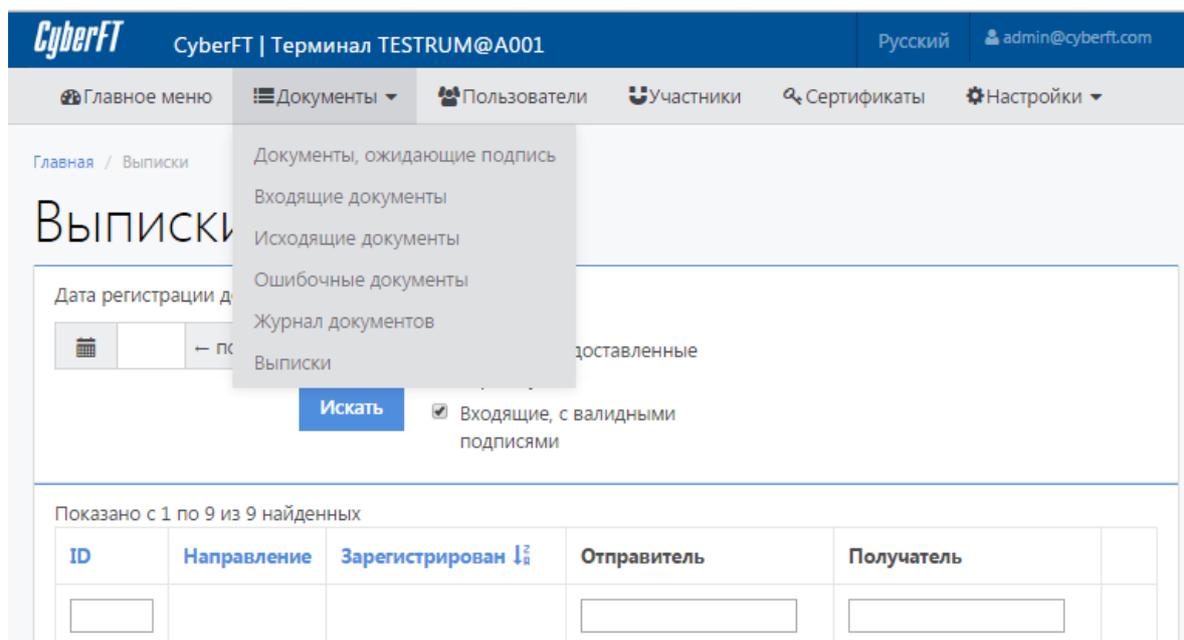


Рисунок 44. Документы.

Таблица документов (независимо от выбранного раздела журнала) содержит следующие столбцы:

Столбец	Значение
ID	локальный порядковый номер (идентификатор документа в БД MySQL Терминала);
Тип	тип документа
Подтип	подтип документа
Отправитель	адрес терминала отправителя
Получатель	адрес терминала получателя
UUID	глобальный идентификатор (уникальный идентификатор документа в системе CyberFT)
Идентификатор ABS	идентификатор документа в Автоматизированной Банковской Системе Участника
Статус документа	статус обработки документа системой CyberFT
Код ошибки	код ошибки системы при транспортировке документа
Дата регистрации	дата регистрации документа в системе CyberFT

The screenshot displays the 'Журнал документов' (Document Journal) interface. At the top, there are navigation tabs: 'Главное меню', 'Документы', 'Пользователи', and 'Настройки'. Below the title, there are search filters for 'Дата регистрации документа' and 'Отображать документы'. The search filters include checkboxes for 'Исходящие, не доставленные адресату', 'Исходящие, доставленные адресату', 'Входящие, с валидными подписями', 'Входящие, с невалидными подписями', and 'Показывать системные сообщения'. A blue 'Искать' button is present. Below the filters, it says 'Показано с 1 по 50 из 11168 найденных'. The table below has the following columns: '#', 'ID', 'Тип', 'Отправитель', 'Получатель', 'UUID', 'Идентификатор операции ABS', and 'Статус документа'. The first row contains the following data: '# 1', 'ID 65664', 'Тип swiR/103', 'Отправитель TESTRUM@A001', 'Получатель TESTRUM@A001', 'UUID 17EB38B2-7A39-11E4-BC22-03499FA81904', 'Идентификатор операции ABS +234123412341234', and 'Статус документа Сообщение отправлено, ожидаем подтверждения'.

Рисунок 45. Журнал документов.

В таблице документов предусмотрены следующие элементы управления:

- ▶ Упорядочение записей (столбцы с выделенным голубым шрифтом наименованием),
- ▶ Фильтрация записей по строке/подстроке (столбцы с полем текстового ввода),
- ▶ Фильтрация записей по диапазону дат,

В общем Журнале документов дополнительно доступна фильтрация записей по категории документа путем выставления нужных флагов.

