**Описание программного комплекса Оператора фискальных данных (ПК ОФД)**

Настоящий документ содержит описание функциональных характеристик программного комплекса оператора фискальных данных (ПК ОФД), далее именуемого «Система», условия его установки, настройки и эксплуатации.

# Список сокращений

|  |  |  |
| --- | --- | --- |
| БД | – | База данных |
| БП | – | Бизнес-процесс |
| ДМЗ | – | Демилитаризированная зона | |
| ИР ККТ | – | Информационный ресурс контрольно-кассовой техники 2 ФНС России. | |
| ЗСХД | – | Защищенная система хранения данных. | |
| МЭ | – | Межсетевой экран | |
| ПК ОФД | – | Программный комплекс Оператора фискальных данных | |
| ПМ | – | Программный модуль | |
| ПО | – | Программное обеспечение | |
| ФНС | – | Федеральная налоговая служба Российской Федерации | |
| ЦОД | – | Центр обработки данных | |

# Общие положения

## Наименование проектируемой системы

Полное наименование: Программный комплекс оператора фискальных данных для обработки ФД.

Условное обозначение: ПК ОФД.

В настоящем документе используется сокращение «Система».

## Цели, назначение и области использования системы

Система предназначена для выполнения требований законодательства РФ к техническим средствам оператора фискальных данных.

Целью создания системы является:

* Предоставление пользователю сервисов и услуг по передаче данных в налоговые органы.
* Осуществление обработки фискальных данных согласно законодательству РФ:
  + Получение фискальных данных;
  + Проверка достоверности фискальных данных;
  + Запись, систематизация и накопление фискальных данных в хранилище и их хранение в некорректируемом виде;
  + Извлечение фискальных данных из хранилища;
  + Использование фискальных данных;
  + Передача фискальных данных в налоговые органы;
  + Предоставление доступа налоговым органам к фискальным данным, исключая модификацию (корректировку);
  + Обезличивание, блокирование, удаление и уничтожение фискальных данных и информации о расчетах.
* Предоставление покупателям сервисов, обеспечивающих прозрачность торговых сделок с использованием ККТ.

# Функциональные характеристики ПК ОФД

Функционально Система может быть представлена как совокупность трех основных подсистем:

1. Подсистема приема данных – предназначена для идентификации ККТ, приема данных от нее, и помещения их в ЗСХД. Подсистема включает в себя межсетевой экран, взаимодействующий с удаленными ККТ, балансировщик трафика, межсетевой экран ДМЗ, ККМ Сервер, Криптосервер и ПМ быстрой фиксации данных (очередь).
2. Подсистема хранения данных – включает в себя ПМ предварительной обработки данных, хранилище фискальных данных, хранилище агрегатов, хранилище персональных данных, ПМ доступа к данным (Facade) и ФНС API для передачи данных в ФНС по протоколу обмена.
3. Подсистема сервисов – включает в себя WEB-интерфейсы пользователей (НП, покупателя и администратора), компоненты управления бизнес-процессами (БП) с репозиторием БП, компоненты интеграции (сервис e-mail рассылки, СМС, интеграции с СЭР и компонент криптозащиты), компоненты работы с данными (отчеты и выгрузки), компоненты администрирования и конфигурирования системы, API для работы с мобильными устройствами.

## Функции подсистемы приема данных

Подсистема приема данных обеспечивает прием, проверку и квитирование фискальных документов.

Кассовый чек поступает от устройств ККТ в запакованном виде по протоколу TLV на вход Системы ОФД и обрабатывается Межсетевым экраном (МЭ). Межсетевой экран предназначен для защиты Системы от «лишнего» трафика и внешних атак.

Отфильтрованная информация по протоколу TLV передается на Балансировщик трафика и после обработки поступает на Межсетевой экран ДМЗ. При этом формат сообщений не проверяется.

Межсетевой экран ДМЗ выполняет функцию защиты внутренней сети ОФД от внешних угроз. Прошедшие через него сообщения передаются в формате TLV на ККТ-Сервер. ККТ-Сервер производит «вскрытие» транспортного контейнера и передает его в ПКЗ (HSM).

ПКЗ (HSM) осуществляет расшифровку пакета с последующим возвращением расшифрованного чека в ККТ-Сервер.

ККТ-Сервер осуществляет проверку, обработку и размещение расшифрованной информации в очередь (Journal) на занесение в БД. Также ККТ-Сервер формирует квитанцию и отправляет ее в ПКЗ (HSM) для подписания и шифрования.

Зашифрованная и подписанная квитанция отправляется назад через МЭ на ККТ.

## Функции подсистемы хранения данных

Подсистема хранения данных обрабатывает чеки и помещает данные в ЗСХД.

