Утвержден
ИТВБ.00497-03 32 01-ЛУ

СИСТЕМА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА «СЭД-СИРИУС»

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Руководство системного программиста

ИТВБ.00497-03 32 01

Листов 55

Идентификатор документа на электронном носителе:
ИТВБ.00497-03 32 01_РСП.pdf

2022

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Литера

АННОТАЦИЯ

Настоящий документ является эксплуатационным документом отечественного модифицированного программного изделия «СЭД-Сириус» версии 3 ИТВБ.00479-03 (далее – СЭД).

Документ предназначен для системных программистов (со стороны разработчиков и со стороны эксплуатационного персонала объектов применения), реализующих процессы жизненного цикла СЭД: формирование поставочных компакт-дисков СЭД на объекты применения; проверка, установка, настройка; управление функционированием, совершенствованием и развитием (модернизацией) СЭД.

Документ содержит общие сведения о СЭД, сведения о её структуре и функциях, определяет порядок: формирования, проверки комплектности, подлинности и целостности поставочного компакт-диска СЭД; вызова и установки требуемого для функционирования СЭД общего программного обеспечения (ОПО) и собственно СЭД на программно-технические комплексы (ПТК) объектов применения; настройки и последующей проверки работоспособности СЭД; управления функционированием и модернизацией СЭД, а также определяет состав служебных сообщений, выдаваемых системному программисту при реализации процессов жизненного цикла СЭД.

Содержание документа требует от системных программистов ознакомления со следующими программными документами СЭД:

- Описание программы (ИТВБ.00497-03 13 01);

- Руководство оператора (часть 1 ИТВБ.00497-03 34 01-1 и часть 2 ИТВБ.00497-03 34 01-1).

Документ выполнен в соответствии с требованиями ГОСТ 19.503-79 ЕСПД. Руководство системного программиста. Требования к содержанию и оформлению.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

СОДЕРЖАНИЕ

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение СЭД

1.1.1. Областью применения СЭД, разработанного и перманентно модифицируемого по требованиям пользователей, является повседневная деятельность организаций, реализуемая в условиях перехода на электронное взаимодействие на базе единого информационно-коммуникационного пространства.

1.1.2. Функциональным назначением СЭД является автоматизация в распределённой вычислительной и телекоммуникационной сети организаций следующих основных (и других) процессов документационного обеспечения организационного управления (ДООУ), ориентированных на обеспечение государственного управления в условиях постоянно актуализируемых функциональных требований пользователей СЭД при работе с электронными документами (ЭД):

1) процесс обработки входящей корреспонденции;

2) процесс обработки исходящей корреспонденции;

3) процесс работы с обращениями граждан, включая взаимодействие с Порталом ССТУ (сетевой справочный телефонный узел) РФ – федеральным сайтом для органов власти, согласно Руководства для органов власти по настройке функционала импорта данных об обращениях в раздел «Результаты рассмотрения обращений» информационного ресурса ССТУ.РФ в закрытой сети версии 2;

4) процесс обработки служебной корреспонденции;

5) процесс исполнения и контроля поручений и документов;

6) процесс ведения протоколов, формирования и сопровождения отчётных форм;

7) процесс МЭДО.

1.1.3. Эксплуатационным назначением СЭД является внедрение электронного делопроизводства и документооборота в организациях с реализацией основного жизненного цикла электронных документов в целях повышения качества

выполнения функций организации, её подразделений и контроля исполнительской дисциплины с реализацией следующих основных системных требований к СЭД:

- обеспечение высокой производительности;
- обеспечение высокой надежности;
- эволюционная масштабируемость;
- гибкость (возможность внесения модификаций путём настройки);
- минимизация затрат используемых ресурсов технического обеспечения и ОПО;
- модульность построения;
- унификация программных и общесистемных решений;
- защита от несанкционированного доступа к СЭД и исходному коду программы;
- повышение качества реализации процессов повседневной деятельности организации и контроля исполнительской дисциплины.

1.1.4. СЭД обеспечивает возможность реализации электронного документооборота, но не исключает возможности использования традиционного бумажного документооборота. Порядок взаимодействия электронного и бумажного документооборота должен быть отражен в Инструкции по делопроизводству организации.

1.2. Функции СЭД

1.2.1. В соответствии с вышеприведённым назначением СЭД основными функциональными задачами, решаемыми СЭД, являются:

1) повышение эффективности выполнения деловых процессов должностных лиц конкретной организации (внутренних пользователей СЭД) при их коллективной работе с электронными документами, в общем случае, на территориально распределённых объектах применения:

а) при взаимодействии между собой локальных (объектовых) пользователей СЭД, подключаемых к объектовым локальным вычислительным сетям (ЛВС);

б) при взаимодействии объектовых пользователей СЭД с удалёнными пользователями СЭД и между объектами – посредством телекоммуникационных сетей организации;

2) повышение эффективности выполнения совместных деловых процессов должностных лиц конкретной организации государственного управления (внутренних пользователей СЭД) и взаимодействующих внешних организаций государственного управления (внешних пользователей СЭД) при их коллективной работе с ЭД (напрямую через шлюз СЭД) посредством специализированной федеральной системы – системы межведомственного электронного документооборота (МЭДО) с регламентированными протоколами взаимодействия;

3) обеспечение электронного взаимодействия с физическими и юридическими лицами по вопросам деятельности организации посредством сетей общего применения;

4) повышение эффективности выполнения деловых процессов внутренних пользователей СЭД конкретной организации за счёт автоматизации технологических процедур организационного управления, выполняемых посредством реализации в СЭД:

а) функционала Корпоративного портала организации;

б) взаимодействия с имеющимися информационными системами организации;

в) взаимодействия с рядом внешних систем и сервисов: Платформа мобильной электронной подписи (МЭП), Служба активных каталогов (Active Directory – AD), Портал дистанционного приёма граждан «ССТУ.РФ», Единая система идентификации и аутентификации (ЕСИА), Telegram, E-mail и др.

1.2.2. Детализированный функционал СЭД с привязкой к автоматизируемым процессам ДООУ, структуре и алгоритму СЭД приведён в разделе 3 Описания программы (ИТВБ.00497-03 13 01).

1.3. Среда функционирования СЭД

1.3.1. Для обеспечения выполнения СЭД-Сириус используются технические и программные средства ПТК в рамках двух его предельных технических конфигураций, заданных в ТЗ:

- минимальная техническая конфигурация ПТК;
- техническая конфигурация ПТК, рекомендуемая для промышленной эксплуатации СЭД-Сириус в развитых организациях с большим документооборотом.

1.3.2. Минимальная техническая конфигурация ПТК состоит из одного выделенного (физического или виртуального) сервера со следующими характеристиками – комплексный сервер (сервер веб-приложений + сервер БД + сервер полнотекстового поиска + файловый сервер + сервер конвертирования): не менее двух процессоров (количество ядер – 16, тактовая частота – 2 ГГц); оперативная память – не менее 48 ГБ (DDR3, 1600 МГц); ёмкость жестких дисков – не менее 12 ТБ; подключение к сети 100 Мбит/с.

1.3.3. Техническая конфигурация ПТК, рекомендуемая для промышленной эксплуатации СЭД-Сириус в развитых организациях с большим документооборотом, состоит из четырёх выделенных (физических или виртуальных) серверов со следующими характеристиками:

1) сервер веб-приложений: не менее четырёх процессоров (количество ядер – 16, тактовая частота – 2 ГГц); оперативная память – не менее 64 ГБ (DDR3, 1600 МГц); ёмкость жестких дисков – не менее 400 ГБ; подключение к сети 1 Гбит/с;

2) сервер БД: не менее двух процессоров (количество ядер – 8, тактовая частота – 2 ГГц); оперативная память – не менее 64 ГБ (DDR3, 1600 МГц); ёмкость жестких дисков – не менее 2 ТБ; подключение к сети 100 Мбит/с;

3) файловый сервер с сервером полнотекстового поиска: не менее двух процессоров (количество ядер – 8, тактовая частота – 2 ГГц); оперативная память – не менее 16 ГБ (DDR3, 1600 МГц); ёмкость жестких дисков – не менее 10 ТБ; подключение к сети 1 Гбит/с;

4) сервер конвертирования: не менее двух процессоров (количество ядер – 4, тактовая частота – 2 ГГц); оперативная память – не менее 16 ГБ (DDR3, 1600 МГц); ёмкость жестких дисков – не менее 40 ГБ; подключение к сети 1 Гбит/с.