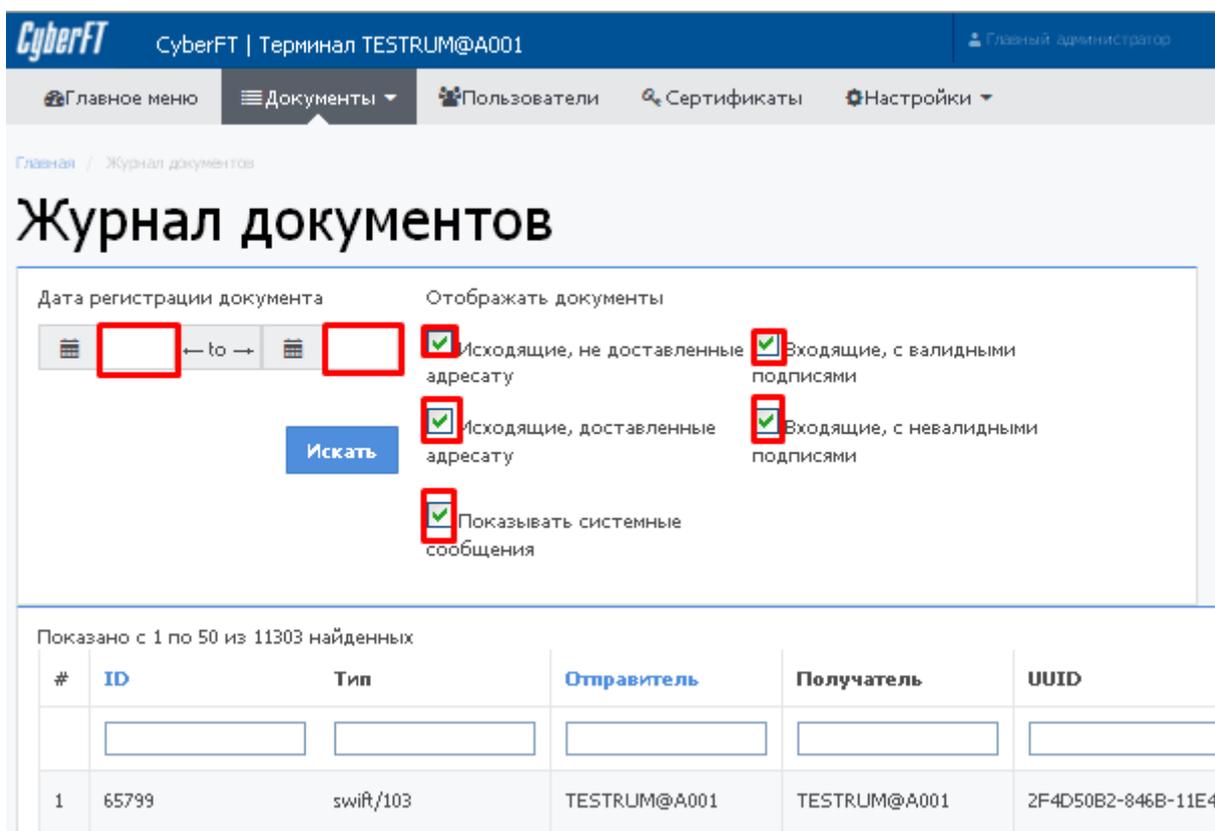


Рисунок 46. Фильтр документов.

9.3.9. Главное меню Терминала

В Главном меню также доступны для просмотра журналы документов, процессы, запущенные на сервере и график статусов документов.

10. МОДУЛЬ ДБО

Модуль ДБО – Дистанционное Банковское Обслуживание – предназначен для безопасного обмена сообщениями между Банком и его Клиентом. Терминал с ДБО модулем устанавливается на стороне Клиента. Модуль служит для создания и отправки в Банк документов с ЭП Клиента (платежные поручения и пр.), а также для отображения входящих сообщений и выписок из Банка. Модуль поддерживает импорт из 1С /экспорт в 1С.

10.1. Настройка ДБО ролей

В системе CyberFT предусмотрены две роли для работы в ДБО-модуле: **Оператор ДБО** и **Проверяющий ДБО**. Роли настраиваются Главным Администратором в карточке пользователя при создании/редактировании его учетной записи (см. раздел 9.3.6 Управление пользователями), в соответствующем поле:

The screenshot shows a web interface for creating a user. At the top, there are navigation links: 'Главное меню', 'Документы', 'Пользователи', and 'Участники'. Below that is a breadcrumb trail: 'Главная / Пользователи / Создать'. The main heading is 'Создать'. The form contains the following fields:

- Email:** A text input field containing 'test@test.test'.
- Имя:** A text input field containing 'testUser'.
- Роль:** A dropdown menu with the following options: 'Подписант' (selected), 'Подписант', 'Главный администратор', 'Оператор ДБО', and 'Проверяющий ДБО'. The last two options are enclosed in a red rectangular box.
- Статус:** A dropdown menu with the option 'Активен'.

At the bottom of the form is a green button labeled 'Создать'.

Рисунок 48. Выбор роли в Карточке создания Пользователя.

Интерфейс ДБО доступен по общему IP адресу Терминала пользователям с ДБО-ролями. В зависимости от роли, в интерфейсе ДБО доступны следующие действия:

Действия	Оператор	Проверяющий
Создание ДБО-документов	+	-
Подписание и Отправка ДБО-документов	+	-
Просмотр документов, выписок и журналов, относящихся к ДБО	+	+
Ведение Справочника контрагентов и других справочников	+	+

Указанные действия в интерфейсе описаны в документе «Терминал сети CyberFT: Руководство пользователя».