Программный модуль первичной обработки данных ETL (Spark) извлекает фискальные документы в формате TLV из ККТ-Сервера, классифицирует и агрегирует их данные, сохраняет в БД полученную информацию (агрегированную информацию в OLAP и исходный документ в ЗСХД).

Данные в БД хранятся в форматах Trift и Avro, сама БД развернута на распределенной структуре под управлением Hbase.

Данные подготавливаются и извлекаются для выгрузки в ИР ККТ-3 в два этапа: сначала первичная выгрузка фискальных данных, а после агрегирования осуществляется выгрузка агрегатов.

## Функции подсистемы сервисов

Подсистема сервисов обеспечивает взаимодействие Системы с пользователями через пользовательские интерфейсы (GUI).

Пользователи обращаются к Системе через пользовательские интерфейсы своих ПК посредством сети Интернет. Запросы с браузеров пользователей в формате HTTPS.

События, инициированные пользователями в интерфейсах, передаются в компонент управления бизнес-процессами Activity в виде сигналов или сообщений.

Компонент Activity, получив сигнал или сообщение, вызывает необходимый бизнес-процесс из репозитория и запускает его экземпляр посредством BPSS, при этом все постоянные данные (константы) процесса загружаются из хранилища данных (через Faсade), а переменные процесса сохраняются в Activity DB. Данные запущенного процесса хранятся до полного его завершения.

Для выполнения регламентов запущенных бизнес-процессов компонент BPSS может вызывать компоненты сервиса интеграции (e-mail рассылка, СМС-рассылка, взаимодействие с СЭР, функции работы с КЭП Cripto), а также сервисы Long task (отчеты и выгрузки данных).

Мобильные устройства интегрируются и получают доступ к своим данным посредством Мобильного API.

# Информации по установке и эксплуатации ПК ОФД

## Требования к серверам

Компоненты Системы устанавливаются на выделенных серверах, предназначенных исключительно для эксплуатации серверных компонентов Системы.

Для эксплуатации Системы необходимо минимум 6 серверов приложений PowerEdge R430 и 4 сервера хранения PowerEdge R730.

Сервера приложений должны иметь следующие характеристики:

* Контроллеры RAID (Внутренние: PERC S130, PERC H330, PERC H730, PERC H730P; Внешние: PERC H830);
* Диски: 4 x 800G SSD, 4 x 2TB HDD;
* Процессор: 2x Intel(R) Xeon(R) CPU E5-2600 v4;
* Память: модули DIMM DDR4 скоростью до 2133 млн транзакций в секунду. Максимальный объем ОЗУ: до 384 Гбайт (12 разъемов для модулей DIMM): 2/4/8/16/32 Гбайт

Сервера хранения должны иметь следующие характеристики:

* Контроллеры RAID (Внутренние: PERC S130, PERC H330, PERC H730, PERC H730P; Внешние: PERC H830);
* Диски: 2 x 250G SSD, 12 x 6TB HDD;
* Процессор: Intel(R) Xeon(R) CPU E5-2600 v4;
* Память: модули памяти DDR4 объемом 4, 8, 16, 32, 64 или 128 Гбайт с пропускной способностью до 2 400 млн. транзакций в секунду

## Требования к ПО серверной части

Для поддержки функционирования Системы рекомендуется использовать операционные системы семейства Linux.

Требования к операционной системе серверной части:

1. Ubuntu 14.04 LTS amd64;
2. LVM;
3. Volume group system: 22G:

* root: 10G;
* tmp: 1G;
* swap: 1G;
* var: 10G.

1. Volume group shared: - зависит от VM.

## Требования к операционной системе

Установка должна производиться под операционной системой **Ubuntu 14.04.5** **lts**  (операционную систему можно скачать по адресу: <http://releases.ubuntu.com/14.04/ubuntu-14.04.5-server-amd64.iso>) на отдельный сервер, имеющий характеристики не ниже следующих:

* RAM: 24 Гб;
* CPU: 32 ядра;
* HDD: 150 Гб.

## Документация для ознакомления

Перед началом установки программного обеспечения ОФД необходимо ознакомиться со следующим списком литературы:

* «Руководство по Ubuntu Server» http://team.ubuntu.ru/\_media/translate/docs/serverguide-precise-ru.pdf;
* «Руководство по управлению гипервизором KVM посредством libvirt» http://help.ubuntu.ru/wiki/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE\_%D0%BF%D0%BE\_ubuntu\_server/%D0%B2%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F/libvirt/

## Действия перед запуском виртуальной машины

Перед запуском виртуальной машины на основе образа диска **testofdenv.img** с standalone версией окружения ОФД используется гипервизор KVM. Для его установки требуется установить следующие пакеты:

* qemu-kvm;
* libvirt-bin;
* bridge-utils.