1.3.4. Клиентские автоматизированные рабочие места (АРМ), обеспечивающие доступ к СЭД-Сириус, соответствуют следующим характеристикам, заданным в ТЗ:

- имеют предустановленную программу для просмотра веб-сайтов (далее – браузер) с поддержкой HTML 5 и JavaScript;

- используют браузеры Google Chrome, Firefox Mozilla, Яндекс Браузер, Спутник;

- имеют цветной дисплей с поддержкой не менее 4096 цветов и разрешение по ширине не менее 1024 пикселей, по высоте не менее 640 пикселей;

- обеспечивают возможность навигации по экранным элементам управления и ввода данных по средством графических меню и экранных и/или подключаемых клавиатур;

- имеют стабильный доступ к сети для работы с СЭД-Сириус на скорости не менее 320 кбит/с (для обеспечения отображения страниц в пределах 5 с).

1.3.5. Для обеспечения функционирования СЭД-Сириус используется следующая программная среда:

1) в минимальной технической конфигурации ПТК используется следующая конфигурация ОПО – на комплексном сервере (сервер веб-приложений + сервер БД + сервер полнотекстового поиска + файловый сервер + сервер конвертирования): серверная операционная система (ОС) специального назначения Astra Linux Common Edition Релиз Смоленск 1.7, а также сгенерированные в составе указанной ОС защищенные версии веб-сервера Apache 2.2, системы управления базами данных (СУБД) PostgreSQL 11.10 и текстовый процессор пакета офисных приложений Libre Office 7.0.3 (или более поздняя версия);

2) в рекомендуемой технической конфигурации ПТК используется следующая конфигурация ОПО:

а) на сервере веб-приложений – серверная ОС специального назначения Astra Linux Special Edition Релиз Смоленск 1.7 и защищенная версия веб-сервера Apache 2.2, сгенерированная в составе указанной ОС;

б) на сервере БД – серверная ОС специального назначения Astra Linux Special Edition Релиз Смоленск 1.7 и защищенная СУБД PostgreSQL 11.10, сгенерированная в составе указанной ОС;

в) на файловом сервере с сервером полнотекстового поиска – серверная ОС специального назначения Astra Linux Special Edition Релиз Смоленск 1.7 и файловая система, сгенерированная в составе указанной ОС;

г) на сервере конвертирования – серверная ОС специального назначения Astra Linux Special Edition Релиз Смоленск 1.7 и текстовый процессор пакета офисных приложений Libre Office 7.0.3 (или более поздняя версия);

3) клиентские АРМ имеют предустановленные веб-браузеры с поддержкой HTML 5 и JavaScript. Доступ к СЭД-Сириус не привязан к рабочему месту, адаптивный веб-интерфейс обеспечивает полнофункциональную работу на любом типе устройств посредством браузера без установки дополнительного программного обеспечения (за исключением средств криптографической защиты).

1.3.6. СЭД-Сириус разработана на интерпретируемых языках объектно-ориентированного программирования высокого уровня и языках гипертекстовой разметки (при этом ограничительные требования к языковому набору не предъявляются):

- PHP 5.3;
- JavaScript;
- HTML 5;
- CSS.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

2. СТРУКТУРА ПРОГРАММЫ

2.1. Структурное построение СЭД

2.1.1. СЭД функционирует в конфиденциальном контуре АС организации.

2.1.2. При изменении и добавлении функционала СЭД применяются:

1) логические методы построения алгоритмов автоматизируемых процедур документационного обеспечения управления (см. раздел 3 Описания программы ИТВБ.00497-03 13 01). Это связано с тем, что данные процессы не содержат расчётов и моделей, а ориентированы на выполнение операций по приёму, обработке, хранению и выдаче данных, формированию файловых хранилищ и баз данных;

2) технологические методы обработки информации:

а) методы использующиеся файловой системой (чтение содержимого файлов, перемещение файлов);

б) методы обработки «get»-запросов (чтение переменных и вложений);

в) методы отправки сообщений с использованием API.

2.1.3. Согласно многоуровневой «клиент-серверной» архитектурной модели построения СЭД функциональные ПТК, используемые для непосредственного размещения и обеспечения работы модулей СЭД, так же построены по логической архитектуре «клиент-сервер»:

1) презентационный уровень (обеспечивает реализацию пользовательского интерфейса СЭД на стороне клиента);

2) промежуточный уровень приложений (обеспечивает реализацию функциональных и лингвистических компонентов СЭД на стороне серверов приложений);

3) уровень данных (обеспечивает реализацию информационных компонентов СЭД на стороне серверов данных).

2.1.4. В качестве метода построения СЭД используется архитектурная концепция «Модель-Представление-Элемент управления». Данная концепция

позволяет разделять данные, представление и обработку действий пользователя на три отдельных компонента:

1) Модель предоставляет данные (обычно для Представления), а также реагирует на запросы (обычно от Контроллера), изменяя своё состояние;

2) Представление отвечает за отображение информации (пользовательский интерфейс);

3) Элемент управления интерпретирует данные, введённые пользователем, и информирует Модель и Представление о необходимости соответствующей реакции.

Уровень хранения данных реализован с применением разработанных реляционных БД, управляемых СУБД.

Прикладное программное обеспечение комплексного сервера веб-приложений разработано:

1) на базовых решениях «СЭД-Сириус» версий 1 и 2 (ИТВБ.00497-01 и ИТВБ.00497-02 соответственно);

2) с использованием дополнительных свободно распространяемых библиотек общего программного обеспечения (ОПО) Vue.js v2.2.0, Bootstrap v3.3.6, Font Awesome 4.7.0, jQuery JavaScript Library v2.1.4, php 7.4 и выше, postgresql9.6 и выше;

3) путём изменения существующих и разработки дополнительных модулей СЭД с использованием следующих языков программирования и гипертекстовой разметки:

а) PHP – версия 5.3;

б) CSS – версия css3;

в) JavaScript – версия ES6;

г) ECMAScript 2015;

д) HTML – версия 5;

е) Python;

4) с использованием языка ввода-вывода данных и манипулирования данными, поддерживающего стандарт SQL-99.

Презентационный уровень реализован с использованием технологии «тонкого клиента», обеспечивающей работу пользователя с СЭД посредством стандартных

средств просмотра интернет-страниц (веб-браузеров) с реализацией содержательной функциональной обработки информации на серверах веб-приложений и баз данных.

2.1.5. Среда исполнения (функционирования) СЭД состоит из следующих элементов:

1) прикладные функциональные модули и описание структуры БД, разработанное с использованием базовых решений «СЭД-Сириус» по построению базы данных и функционала, свободно распространяемых библиотек ОПО и ОСПО, языков программирования и гипертекстовой разметки;

2) среда исполнения свободно распространяемых библиотек ОПО и ОСПО, инструментария языков программирования и гипертекстовой разметки;

3) среда исполнения разработанных модулей веб-приложений СЭД на АРМ пользователей (вэб-браузеры);

4) ОПО среды функционирования (см. подраздел 1.3).

2.1.6. СЭД является интерпретируемой программой, исходный код и дистрибутив которой совпадают между собой, содержат комментарии и представляются на объекты применения на поставочном электронном носителе (ЭН). Детальнее структура СЭД изложена в Описании программы ИТВБ.00497-03 13 01).