10.2. Доступ к ДБО-модюлю для Главного Администратора

Действия, соответствующие роли Проверяющего, доступны также Главному Администратору Терминала. А именно:

- Просмотр документов/выписок/журналов (через общие Журналы документов и выписок);
- Ведение справочников: Контрагентов/Назначений платежа/Банков.

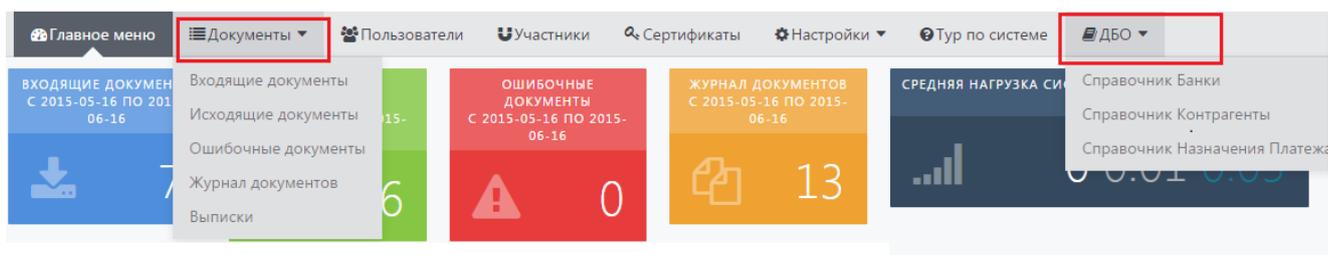


Рисунок 49. Действия с ДБО, доступные Главному Администратору.

10.3. ДБО-Справочники

Для автоматизации создания документов в ДБО-модуле предусмотрены следующие справочники:

Справочник	Автомат заполнения, где применяется Справочник	Источники данных
Справочник Банки	разделы «Плательщик» и	Автоматическая загрузка с

	«Получатель»	сайта ЦБР
Справочник Контрагенты	разделы «Банк Плательщика» и «Банк Получателя»	Ручное заведение и автоматический парсинг из платежных документов
Справочник Назначения Платежа	поле «Назначение платежа»	Ручное заведение и автоматический парсинг из платежных документов

Далее данный перечень Справочников ДБО рассмотрен подробно.

10.3.1. Справочник Банки

Порядок Заполнения/Обновления Справочника Банков Пользователем:

1. Скачать с сайта ЦБР актуальный архив справочника (файл вида bik_db_17062015.zip по ссылке <http://www.cbr.ru/mcirabis/?PrId=bic>),
2. Выбрать через Обзор скачанный архив, и нажать кнопку «Загрузить».

Редактировать в данном Справочнике пользователю доступно только адрес Терминала, ассоциированный с записью данного Справочника:

Главное меню | Документы | ДБО

Главная / Справочник Банки

Справочник Банки

Выберите файл для загрузки Обзор Загрузить

Показаны записи 1-20 из 2991.

#	БИК	Корреспондентский счет	Имя	Город	Terminal ID
1	040001002		ПУ БАНКА РОССИИ N 43192		SABRRUMMXXXX
2	040002002		ПУ БАНКА РОССИИ N 43197		(не задано)
3	040004002		ПУ БАНКА РОССИИ N 67903		(не задано)

Рисунок 50. Справочник Банки.

10.3.2. Справочник Контрагенты

Пополнение Справочника Контрагенты может осуществляться как пользователем Терминала, так и в автоматическом режиме, путем парсинга платежных документов.

Для создания нового профиля Плательщика или Получателя нужно пройти в Справочник (ДБО->Справочник Контрагенты), и нажать кнопку «Создать»:

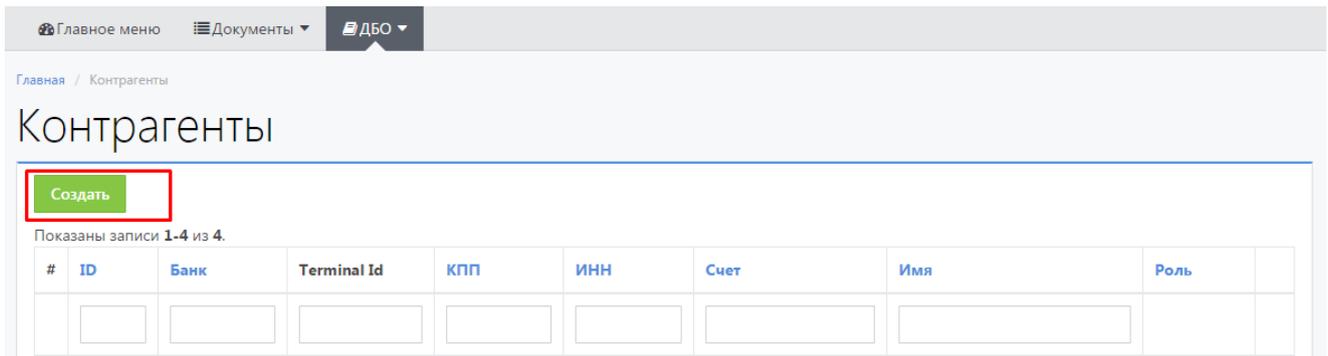


Рисунок 51. Создание Контрагента из Справочника.