Установку пакетов можно осуществить с помощью команды: **# apt-get install –y <название пакетов>**.

Для запуска системы управления виртуальными машинами на основе гипервизора КVM требуется запустить службу libvirtd: **# service libvirtd start**

Для автоматического запуска системы управления виртуальными машинами на основе гипервизора KVM при старте операционной системы требуется выполнить следующую команду: **# update-rc.d libvirtd enable**

*Примечание:* *Образ диска* ***testofdenv.img*** *с standalone версией окружения ОФД передается комплектом на физическом накопителе.*

Для запуска виртуальной машины на основе образа диска **testofdenv.img** нужно создать шаблон виртуальной машины в формате XML.

Пример XML- шаблона:

<domain type='kvm'>

<name>**Имя VM**</name>

<memory>**Объем RAM в Kb**</memory>

<vcpu>**Количество CPU**</vcpu>

<os>

<type arch="x86\_64">hvm</type>

</os>

<clock sync="localtime"/>

<devices>

<emulator>/usr/bin/qemu-system-x86\_64</emulator>

<disk type='file' device='disk'>

<source file='**Путь до образа диска**'/>

<target dev='sda'/>

</disk>

<interface type='network'>

<source network='default'/>

</interface>

<graphics type='vnc' port='-1' keymap='en-us'/>

</devices>

</domain>

Пояснения к приведенному ранее примеру XML-шаблона:

* «Имя VM» – имя виртуальной машины, отображаемое в консоли гипервизора;
* «Объем RAM в Kb» – объем оперативной памяти виртуальной машины в Кб;
* «Количество CPU» – количество ядер процессора, выделенных для установки программного обеспечения ОФД в виртуальной машине;
* «Путь до образа диска» – путь до образа диска **testofdenv.img** с standalone версией окружения ОФД относительно корня файловой системы.

Загрузка XML-шаблона происходит через консоль гипервизора. Пример загрузки XML-шаблона: **# virsh define template.xml** ,

где вместо «template.xml» следует указать путь до созданного XML-шаблона.

## Запуск виртуальной машины

Запуск виртуальной машины из созданного и загруженного XML-шаблона осуществляется следующим образом: **# virsh start имя виртуальной машины**

Особенности работы виртуальной машины, запущенной из предоставленного образа диска **testofdenv.img**:

* Получение ip-адреса происходит по DHCP-протоколу;
* Не требуется дополнительной настройки служб и процессов;
* Работа ОФД в полном нормальном режиме возможна только через 5-10 минут после старта виртуальной машины.

## Список адресов служб

Ниже приведен список адресов служб, работающих на виртуальной машине с использованием образа диска **testofdenv.img** с standalone версией окружения ОФД:

* Личный кабинет налогоплательщика – http://ip-адрес виртуальной машины:9849;
* Система управления ОФД – http://ip-адрес виртуальной машины:8014;
* Прием фискальных документов – tsp://ip-адрес виртуальной машины:7777;
* Web-интерфейс Spark-кластера для контроля роботы Spark-приложений – http://ip-адрес виртуальной машины:8080;
* Сервис поиска чеков – http://ip-адрес виртуальной машины:9850.

# Обеспечение надёжности функционирования ПК ОФД

Система работает в условиях высокой доступности - 99,9%

Режим работы системы – 365/7/24.

Для обеспечения надежного резервирования данных, уменьшения нагрузки на сервера, а также выполнения требований по отказоустойчивости Система представляет собой функциональную структуру серверов, объединённых в подсистемы, размещаемых в отдельном ЦОДе. Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию запрещен.

Эксплуатация Системы предусматривает два вида технического обслуживания: оперативное обслуживание и профилактические работы. Оперативное обслуживание включает ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов Системы. Оперативное обслуживание не нарушает выполнение функций Системы в целом. Профилактические работы предусматривают периодическую проверку и обслуживание составных частей Системы.

Для обеспечения надежности Системы предусматривается выполнение различных видов резервирования. В ходе эксплуатации системы для обеспечения ее бесперебойной и надежной работы выполняется полное резервное копирование фискальных БД и АС JIRA.

Отказоустойчивость Системы обеспечивается распределением программного обеспечения по разным физическим серверам и его дублированием (включая балансировщик, ККТ-Сервера, очереди данных, приложения обработки данных, средства защиты фискальных данных, все БД и приложения интерфейса доступа к данным).

Средства защиты информации обеспечивают безопасный доступ и хранение данных, контроль за доступом пользователей к ресурсам, защиту от вирусных атак, криптографическую защиту каналов связи, а также сканирование безопасности Системы для выявления уязвимости.