2.2. Связи СЭД с другими программами

2.2.1. Связи СЭД с другими (внешними) программами строятся на основе применения унифицированных методов и средств доступа к информации, унифицированных протоколов обмена информацией в целях реализации в процессах ДООУ следующих типовых функций:

- импорт и использование справочников и классификаторов из сопрягаемых автоматизированных информационных систем;

- импорт и использование справочников и классификаторов из имеющихся информационных систем организации;

- экспорт справочников и классификаторов во взаимодействующие информационные системы.

2.2.2. Обмен электронными сообщениями при взаимодействии СЭД с информационными системами электронного документооборота органов и организаций государственной власти, государственных внебюджетных фондов, иных организаций реализуется посредством МЭДО.

Цель создания и использования МЭДО – повышение эффективности государственного управления за счет сокращения времени прохождения документов между организациями и ведомствами, минимизации затрат на обработку и транспортировку документов, мониторинга хода рассмотрения и исполнения документов.

2.2.2.1. Механизм взаимодействия СЭД с системой МЭДО реализован как двухсторонний опосредованный. Взаимодействие должно происходить с использованием общих ресурсов СЭД и системы МЭДО путем чтения и записи файлов заголовков корреспонденции, уведомлений, содержимого документов в общих ресурсах. Проверка состояния общих ресурсов должна производиться СЭД с определенной периодичностью, устанавливаемой в конфигурации СЭД.

Основным принципом МЭДО является интеграция имеющихся СЭД участников МЭДО и транспортной системы (почтовой службы), обеспечивающей в автоматизированном режиме защищенный обмен электронными сообщениями.

Организатором МЭДО является ФСО России, которая в этом качестве реализует организационное и методическое обеспечение МЭДО, ведение адресных справочников МЭДО, создание и эксплуатацию технико-технологической инфраструктуры и обеспечивает информационную безопасность МЭДО.

2.2.2.2. В основу реализации МЭДО положены следующие принципы:

1) все участники МЭДО используют единый формат обмена электронными сообщениями, утвержденный ФСО России и Минкомсвязи России;

2) каждый участник МЭДО использует ПТК (шлюз), обеспечивающий обмен электронными сообщениями между своей СЭД и МЭДО (реализующий временное

хранение сообщений, выгрузку поступивших сообщений из транспортирной системы МЭДО и загрузку исходящих сообщений в транспортную систему МЭДО);

3) каждый участник МЭДО использует программный комплекс сопряжения (адаптер) своей СЭД с МЭДО, обеспечивающий:

а) для поступающих по МЭДО сообщений – прием и преобразование из единого формата обмена во формат СЭД для дальнейшей обработки;

б) для исходящих по МЭДО сообщений – их формирование, преобразование из формата СЭД в единый формат обмена и подготовку к передаче по транспортной системе МЭДО.

2.2.2.3. Взаимодействие сопрягаемых СЭД с МЭДО осуществляется в соответствии с со следующими требованиями:

- Технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти, утвержденные распоряжением Правительства Российской Федерации от 2 октября 2009 г. № 1403-р;

- Технические требования, утверждённые приказом Минцифры России и ФСО России от 29 июня 2022 г. № 500/82 «Технические требования к порядку ведения нормативно-справочной информации системы межведомственного электронного документооборота».

2.2.2.4. Интеграция СЭД с МЭДО позволяет:

- соблюдать нормативные требования, предъявляемые к организации МЭДО в организациях-участниках МЭДО (абонентах);

- минимизировать трудозатраты делопроизводителей и ИТ-специалистов, связанные с появлением нового способа доставки/отправки корреспонденции;

- исключить финансовые затраты на доставку корреспонденции (почтовые расходы, курьерские услуги) другим участникам МЭДО;

- значительно сократить сроки прохождения корреспонденции между абонентами МЭДО (до нескольких часов);

- своевременно получать оперативную информацию о результатах рассмотрения документов, отправленных в адрес других абонентов.

Информационное взаимодействие с использованием транспортной шины-МЭДО осуществляется путем обмена транспортными контейнерами (ТК), содержащими документы в электронном виде, подписанные электронной подписью (ЭП), и технологическими электронными сообщениями (уведомлениями).

Актуальная информация о действующих участниках информационного взаимодействия с указанием их точных наименований, электронных адресов и идентификаторов МЭДО размещается в МЭДО и доступна для использования участниками информационного взаимодействия.

2.2.2.5. Краткое описание ТК:

1) ТК документа в электронном виде может быть представлен как в виде набора отдельных файлов, так и одного файла. Получатель и отправитель ЭД могут преобразовывать ТК из одного вида представления в другой в процессе его создания, обработки и хранения. Преобразование ТК из одного вида в другой не считается его изменением;

2) при представлении ТК в электронном виде в виде одного файла должен использоваться формат ZIP-папки, описанный в открытой спецификации, доступной по адресу http://www.pkware.com/documents/casestudies/APPNOTE.TXT, в части использования возможностей и технологий, в отношении которых спецификацией допускается их свободное (без ограничений) использование;

3) для передачи по МЭДО транспортный контейнер документа в электронном виде представляется в виде одного файла и передаётся в составе сообщения МЭДО типа «Транспортный контейнер» согласно требованиям к организационно-техническому взаимодействию государственных органов и организаций посредством обмена документами в электронном виде;

4) ТК документа в электронном виде должен соответствовать его описанию согласно требованиям к организационно-техническому взаимодействию государственных органов и организаций посредством обмена документами в электронном виде.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

ТК документа в электронном виде состоит из следующих файлов:

1) файл описания транспортного контейнера, определяющий состав контейнера и содержащий минимальную атрибутику документа и представляемый в виде типизированного XML;

2) приложенные файлы, в том числе:

а) файл документа;

б) файлы электронных подписей документа;

в) файлы графических элементов регистрационных данных и графических элементов отметок об ЭП;

г) файлы приложений к документу и файлы их электронных подписей (при наличии);

д) файл электронной подписи набора файлов транспортного контейнера (за исключением данного файла, при наличии);

3) файлы описания транспортного контейнера.

2.2.3. СЭД реализует взаимосвязь со смежными информационными системами организации на основе сервис-ориентированной архитектуры (СОА) и веб-сервисов. В основе СОА лежат принципы многократного использования функциональных элементов ИТ, унификации типовых операционных процессов. Компоненты программы могут быть распределены по разным узлам сети, и предлагаются как независимые и слабо связанные, заменяемые сервисы-приложения. Интерфейс компонентов СОА-программы осуществляет инкапсуляцию деталей реализации конкретного компонента (ОС, языка программирования и т.п.). СОА хорошо зарекомендовала себя при построении крупных корпоративных программных систем.

Взаимосвязь между смежными информационными системами происходит при помощи обмена информацией в формате .xml по протоколу обмена структурированными сообщениями в распределённой вычислительной среде (SOAP).

Преимущества применения протокола SOAP перед другими форматами для передачи данных:

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

- простота кодирования XML структур данных;

- при использовании SOAP-сообщений предоставляются дополнительные инструменты, позволяющие легко добавлять, например, функции обеспечения безопасности или трассировки;

- имеются наборы инструментов SOAP для различных языков программирования. Для обеспечения связи с сервисом посредством методов GET и POST протокола HTTP отсутствует необходимость самостоятельно конструировать строку запроса, а затем проводить синтаксический анализ ответа.

2.2.4. В СЭД используется следующий формат электронного документа:

- файл документа, а также файл электронного образа документа с внедренными графическими элементами регистрационных данных и отметок об ЭП (в случае его формирования) имеют формат PDF/A-1, соответствующий требованиям Международного стандарта ISO 19005-1:2005. Управление документацией. Формат файлов электронных документов для долгосрочного хранения. Часть 1. Использование PDF 1.4 (PDF/A-1);

- содержательная часть документа включается в файл формата PDF/A-1 в текстовом виде.

Совместимость СЭД со смежными и внешними ИС обеспечивается за счет использования общих форматов данных.

В качестве форматов обмена данными используются XML 1.1, JSON.