Откроется форма создания Контрагента:

Главная / Контрагенты / Создать

Создать

Роль

Банк

Terminal Id

КПП

ИНН

Счет

Валюта

Имя

Создать Cancel

Рисунок 52. Форма создания Контрагента.

10.3.3. Справочник Назначения платежа

Пополнение Справочника Назначения платежа может осуществляться как пользователем Терминала, так и в автоматическом режиме, путем парсинга платежных документов.

Для создания нового шаблона Назначения платежа нужно пройти в Справочник (ДБО->Справочник Назначения платежа), и нажать кнопку «Создать»:

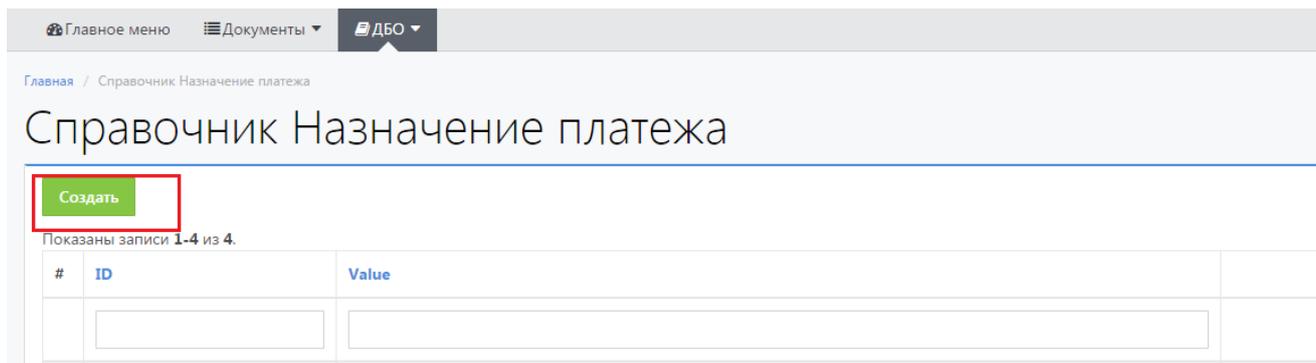


Рисунок 53. Создание Назначения платежа из Справочника.

Откроется форма создания Назначения платежа:

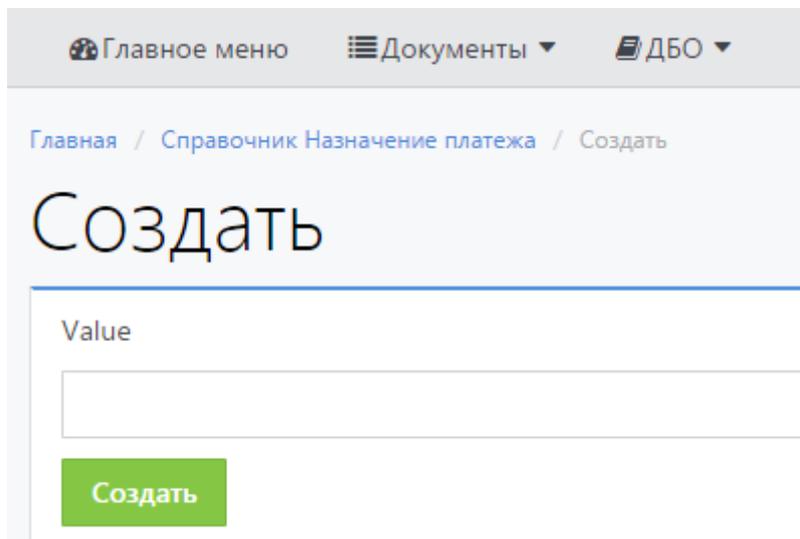


Рисунок 54. Форма создания Назначения платежа.

11. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

11.1. Файловый обмен FileAct

В системе CyberFT реализована возможность обмена файлами, т.н. FileAct. Ниже описан его регламент.

11.1.1. Порядок файлового обмена FileAct

1. Отправитель должен передать в установленные каталоги комплект их 2х файлов:

Файл	Путь
отправляемый файл (т.н. bin, бинарник, архив)	<code>/var/www/cyberswift/import/fileact/bin</code>
xml-инструкция (т.н. PDU), содержащая: адреса участников, имя отправляемого файла и другие сведения	<code>/var/www/cyberswift/import/fileact/xml</code>

2. Терминал изменяет имя файла и содержимое PDU, добавляя временные метки, идентификаторы, и другие сведения. После чего передает измененный комплект в Сеть CyberFT.
Подробнее правила изменения Терминалом файла и PDU описаны в следующем разделе.
3. Комплект PDU+файл доставляется сетью на терминал получателя, и автоматически экспортируется терминалом в следующие каталоги:
`/var/www/cyberswift/export/fileact/xml`
`/var/www/cyberswift/export/fileact/bin`
4. Одновременно с экспортом на терминале получателя формируется квитанция (т.н. ask, prt) и передается на терминал отправителя, где экспортируется в папку:
`/var/www/cyberswift/export/fileact/receipt`