2.2.5. В СЭД используется усиленная квалифицированная электронная подпись (ЭП):

- ЭП, формируемые при организации информационного взаимодействия, соответствуют требованиям к усиленной квалифицированной электронной подписи. При создании таких ЭП используется формат PKCS#7 (Public-Key Cryptography Standard #7). Общее описание стандарта PKCS#7, опубликованного в качестве RFC (Request for Comments) с номером 2315, доступно по адресу http://tools.ietf.org/html/rfc2315 без включения подписываемых данных;

- ЭП должностных лиц и организаций, создаваемые в рамках обмена документами в электронном виде при организации информационного

взаимодействия, формируются в отдельных файлах (ЭП одного должностного лица должен соответствовать отдельный файл).

2.2.6. В СЭД реализовано взаимодействие с Платформой МЭП.

Платформа МЭП состоит из следующих основных частей:

1) Услуга МЭП для Абонентов МегаФон;

2) Партнёрская программа МЭП, для поставщиков услуг (Сервис-провайдеров);

3) Партнерские Удостоверяющие центры (УЦ).

2.2.6.1. Услуга МЭП – продукт для Абонентов Оператора мобильной связи МегаФон, физических и юридических лиц, позволяющий проводить операции с ЭП с использованием мобильных устройств (мобильные телефоны, планшеты со слотом для SIM-карты) и специальной SIM-карты. Основное предназначением МЭП – это идентификация лица, подписавшего электронный документ.

Другие функции МЭП:

- доказательное подтверждение авторства документа. Есть возможность подписывать такие поля, как «автор», «внесённые изменения», «метка времени» и др.;

- контроль целостности передаваемого документа. Подпись изменяется и становится недействительной при любом случайном или преднамеренном изменении документа;

- защита от подделки документа;

- невозможность отказа от авторства. Владелец не может отказаться от своей подписи под документом, поскольку корректную подпись можно создать, лишь зная закрытый ключ, а он известен только владельцу (автору).

2.2.6.2. Партнерская программа МЭП – набор услуг для Сервис-провайдеров (юридических лиц, индивидуальных предпринимателей, государственных учреждений), позволяющий использовать Услугу МЭП в собственных ИС и организовывать процессы предоставления услуг Абонентам с использованием электронного документооборота.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Основные услуги, предоставляемые Платформой МЭП для Сервис-провайдеров:

- подписание произвольного электронного документа;

- аутентификация абонента в ИС Сервис-провайдеров;

2.2.6.3. Интеграция с Сервис-провайдерами – перед началом использования, все приложения Сервис-провайдера должны быть зарегистрированы в Платформе МЭП:

- МегаФон передает серверный SSL-сертификат;

- Сервис-провайдер генерирует ключевую пару RSA, создает сертификат и передает сертификат в МегаФон. (более подробно смотри раздел Аутентификация Партнерских систем);

- опционально, если Сервис-провайдер собирается использовать push стратегию нотификации. URL адреса call back методов, на которые будет осуществляться доставка статусов и результатов операций, при push-стратегии нотификации;

- МегаФон регистрирует приложение Сервис-провайдера и присваивает ему Partner_id- идентификатор приложения Сервис-провайдера, используется при взаимодействии приложения Сервис-провайдера и Платформы МЭП.

При интеграции Сервис-провайдеров с Платформой МЭП возможны два основных подхода:

1) подписание документов через публичный SOAP API – предназначен для интеграции:

а) доверенных ИС Сервис-провайдеров, таких как Сайт государственных услуг;

б) внутренних систем (CRM, ERP и т.п.);

в) систем, имеющих десктоп или мобильных клиентов;

2) подписание документов в защищенном разделе Сайта МегаФон – для интеграции с любыми Сервис-провайдерами, предоставляющими услуги в сети Интернет.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Подписание документов через публичный SOAP API – данный подход используется в ИС, в которых абонент регистрируется и аутентифицируется для выполнения бизнес-процессов – различные внутренние ИС, системы использующие мобильные клиенты или государственные ИС. Причем аутентификация абонента может выполняться как с помощью «МЭП Аутентификации», так и с использованием внутренней аутентификации в ИС Сервис-провайдера:

1) отличительной особенностью данного подхода является то, что абонент может работать только в ИС или с оборудованием Сервис-провайдера, не перенаправляясь на Сайт МегаФон;

2) для подписания и получения статуса подписания используются методы SOAP интерфейса Service Provider API. Пример приложений, где удобно использовать данный подход:

а) подтверждение транзакций в интернет-банке;

б) CRM, ERP и т.п. внутренние системы;

в) портал государственных услуг.

Подписание документов в защищенном разделе сайта МегаФон – при использовании данного подхода (в случае необходимости произвести какие-либо действия, связанные с использованием МЭП для подписания документов) применяется приложение Сервис-провайдер, которое:

- осуществляет HTTP redirect на защищенный раздел Сайта МегаФон, где размещена специализированная страница. При данном подходе необходимость использовать HTTP redirect ограничивает использование данного подхода только internet-сайтами. Также данный подход используется в случаях, когда ИС Сервис-провайдера использует готовые бизнес-сервисы Платформы МЭП;

- встраивает виджет, предоставленный МегаФон, в свой Сайт.

2.2.6.4. Стратегии нотификации – при работе с методами подписания и аутентификации можно использовать два вида нотификации о статусе выполнения операции и получения результатов:

1) push-стратегия – платформа МЭП информирует ИС Сервис Провайдера о статусе операции;

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

2) pull-стратегия – ИС Сервис Провайдера запрашивает Платформу МЭП о статусе операции.

Для использования push-стратегии Сервис-провайдер должен зарегистрировать в Платформе МЭП список URL на которые возможна отсылка call back вызова. Конкретный call back url ИС Сервис-провайдера указывает при вызове методов Service Provider API:

- в случае, если Платформа МЭП получит статус операции отличный от ожидаемого (200, 201, 202), она будет осуществлять 5 попыток повторной доставки статуса, по следующему расписанию: через 5 мин, через 30 мин, через 1 ч, через 3 ч, через 24 ч;

- если статус не будет доставлен, то он будет храниться в персистентном хранилище Платформы МЭП в течение 10 суток. ИС Сервис-провайдера сможет получить его с использованием pull-стратегии, т.е. запросив соответствующий метод API.

При использовании pull-стратегии рекомендуется опрашивать о статусе и результате операции по следующему расписанию:

- первый запрос, не ранее, чем через 60 с, после отправки запроса на подписание;

- следующие запросы, с интервалом в 30 с и более.

2.2.7. В СЭД реализовано взаимодействие с Active Directory (в части обеспечения единых параметров авторизации пользователей).

Настройка взаимодействия с Active Directory производится после установки и настройки программного обеспечения серверов и СЭД.

Для взаимодействия с Active Directory используется библиотека PHP – php-ldap.

2.2.8. В СЭД реализовано взаимодействие с системой мгновенного обмена сообщениями Telegram (в части отправки уведомлений и файлов документов).

Механизм взаимодействия СЭД с системой мгновенного обмена сообщениями Telegram реализован через протокол Server Message Block.

3. УСТАНОВКА И НАСТРОЙКА

3.1. Входной контроль поставочного комплекта СЭД

3.1.1. Входной контроль поставочного комплекта программного изделия СЭД, прошедшего все установленные виды испытаний и принятого в промышленную эксплуатацию, является начальным этапом его жизненного цикла на объекте применения.

Порядок проведения входного контроля средств вычислительной техники определяется соответствующей Инструкцией, принятой в организации.

3.1.2. Входной контроль СЭД предусматривает проведение её эксплуатационным персоналом следующих проверок:

- визуальная проверка комплектности и физической целостности поставочного ЭН на соответствие табл. 1 Описания программы (ИТВБ.00497-03 13 01);

- визуальная проверка взаимного соответствия информации, приведённой на маркировке поставочного ЭН, его Этикетке и Информационно-удостоверяющем листе (включая проверку заполнения их граф);

- инструментальная проверка на АРМ Администратора комплектности, подлинности и целостности поставочного ЭН по КС в соответствии с процедурой, приведённой в разделе 4;

- содержательная проверка на АРМ Администратора комплектности информации (файлов), записанной на поставочный ЭН, путём вызова и визуализации всех файлов.