11.1.2. Правила формирования документов Терминалом

1. В квитанцию в качестве идентификаторов записываются 2 уникальных идентификатора (UID): идентификаторы документа у отправителя (SWIFT Request Reference) и у получателя (Message Output Reference). Идентификатор UID доступен в интерфейсе терминала (в карточке file-act документа и в поиске по журналу).
2. При регистрации комплекта pdu+файл на терминале отправителя изменяется имя бинарника, и оно прописывается в содержимое тэга Body в out-файле. Старое

имя файла переносится из Body в FileLogicalName.

Формат именования файлов: [имя бинарника in][значение <Saa:TransferRef>].out

Пример:

было в in-pdu:

```
<Saa:Body>AFT_FA.JPG</Saa:Body>
```

стало в out-pdu:

```
<Saa:FileLogicalName>AFT_FA.JPG</Saa:FileLogicalName>
```

```
... <Saa:Body>AFT_FA.JPG.SNL02013D11330603738010042C.out</Saa:Body>
```

3. Также в out-pdu Терминалом отправителя записываются временные метки и идентификаторы документа, формируемые по следующим правилам:

Тэг	Значение	Комментарий
<Saa:FileLogicalName>	входящее значение имени файла	Источник поля - входящий xml-файл либо (в случае отсутствия этого тэга в in) - исходное значение body там же. Ограничение на длину - не более 254 символов.
<Saa:NetworkInfo>\<Saa:Priority>	"Normal"	Во входящем файле опционально, добавляется сетью в out и ask
<Saa:NetworkInfo>\<Saa:SWIFTNetNetworkInfo>\<Saa:SNLRef>	SNLid-YYYY-MM-DDTHH:MM:SS.procid.digitsZ	Присваивается сетью, добавляется в out-pdu. Должен быть уникальным по всей базе.
<Saa:NetworkInfo>\<Saa:SWIFTNetNetworkInfo>\<Saa:TransferRef>	SNL[SNLid]D1[timestamp]010042C	Присваивается сетью, добавляется в out. Должен быть уникальным по всей базе. timestamp соответствует времени регистрации файла на Терминале отправителя.
<Saa:NetworkInfo>\<Saa:SWIFTNetNetworkInfo>\<Saa:FileStartTime>	YYYYMMDDHHMMSS	Время начала отправки. Используется в out файле.
<Saa:NetworkInfo>\<Saa:SWIFTNetNetworkInfo>\<Saa:FileEndTime>	YYYYMMDDHHMMSS	Время окончания передачи файла. Используется в out и ask файлах. Заполняется по окончании экспорта у получателя.

11.2. Статусы документов в CyberFT

В системе CyberFT предусмотрены следующие статусы документов (отображаются в поле «Статус документа» Журнала документов):

Исходящие документы

ID	Описание статуса
0	Документ не готов к отправке (новый статус)
1	Новое сообщение в очереди исходящих, готово к отправке
2	Сообщение отправлено, ожидаем подтверждения
3	Сообщение получено процессингом
4	Сообщение отвергнуто процессингом (возвращено), дополнительно указывается код ошибки;
7	Сообщение получено получателем.

Входящие документы

ID	Описание статуса
5	Новое сообщение в очереди входящих
6	Сообщение выгружено из очереди входящих
8	Сообщение подписано доверенными подписями
9	Сообщение содержит хотя бы одну не валидную подпись

11.3. Описание ошибок

В Терминале CyberFT обрабатываются следующие ошибки:

- ▶ 501 – Ошибка доступа к БД терминала;
- ▶ 502 – Документ не найден в рабочей папке терминала;
- ▶ 503 – Системная ошибка при работе с файлом документа;
- ▶ 504 – Отсутствует секретный ключ автоподписанта;
- ▶ 505 – Отсутствует сертификат процессинга;
- ▶ 506 – Ошибка связи с процессингом;

- ▶ 507 – Не валидна подпись отправителя;
- ▶ 508 – Не валидна подпись процессинга;
- ▶ 509 – Не найден сертификат отправителя;
- ▶ 510 – Ошибка доступа к папке «Out»;
- ▶ 511 – Ошибка доступа к рабочим папкам терминала;
- ▶ 512 – Неверный пароль активации ключа Автоподписанта;
- ▶ 513 – Ошибка крипто библиотеки;
- ▶ 514 – Ошибка создания конверта с документом и подписью;
- ▶ 515 – API процессинга вернуло ошибку;
- ▶ 516 – Формат ответа процессинга не верный;
- ▶ 517 – Вышло время запроса (таймаут) к процессингу;
- ▶ 518 – Не найден секретный ключ Пользователя;

12. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

12.1. Введение

При использовании Терминала необходимо учитывать угрозы, источником которых являются следующие лица:

- ▶ злоумышленники, которые могут выполнить преднамеренное заражение компьютера, на котором установлен Терминал, или компьютеров, с которых к Терминалу подключаются пользователи, через уязвимости системного и прикладного ПО (операционной системы, Web-браузера, почтового клиента и пр.) с последующим дистанционным хищением ключей ЭП и паролей, либо непосредственно получить удаленный доступ к системе штатными средствами путем подбора/кражи пароля и т.п.;
- ▶ лица, случайно или целенаправленно получившие доступ к ключам ЭП, в том числе сотрудники организации и ИТ-сотрудники, имеющие либо имевшие доступ к носителям с ключами ЭП (дискетам, флэш-картам, жестким дискам и пр.), а также доступ к компьютерам, на которых использовались средства ЭП;
- ▶ нештатные (приходящие по вызову) ИТ-специалисты, выполняющие профилактику и подключение компьютеров к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютеры, где использовались средства ЭП.

Основные последствия реализации таких угроз состоят в:

- ▶ возможности подписать любой документ от имени организации-владельца ЭП;
- ▶ возможности подменить любой документ владельца ЭП.

12.2. Общие рекомендации по обеспечению безопасности

Сеть CyberFT не осуществляет хранение ключей электронных подписей пользователей Сети и не может от имени ее пользователей сформировать корректную ЭП под каким-либо документом. Вся ответственность за конфиденциальность ключей ЭП полностью лежит на пользователе Сети, как единственном владельце ключей ЭП.

Администрация не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭП, пароли, а также прочую конфиденциальную информацию. Также не рассылаются по электронной почте какие-либо программы для установки на компьютеры пользователей Системы. Все программы должны быть скачаны с официального сайта Сети <http://cyberft.ru/>.

Необходимо строго соблюдать правила информационной безопасности, правила хранения и использования ключей ЭП. Необходимо строго ограничить доступ к персональным компьютерам или серверам, на которых установлено ПО Терминала, и с которых осуществляется работа со средствами ЭП.

Чтобы воспрепятствовать хищению и использованию ключа ЭП злоумышленниками, требуется придерживаться приведенных ниже базовых правил и рекомендаций:

- ▶ рекомендации по размещению и защите терминала CyberFT (см. раздел 12.3 данного Руководства);
- ▶ общие требования к персональному компьютеру, используемому для работы со средствами электронной подписи (см. раздел 12.4 данного Руководства);
- ▶ не передавать персональный ключевой носитель третьим лицам, не оставлять его без присмотра, не хранить его в доступном месте, не оставлять его дольше необходимого времени подключенным к компьютеру;
- ▶ использовать для хранения персонального ключевого носителя сейф или иное хранилище, обеспечивающее его надлежащую сохранность;
- ▶ хранение персонального ключа ЭП допускается только на съемном носителе (токене, дискете, флэш-карте и т.д.). Рекомендуется использовать для хранения персонального ключа ЭП именно токены, так как доступ к ключу ЭП будет предоставляться только после ввода пользователем PIN-кода;
- ▶ не выписывать пароли, PIN-коды и прочие данные, используемые для аутентификации в операционной системе, токенах или компонентах системы электронного документооборота, на бумагу или в файлы;
- ▶ следить за тем, чтобы на электронном носителе (дискете, флэш-карте) ключей ЭП не находилась любая иная информация;
- ▶ никогда не совмещать подключение ключевого носителя и работу с любыми ресурсами в сети Интернет, а также программами ICQ, Skype и т.п.

Если возникают сомнения в конфиденциальности используемых ключей ЭП, или возникло подозрение на их компрометацию (незаконное копирование), необходимо

немедленно заявить Администрации о необходимости аннулировать сертификат проверки ЭП (см. раздел 12.5 данного Руководства), а также выполнить необходимые действия по блокировке сертификата (см. раздел 9.3.1 данного Руководства).

12.3. Рекомендации по размещению и защите терминала CyberFT

Существуют различные варианты размещения Терминала в локальной вычислительной сети (ЛВС) организации, зависящие от размера сети, ее распределенности и схемы построения, используемого телекоммуникационного оборудования, количества и месторасположения пользователей Терминала и т.д.

Один из вариантов размещения Терминала и организации его взаимодействия с другими ресурсами показан на следующем рисунке:

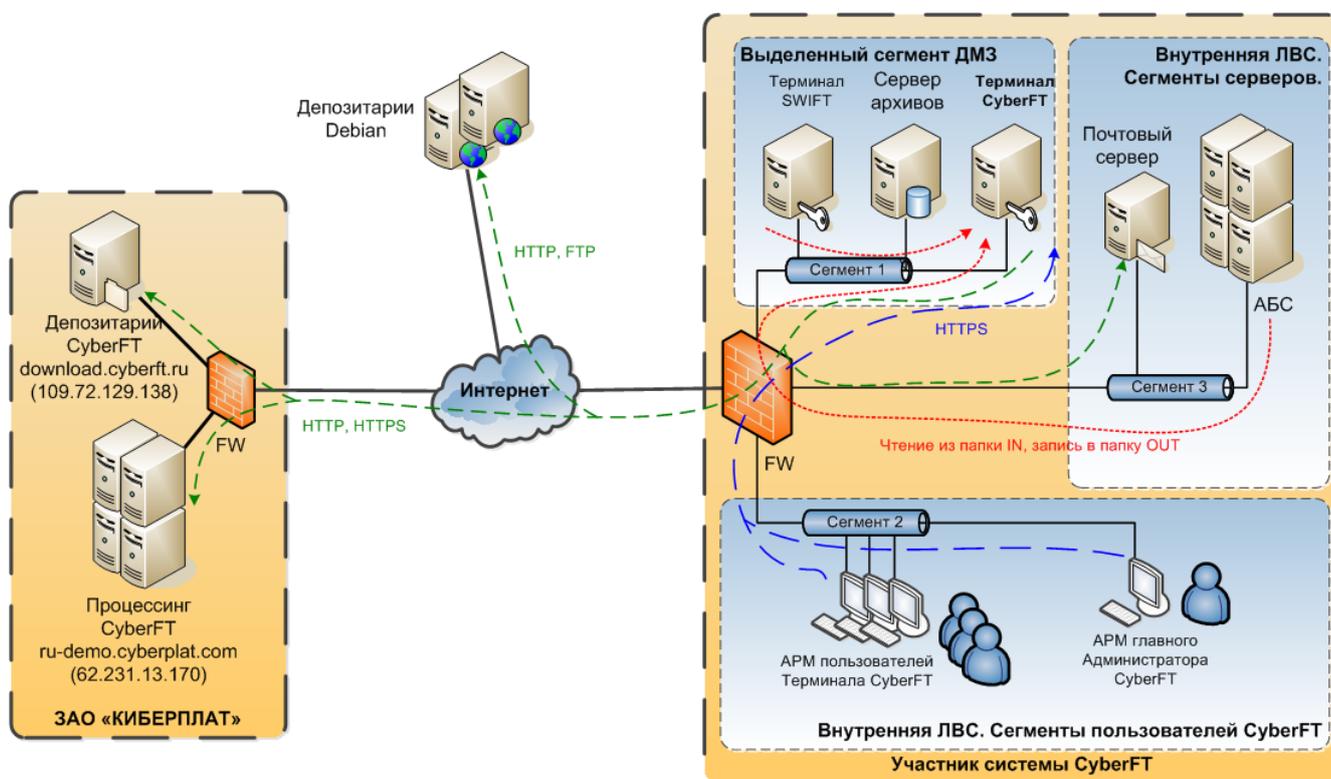


Рисунок 55. Вариант размещения Терминала CyberFT и организации его взаимодействия с другими внешними и внутренними ресурсами Участника системы

Чтобы воспрепятствовать хищению и использованию ключа ЭП злоумышленниками, несанкционированному доступу к системе, обеспечить ее доступность и отказоустойчивость требуется придерживаться приведенных ниже базовых правил и рекомендаций:

- ▶ выделить для установки Терминала и работы с ключевыми носителями отдельный сервер (физический или виртуальный), не использовать данный компьютер для других целей;
- ▶ обеспечить физические (запираемое помещение с ограниченным доступом; наличие систем кондиционирования, пожаротушения, бесперебойного энергоснабжения, контроля и управления доступом, видеонаблюдения и т.п.) и организационные меры безопасности (назначение ответственных лиц; подготовка организационно-распорядительных документов; организация учета используемых СКЗИ и ключевых носителей; разработка плана обеспечения непрерывности и восстановления работоспособности Терминала);
- ▶ расположить сервер с Терминалом в выделенном сегменте демилитаризованной зоны (ДМЗ) ЛВС;
- ▶ прописать настройки расположения каталогов import и export вне сервера Терминала, для минимизации доступа к серверу;
- ▶ на используемом сетевом оборудовании (межсетевом экране) запретить к серверу любой доступ из сети Интернет, а также доступ с сервера к ресурсам сети Интернет, за исключением следующих ресурсов:
 - tcp://service.cyberft.ru (TCP/443, 80);
 - download.cyberplat.ru (109.72.129.138, TCP/443, 80)
 - используемые репозитории ОС Debian (HTTP, FTP).
- ▶ ограничить доступ к серверу на используемом сетевом оборудовании (межсетевом экране) минимально необходимым перечнем взаимодействующих с ним внутренних серверов и рабочих станций (АБС, почтовый сервер, АРМ Главного администратора и пользователей Терминала), расположенных в других сегментах, в том числе, запретить удаленный доступ со стороны системных администраторов (типовые направления и протоколы взаимодействия Терминала с другими элементами системы отображены на Рисунке «Вариант размещения Терминала CyberFT и организации его взаимодействия с другими внешними и внутренними ресурсами Участника системы»);
- ▶ если в выделенном сегменте сети кроме Терминала будет располагаться другое оборудование, целесообразно на программном межсетевом экране, установленном на сервере, запретить взаимодействие с другими серверами сегмента, кроме минимально необходимого доступа, например, с терминала SWIFT (см. Рисунок «Вариант размещения Терминала CyberFT и организации его взаимодействия с другими внешними и внутренними ресурсами Участника системы»);
- ▶ на сервере Терминала:
 - в BIOS установить пароль на изменение, отключить загрузку с внешних носителей;
 - использовать файловую систему Ext4 с включенным журналированием;