3.1.3. При отсутствии замечаний по указанным проверкам входной контроль считается выполненным, о чём составляется приёмочный Акт, и поставочный комплект программного изделия СЭД переходит на второй этап объектового жизненного цикла.

В противном случае составляется рекламационный Акт и поставочный ЭН СЭД возвращается поставщику изделия.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

3.2. Вызов и загрузка СЭД

3.2.1. На втором этапе объектового жизненного цикла СЭД выполняется проверка вызова с поставочного ЭН дистрибутива СЭД и его загрузки на соответствующие серверные ПТК их «клиент-серверной» архитектуры, обеспечивающие функционирование СЭД (см. подраздел 1.3).

3.2.2. Вызов и загрузка СЭД может осуществляется индивидуально на каждый серверный ПТК одним из двух возможных способов:

1) непосредственно с поставочного компакт-диска;

2) путем перехода по ссылке, формируемой в соответствии с настройками серверной части ПТК. Переход по ссылке происходит в браузере АРМ Администратора.

3.2.3. Для вызова и загрузки СЭД необходимо создать ярлык с адресом сервера, на котором установлена соответствующая серверная часть СЭД, либо вписать адрес сервера непосредственно в строку адреса веб-браузера.

Адрес сервера должен иметь следующий формат:

http://<адрес_сервера>

3.2.4. В приложении 1 приведён порядок проведения базовой установки и настройки ОПО на комплексном сервере ПТК (см. подраздел 1.3), базирующемся на ОС Astra Linux SE или UBUNTU SERVER 16.04.4.

3.2.5. В приложении 2 приведён порядок проведения базовой установки и настройки программного и информационного обеспечения СЭД на комплексном сервере ПТК (см. подраздел 1.3), базирующемся на ОС Windows Server 2012 R2 Std.

3.3. Настройка взаимодействия СЭД с внешними системами и сервисами

3.3.1. Внешними ИС и сервисами, с которыми осуществляется интеграция СЭД, являются:

- Система межведомственного электронного документооборота (МЭДО);
- Платформа МЭП;

- Active Directory (в части обеспечения единых параметров авторизации пользователей);

- Telegram.

3.3.2. Настройка взаимодействия с МЭДО производится после установки и настройки программного обеспечения серверов и СЭД путём выполнения Администратором, обеспечивающим эксплуатацию системы (системным программистом), процедур в следующем порядке:

1) установка ПО CIFS (сетевой протокол прикладного уровня) для подключения общих папок для обмена документами:

sudo apt-get install cifs-utils

2) добавление в fstab (конфигурационный файл) директив для автоматического подключения папок при перезагрузке системы:

sudo nano /etc/fstab

//<адрес_папки_с _исходящими_файлами>

/var/www/storage/exchange/igdw/outbox cifs

user=<логин_подключения>,pass=<пароль_подключения>,iocharset=utf8,noperm,uid=www-data,gid=www-data,dir_mode=0777,file_mode=0777,auto 0 0

//<адрес_папки_с _входящими_файлами>

/var/www/storage/exchange/igdw/inbox cifs

user=<логин_подключения>,pass=<пароль_подключения>,iocharset=utf8,noperm,uid=www-data,gid=www-data,dir_mode=0777,file_mode=0777,auto 0 0

3) монтирование папок:

mount –a

4) добавление в cron (планировщик заданий) задачи для запуска скрипта для просмотра монтированных папок:

а) sudo su

б) crontab –e

5) добавление строки запуска скрипта:

0 */1 * * * /usr/bin/php /var/www/postoffice-in-igdw.php >/dev/null 2>&1

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Механизм взаимодействия СЭД с системой МЭДО реализован согласно следующих документов:

1) Правила обмена документами в электронном виде при организации информационного взаимодействия (утв. постановлением Правительства РФ от 25.12.2014 № 1494), предполагающие отказ от направления бумажных документов и реализацию обмена документами в электронном виде с электронной подписью;

2) Перечень видов документов, предусмотренного Правилами обмена документами в электронном виде при организации информационного взаимодействия (утв. распоряжением Правительства РФ от 02.04.2015 № 583-р);

3) Требования к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде (утв. совместным приказом Минкомсвязь России и ФСО России от 27.05.2015 № 186/258).

Взаимодействие происходит с использованием общих ресурсов СЭД и системы МЭДО путем чтения и записи файлов заголовков корреспонденции, уведомлений, содержимого документов в общих ресурсах. Проверка состояния общих ресурсов должна производиться системой с определенной периодичностью, устанавливаемой в конфигурации операционной системы.

3.3.3. Настройка взаимодействия с Платформой МЭП производится после установки и настройки программного обеспечения серверов и СЭД в следующем порядке:

1) добавление в cron задачи для запуска скрипта для опроса сервисов:

а) sudo su

б) crontab –e

2) добавление строки запуска скрипта:

*/1 * * * * /usr/bin/php /var/www/tools/signers/pull.php Megafon --verbose >/dev/nul 2>&1

3.3.3.1. Чтобы пользователь начал пользоваться МЭП необходимо добавить необходимые реквизиты в профиль пользователя как описано в Руководстве оператора. Часть 2 (ИТВБ.00497-03 34 01-2).

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

3.3.3.2. Механизм взаимодействия СЭД с платформой МЭП реализован через протокол SOAP API. Для подписания и проверки статуса подписанного документа используются методы SOAP интерфейса Service Provider API. Проверка состояния подписания должна производиться системой с определенной периодичностью, устанавливаемой в конфигурации операционной системы.

Механизм взаимодействия включает наличие и реализацию процедур:

1) подписание документа, обеспечивающий «сквозной» сценарий подписания произвольного документа ИС Сервис-Провайдера через Service Provider API.

Описание сервиса подписания документов и/или текстов с использованием API доступно по адресу https://msign.megafon.ru/mes-ws/sign?wsdl

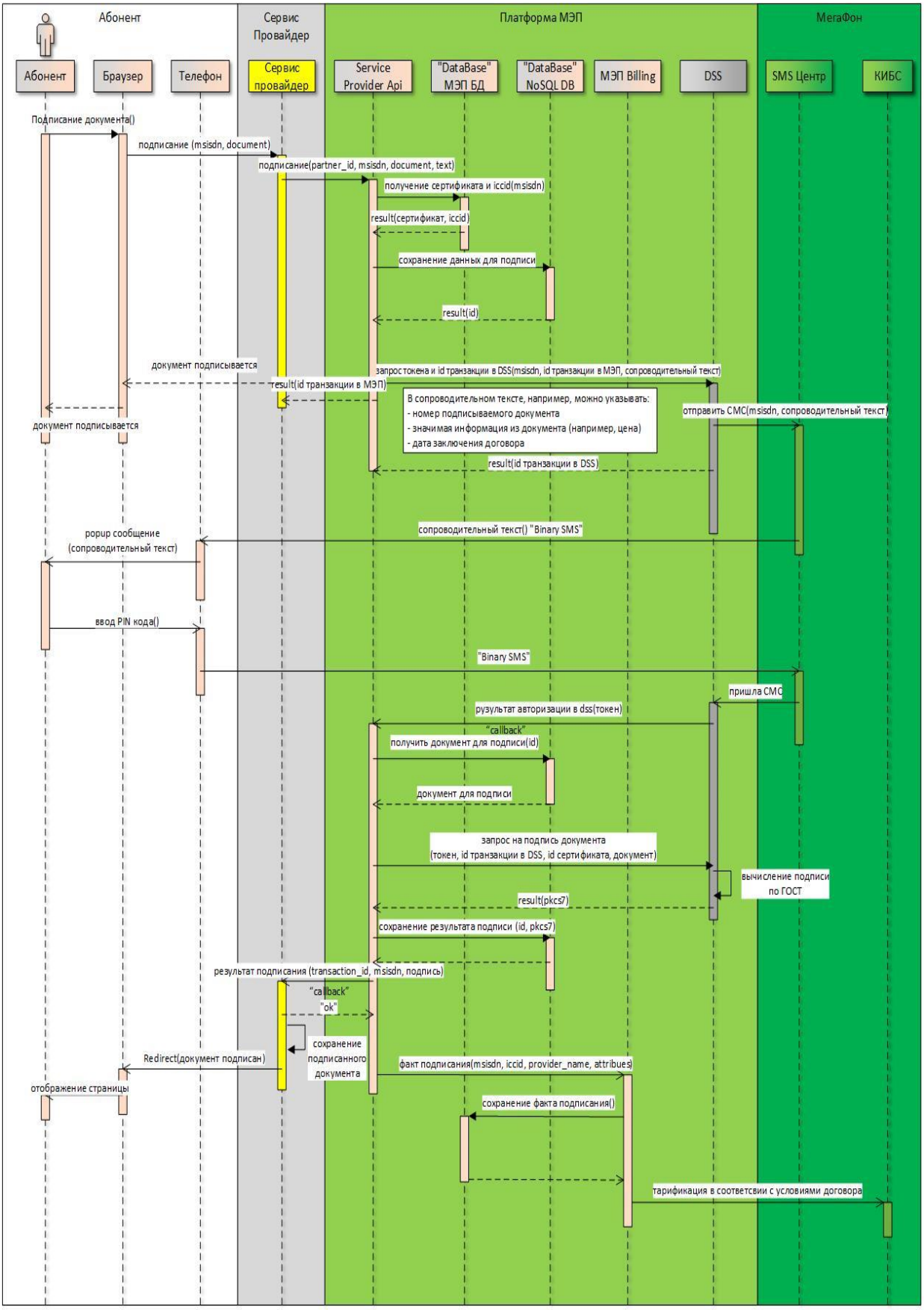
На рис. 1 приведено описание API в части подписания документа с использованием услуги МЭП;