- выделить под каталоги /home, /tmp, /var, /boot, /log отдельные разделы; задать квоты использования свободного пространства на диске; каталог /log сделать недоступным для чтения пользователям;
- установить пароль на загрузку (LILO или GRAB), запретить загрузку в режиме BusyBox;
- запретить использование клавиши SysRq;
- в разделах /tmp, /log запретить запуск исполняемых файлов (noexec);
- отключить и деинсталлировать неиспользуемые программные пакеты и демоны (список используемого ПО приведен в разделе 6.2.1 данного Руководства);
- при использовании функционала оповещения администраторов по внутренней электронной почте о различных критичных событиях на Терминале, разрешить отправку сообщений только на необходимые внутренние адреса;
- своевременно обновлять операционную систему, проводить установку патчей, критичных обновлений; для установки/обновления операционной системы и ПО использовать доверенные репозитории;
- не использовать права администратора при отсутствии необходимости; в повседневной практике входить в систему как пользователь, не имеющий прав администратора (при необходимости повышенных привилегий использовать sudo);
- в /etc/security/access.conf запретить удалённый доступ (как минимум, при невозможности отказаться от удаленного доступа, запретить удаленный доступ с правами root);
- включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ. Периодически, как минимум раз в неделю, просматривать журнал аудита и должным образом реагировать на обнаруженные сообщения об ошибках;
- запретить использование незащищенных протоколов (Telnet, FTP);
- для каждого пользователя и АС, получающих доступ к Терминалу, использовать персональные учетные записи (логин/пароль);
- длина пароля должна быть не менее 8 символов, и он должен быть сложным (использовать цифры, буквы разных регистров и специальные символы; не являться последовательностью символов на клавиатуре или словарным выражением);
- установить время жизни пароля не более 3 месяцев (/etc/login.defs) и для исключения возможности автоматического подбора пароля задержку повторного ввода 30 сек. (/etc/pam.d/login);
- ограничить права доступа к файловой системе и сервисам для разных ролей пользователей минимально необходимыми правами; установить

параметр DIR_MODE в конфигурационном файле /etc/adduser.conf в значение 0750;

- отключить возможность запуска программ с монтируемых отчуждаемых устройств;
- ▶ принять меры по обеспечению сохранности и защиты от несанкционированного доступа закрытого ключа ЭП автоматического подписанта, используемого на Терминале, не сохранять пароль доступа к нему в конфигурационных файлах;
- ▶ не выписывать пароли, PIN-коды и прочие данные, используемые для аутентификации в операционной системе или компонентах системы на бумагу или в файлы.

12.4. Общие требования к персональному компьютеру, используемому для работы со средствами электронной подписи

Персональный компьютер, используемый для работы со средствами ЭП, должен удовлетворять (не ограничиваясь) следующим требованиям:

- ▶ должно быть установлено только лицензионное программное обеспечение (операционная система, служебные и прикладные пакеты и т.д.);
- ▶ должен быть установлен и своевременно обновляться антивирус;
- ▶ пароли учетных записей пользователей должны быть сложными (не менее 8 символов, включая буквы, цифры и спецсимволы) и меняться не реже одного раза в три месяца;
- ▶ не должно быть учетных записей с пустыми паролями;
- ▶ должны быть установлены все обновления к установленной операционной системе и используемым пакетам ПО;
- ▶ необходимо запретить или существенно ограничить до минимально необходимого использование любых средств удалённого доступа (обычно используется IT-специалистами для удалённой поддержки);
- ▶ при монтировании отчуждаемых носителей запретить запуск исполняемых файлов и настроить автоматический запуск их проверки на вирусы;
- ▶ физический доступ к компьютеру должен быть ограничен перечнем допущенных лиц и т.д.

12.5. Действия при нештатных ситуациях

К нештатным ситуациям при работе со средствами ЭП и ключами ЭП относятся:

- ▶ установлены факты хищения или копирования ключей ЭП, или произошла утрата ключевого носителя;
- ▶ произошла утрата ключевых носителей, с их последующим обнаружением;

- ▶ возникло подозрение или произошло нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;
- ▶ произошло нарушение целостности хранилища (сейфа, металлического шкафа, или иного хранилища) с ключевыми носителями;
- ▶ случаи, когда на персональном компьютере, где использовались средства ЭП, были обнаружены компьютерные вирусы, закладки, иные средства скрытного информационного воздействия, или иные средства негласного съема информации;
- ▶ прочие подозрения или установленные факты компрометации ключа ЭП, при которых данные ключа ЭП стали известны третьим лицам (или неустановленному кругу лиц).

При возникновении нештатной ситуации при работе со средствами ЭП и ключами ЭП необходимо уведомить Администрацию наиболее быстрым способом: через интерфейс Терминала CyberFT, по электронной почте, по факсимильной связи или иным образом по реквизитам, указанным на информационном сервере <http://cyberft.ru/>.