2) проверка интеграции с МЭП, осуществляется при помощи подписания любого ЭД с помощь мобильной электронной подписи. После подписания документа появится графическое отображение подписанного документа.

3.3.3.3. В СЭД подписание документа осуществляется с помощью сервиса SIGNDOCUMENT.

Используемый в данном сервисе метод предназначен для подписания произвольных документов, с использованием МЭП.

Настройка процедуры подписания документа при помощи МЭП осуществляется при помощи сервисов, приведенных в табл. 1,2.



Описание API в части подписания документа с использованием услуги МЭП

Рис. 1

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Таблица 1 – Входные параметры

Название параметра	Тип	Обязательность	Описание
partner_id	string	Да	Идентификатор ИС Сервис-Провайдера осуществляющей операцию подписание
msisdn	string	Нет	Мобильный номер SIM карты клиента с ЭП (обязательно для указания, если не указана transacrionId, совместно не используются)
transactionId	string	Нет	Id авторизационной транзакции, которая будет использована для подписания (обязательно для указания, если не указан msisdn, совместно не используются)
text	string	Да	Текст, который будет отображен на Мобильном Устройстве Абонента при подписании документа. пример: Договор № 12345 от 21.12.2012, количество позиций 23, на сумму 123456.78 руб. Передается в виде Base 64
document	string	Да	Подписываемый документ (накладная, договор, скан и т.п.), передается в виде Base64
signType	string	Нет	Тип подписи. Возможные значения: – Attached – прикрепленная подпись – Detached – открепленная подпись Если параметр отсутствует, Платформа МЭП создает detached подпись.
cbURL	String	Нет	Call back URL для push стратегии нотификации. Передается в base64. Если данный параметр не задан, то используется pull стратегия нотификации.
digest	string	Да	Специфицируемая «свертка» от документа (8 шестнадцатеричных символов).
ca	string	Нет	Идентификатор Удостоверяющего Центра. Используется, если для Сервис-Партнера сконфигурировано использование нескольких УЦ. Если параметр не передан – используется первый УЦ из списка УЦ ассоциированных с Сервис Провайдером. Параметр не используется

Таблица 2 – Возвращаемые параметры

Название параметра	Тип	Обязательность	Описание
status	string	Да	статус транзакции
transaction_id	string	Нет	Уникальный идентификатор транзакции
cms	string	Нет	Электронная подпись документа в формате Base 64

Таблица 3 – Возможные значения поля Status

Значение	Описание
100	Запрос на подписание отослан на мобильный телефон
200	Отсутствует один или несколько обязательных параметров
201	Один из параметров имеет неверный формат
202	Сертификат для данного клиента не выпущен или отозван или истек
203	Неизвестный идентификатор транзакции
206	Текст для отображения на экране имеет слишком большую длину
207	Неизвестный msisdn
208	Неизвестный код УЦ или УЦ с указанным кодом не авторизован для работы с указанным Сервис-Провайдером.
400	Неизвестный partner_id или используется неизвестный русурс партнера
401	Неизвестный сертификат SSL или сертификат SSL не соответствует парнёру (partner_id).
402	Поле digest не соответствует переданному документу.
476	Sim карта заблокирована
500	Внутренняя ошибка сервера, повторите запрос позже
800	Время жизни транзакции истекло
808	Предыдущая транзакция на подписание не завершена

3.3.3.4. Правила формирования текста показываемого на экране телефона.

Текст, показываемый Абоненту на экране телефона, формируется по следующему алгоритму – показываемый Текст = text + “/n” + digest

Пример:

- поле text = Договор № 12345 от 21.12.2012, количество позиций 23, на сумму 123456.78 руб.

поле digest = A1B2F94D

- показываемый текст:

Договор № 12345 от 21.12.2012, количество позиций 23, на сумму 123456.78 руб.

A1B2F94D

Примечание. Платформа МЭП производит повторное вычисление digest и сверяет с переданным.

3.3.3.5. Правила формирования свертки (поле digest):

1) вычисляется MD5 от представления документа в формате Base 64;

2) в цикле от 0 до 8 вычисляется XOR от I, I+8, I+16, I+24;

3) полученные шестнадцатеричные цифры конкатенируются в строковом представлении.

Пример:

- MD5 от представления документа в формате Base 64 = 1234567890ABCDEFABCDEF1234567890 (см. табл. 4);

- результат свертки: 1D040C15

Таблица 4

MD5 сумма разбита на 8 групп по 4 символа	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	9	0	A	B	C	D	E	F
	A	B	C	D	E	F	1	2
	3	4	5	6	7	8	9	0
Операция XOR по столбцам (группам)	XOR (1,9,A,3)	XOR (2,0,B,4)	XOR (3,A,C,5)	XOR (4,B,D,6)	XOR (5,C,E,7)	XOR (6,D,F,8)	XOR (7,E,1,9)	XOR (8,F,2,0)
Результат операции XOR	1	D	0	4	0	C	1	5

3.3.4. Active Directory (в части обеспечения единых параметров авторизации пользователей).

Настройка взаимодействия с Active Directory производится после установки и настройки программного обеспечения серверов.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Для взаимодействия с Active Directory используется библиотека PHP – php-ldap.

Для настройки необходимо указать параметры подключения к Active Directory в конфигурационном файле db.ini раздела [ldap], находящемся на сервере в папке cfg.

3.3.5. Telegram (в части отправки уведомлений и файлов документов).

Настройка взаимодействия с системой мгновенного обмена сообщениями Telegram осуществляется путем установки протокола Server Message Block (SMB - далее Samba), а также созданием SSL сертификата для сайта. Действия по установке и настройке приведены в приложениях 3, 4.

4. ПРОВЕРКА ПРОГРАММЫ

4.1. Порядок формирования и проверки контрольных сумм СЭД

4.1.1. Формирование и проверка КС информации, записанной на поставочном ЭН СЭД, осуществляется на произвольном компьютере с установленной ОС типа Astra Linux.

КС подтверждает подлинность и целостность информации поставочного ЭН СЭД, включающего как программные файлы СЭД на исходном интерпретируемом языке и в виде дистрибутива, так и текстовые файлы отчётных документов по выполнению ГК.

4.1.2. Подсчёт КС ЭН СЭД выполняется в следующей последовательности:

- установить ЭН в устройство чтения оптических компакт-дисков;
- выполнить монтирование файловой системы устройства чтения компакт-дисков, дважды нажав в появившемся окне кнопку «Монтировать»;
- запустить «Терминал» и перейти в папку компакт-диска командой cd /media/cdrom;
- набрать в командной строке tar –c * | md5sum и нажать клавишу «Enter»;
- ожидать завершения работы программы подсчета КС (до 3 мин.) – выдачи на экран компьютера подсчитанного значения КС;
- произвести размонтирование файловой системы устройства чтения оптических компакт-дисков, выполнив команду cd;umount /media/cdrom;
- извлечь ЭН из устройства чтения оптических компакт-дисков.

4.1.3. Проверка КС ЭН СЭД выполняется в следующей последовательности:

- сравнить подсчитанное значение КС со значением КТ, указанным на маркировке, Этикетке и Информационно-удостоверяющем листе ЭН;
- при совпадении этих значений КС проверка считается успешно выполненной;
- в противном случае следует повторно выполнить подсчёт и проверку КС ЭН СЭД;

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

- в случае повторного несовпадения значений КС составляется рекламационный Акт и поставочный ЭН СЭД возвращается поставщику изделия.

4.2. Проверка работоспособности СЭД

4.2.1. Проверка работоспособности СЭД выполняется:

- после начальной установки и наладки СЭД на объекте применения;
- периодически в соответствии с установленным регламентом технического обслуживания (рекомендуется не реже одного раза в год);
- после выявления и устранения отказов СЭД в процессе её функционирования;
- после повторного получения результата проверки о неработоспособности СЭД.

4.2.2. Проверка работоспособности СЭД выполняется при соблюдении следующих условий:

- все технические средства ПТК, участвующие в проверке, должны быть исправны и работать в штатных режимах;
- всё программное обеспечение ПТК, участвующее в проверке, должно быть установлено и настроено в соответствии с разделом 3;
- персонал, участвующий в проверке, должен иметь соответствующую квалификацию.

4.2.3. Перед проверкой работоспособности СЭД необходимо создать тестовую резервную копию программных файлов СЭД и базы данных в соответствии с разделом 6.

4.2.4. Проверка работоспособности СЭД осуществляется методом экспресс-тестирования путём последовательного выполнения следующих действий:

1) войти в главное меню СЭД;

2) провести последовательную проверку «активизации» всех кнопок подменю, расположенных по горизонтали и по вертикали панели инструментов главного меню СЭД.

Оценка результатов проверки:

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

- отсутствие сообщений об ошибках на АРМ системного программиста при каждой «активизации» кнопок подменю подтверждает работоспособность СЭД;

- при «зависании» СЭД (запускаемые кнопки главного меню СЭД не «активизируются») или поступлении любого сообщения об ошибке на АРМ системного программиста СЭД считается неработоспособной и подлежит оперативной повторной проверке.

4.2.5. При оперативной повторной проверке СЭД необходимо выполнить действия согласно п. 4.2.4.

Оценка результатов оперативной повторной проверки:

- отсутствие сообщений об ошибках на АРМ системного программиста при каждой «активизации» кнопок подменю подтверждает работоспособность СЭД;

- при «зависании» СЭД или поступлении любого сообщения об ошибке на АРМ системного программиста СЭД считается неработоспособной и подлежит полной повторной проверке.

4.2.6. При полной повторной проверке СЭД необходимо:

- повторно проверить подлинность и целостность поставочного ЭН СЭД путём формирования и проверки его КС в соответствии с подразделом 4.1;

- повторно выполнить процедуры по установке и настройке СЭД в соответствии с подразделами 3.2 и 3.3;

- выполнить действия согласно п. 4.2.4.

Оценка результатов полной повторной проверки:

- отсутствие сообщений об ошибках на АРМ системного программиста при каждой «активизации» кнопок подменю подтверждает работоспособность СЭД;

- при «зависании» СЭД или поступлении любого сообщения об ошибке на АРМ системного программиста СЭД считается неработоспособной, о чём составляется рекламационный Акт и поставочный ЭН СЭД возвращается поставщику изделия.

5. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

5.1. СЭД предполагает непрерывную круглосуточную работоспособность, за исключением периодов времени проведения профилактических и восстановительных работ.

СЭД обеспечивает автоматическое восстановление своих функций и данных при возникновении следующих нештатных ситуаций:

- при сбоях в электроснабжении ПТК (восстановление работоспособности СЭД осуществляется перезагрузкой всего программного обеспечения ПТК);

- при ошибках в работе оборудования ПТК, кроме отказов носителей данных и программ (восстановление работоспособности СЭД возлагается на ОС);

- при ошибках, связанных с работой ОПО и СЭД (восстановление работоспособности СЭД возлагается на ОС и СЭД соответственно).

5.2. Для обеспечения надёжного восстановления работоспособности в СЭД реализуются следующие способы резервного копирования:

1) резервное копирования образов виртуальных машин и их файлов, а также их восстановление из графического интерфейса средствами системы виртуализации ОС;

2) резервное копирование в ОС.

5.2.2. Для резервногое копирования всей СЭД в ОС необходимо:

1) выполнить команду:

создание архива файлов системы

sudo tar cvpzf /backup.tgz /var/www

2) с правами суперпользователя (sudo) создать тарбол (tar с ключом c) и заархивировать его архиватором gz (ключ z).

В итоге получается в корне полный архив СЭД в файле backup.tgz

Для разворачивания данного архива необходимо выполнить команду:

tar xvpfz /backup.tgz –C /

Благодаря ключу p СЭД сохраняется в исходном состоянии и с исходными правами доступа к функциям и данным.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

5.2.3. Поскольку заранее не известно какого типа данные и, соответственно, насколько плотно они сожмутся – требуется иметь на жёстком диске, как минимум, 50% свободного места.

Для проверки заполнения диска необходимо выполнить команду:

Df

5.2.4. Для создания архива БД необходимо выполнить команду:

pg_dump -h localhost -p 5432 -U <имя_пользователя_бд> -F c -C -b -v -f <имя_архива> <имя_базы_данных>

5.2.5. Процедуры восстановления СЭД из резервной копии аналогичны процедурам её установки и настройки, приведённым в приложениях 1, 2.

6. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

6.1. Во время выполнения процессов установки, проверки, настройки и функционирования СЭД системный программист (администратор) СЭД получает на свой АРМ служебные сообщения:

- от ОС (согласно её ПД) о состоянии процессов управления функционированием технических и программных средств среды функционирования СЭД и самой СЭД;

- от модулей СЭД о состоянии процессов их функционирования.

6.2. Получаемые Администратором СЭД служебные сообщения разделяются, по признаку причины появления и действия Администратора, на две категории:

- сообщения информационного характера о штатном ходе процессов установки, проверки, настройки и функционирования СЭД, не требующие вмешательства Администратора в исправление хода этих процессов;

- сообщения о нарушениях штатного хода процессов установки, проверки, настройки и функционирования СЭД (сбои и отказы работы технических и программных средств среды функционирования СЭД и самой СЭД, некорректные действия пользователей и самого Администратора СЭД и др.), требующие вмешательства администратора в исправление нарушений в ходе этих процессов.

6.3. Сводный состав основных типовых сообщений, получаемых Администратором СЭД, с указанием их текста, причины и требуемых действий Администратора, приведён в табл. 5.

Таблица 5

Сообщение об ошибке	Причина появления	Действие Администратора СЭД	Правильный результат
This site can’t be reached	Нет связи, не работает web server apache.	Проверить файл с сервером. Установить или включить Apache. Проверка загрузки статического файла sed.citis.ru/img/access-forbidden.png	Картинка с собакой
Таблица со списком	Не отключен модуль	Отключить модуль	Forbidden

Сообщение об ошибке	Причина появления	Действие Администратора СЭД	Правильный результат
файлов в каталоге	autoindex.	autoindex. Проверка что модуль autoindex apache отключен sed.citis.ru/cfg	You don't have permission to access /cfg/ on this server.
Response headers Apache/	Не настроены константы ServerTokens и ServerSignature конфигурационного файла apache. Выдается подробная информация о системе и версии apache.	Настроить константы ServerTokens и ServerSignature. Проверка заголовков HTTP Необходимо открыть инструменты разработчика в браузере (Ctrl+Shift+I для Google Chrome), вкладку Network, выбрать любой файл	Response headers Server: Apache
This page isn’t workinglocalhost is currently unable to handle this request. HTTP ERROR 500. В логе ошибок apache запись: Fatal error: Maximum execution time of 30 seconds exceeded in /var/www/sed-citis/az/server/php/templater-cache.php on line 11	Неправильно настроен пользователь папки cache.	Проверить пользователя папки cache, который должен быть www-data Проверка загрузки страницы авторизации sed.citis.ru	Страница авторизации
Couldnt connect to database.	Нет подключения к postgresql.	Настроить подключение к postgresql в cfg/db.ini. Проверка загрузки страницы авторизации sed.citis.ru	Страница авторизации
Файл не загружается	Неправильно настроен пользователь папки storage/docfiles.	Проверка загрузки pdf файлов размером до 2 Мбайт Проверить пользователя папки storage/docfiles, который должен быть www-data	Файл загружается
Файл не загружается	По умолчанию максимальный размер загружаемых файлов 2 Мбайта	В php.ini изменить директивы upload_max_filesize и post_max_size	Файл загружается

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

Сообщение об ошибке	Причина появления	Действие Администратора СЭД	Правильный результат
		Проверка загрузки файлов размером от 2 до 500 Мбайт	
Файл не загружается	Неправильно настроен пользователь папки cabinet/userPhoto	Проверить пользователя папки cabinet/userPhoto, который должен быть www-data Проверка загрузки фотографии пользователя	Файл загружается
Файл не загружается	Неправильная настройка конвертора в файле db.ini, директива docsaner.	Проверить настройку конвертора в файле db.ini, директива docsaner. Проверить установку libreoffice Проверка загрузки doc файла	Файл загружается

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применены следующие обозначения и сокращения

АРМ	–	автоматизированные рабочие места
БД	–	база данных
ДООУ	–	документационное обеспечение организационного управления
ИС	–	информационная система
МЭДО	–	система межведомственного электронного документооборота федеральных органов исполнительной власти
МЭП	–	мобильная электронная подпись (с мобильного устройства)
ОРД	–	организационно-распорядительный документ
ОПО	–	общее программное обеспечение
ОС	–	операционная система
ПИК	–	программный инструментальный комплекс
ПТК	–	программно-технический комплекс
СОА	–	сервис-ориентированная архитектура
СПО	–	специальное программное обеспечение
СУБД	–	система управления базами данных
СЭД	–	система электронного документооборота
ТК	–	транспортный контейнер
ЭД	–	электронный документ
ЭН	–	электронный носитель
ЭП	–	электронная подпись
Active Directory	–	Службы активных каталогов для ОС

ПРИЛОЖЕНИЕ 1

(обязательное)

БАЗОВАЯ УСТАНОВКА И НАСТРОЙКА ОБЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА КОМПЛЕКСНОМ СЕРВЕРЕ

Необходимо выполнить следующие процедуры.

1) отключить ipv6

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.lo.disable_ipv6=1
sudo sysctl -p
```

2) установить Apache 2.4:

```
sudo apt-get install apache2
```

3) выполнить резервное копирование конфигурационного файла:

```
sudo cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf.bak
```

4) выполнить копирование содержимого в файл apache.conf

```
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#       /etc/apache2/
#       |-- apache2.conf
#       |       `--  ports.conf
#       |-- mods-enabled
#       |       |-- *.load
#       |       `-- *.conf
#       |-- conf-enabled
#       |       `-- *.conf
#       `-- sites-enabled
#               `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
```

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

```
#   together by including all remaining configuration files when starting up the
#   web server.
#
# * ports.conf is always included from the main configuration file. It is
#   supposed to determine listening ports for incoming connections which can be
#   customized anytime.
#
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/
#   directories contain particular configuration snippets which manage modules,
#   global configuration fragments, or virtual host configurations,
#   respectively.
#
#   They are activated by symlinking available configuration files from their
#   respective *-available/ counterparts. These should be managed by using our
#   helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See
#   their respective man pages for detailed information.
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.


# Global configuration
#

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"

#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
#Mutex file:${APACHE_LOCK_DIR} default

#
# The directory where shm and other runtime files will be stored.
#
DefaultRuntimeDir ${APACHE_RUN_DIR}

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}
#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300
#
# KeepAlive: Whether or not to allow persistent connections (more than
```

```
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log
#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn

# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf


# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
```

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

```
# access here, or in any related virtual host.
<Directory />
	Options FollowSymLinks
	AllowOverride None
	Require all denied
</Directory>

<Directory /usr/share>
	AllowOverride None
	Require all granted
</Directory>

<Directory /var/www/>
	Options FollowSymLinks
	AllowOverride All
	Require all granted
</Directory>

#<Directory /srv/>
#	Options Indexes FollowSymLinks
#	AllowOverride None
#	Require all granted
#</Directory>
# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives.  See also the AllowOverride
# directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
	Require all denied
</FilesMatch>


#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.
# Include generic snippets of statements
```

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

```
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

5) включить модуль преобразования URL:

```
sudo a2enmod rewrite headers
```

6) отключить модуль индексирования

```
sudo a2dismod autoindex
```

7) поправить конфигурации security.conf:

```
sudo nano /etc/apache2/conf-available/security.conf
```

8) поправить константы:

```
ServerTokens Prod
ServerSignature Off
```

9) перезагрузить Apache 2.4:

```
sudo systemctl restart apache2
```

10) установить PHP 8.1 и расширения:

```
sudo apt-get install php8.1 php-pear libapache2-mod-php8.0 php8.1-curl php8.1-gd php8.1-ldap
php8.1-pgsql php8.1-mbstring php8.1-zip php8.1-imagick php8.1-imap php8.1-intl php8.1-xmlrpc
php8.1-soap php8.1-xml
```

11) изменить параметры php.ini

```
upload_max_filesize = 500M post_max_size = 500M
```

12) заменить содержимое файла 000-default.conf:

```
sudo nano /etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/sed-citis
```

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

```
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
        # <Location /svn>
        #    DAV svn
        #    SVNParentPath /var/lib/svn
        #    AuthType Basic
        #    AuthName "Your repository name"
        #    AuthUserFile /etc/subversion/passwd
        #    Require valid-user
        #</Location>
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

13) установить дополнительные утилиты:

```
sudo apt-get install poppler-utils netpbm imagemagick libreoffice
```

14) создать рабочую папку:

```
sudo mkdir -p /var/www/sed-citis
```

15) разархиваровать скачанный архив в созданную папку, а далее задать права

```
sudo chmod -R 755 /var/www/sed-citis
sudo chown -R www-data:www-data cache storage cabinet/userPhoto
sudo chmod -R 777 /var/www/sed/cache
sudo chmod -R 777 /var/www/sed/storage
```

16) установить PostgreSQL:

```
sudo apt-get install postgresql
```

17) отредактировать /etc/postgresql/{версия}/main/postgresql.conf

```
max_connections =300
ssl = off
```

18) создать нового пользователя базы данных (БД) с именем *www-data* и *ai-modules* и паролем доступа к БД.

19) создать пустую БД с наименованием *edfs*.

20) выполнить копирование 4 файлов: *en.affix, en.dict, ru.affix, ru.dict* в */usr/share/postgresql/{версия Postgresql}/tsearch_data*.

21) для настройки конфигурации 'ru' необходимо выполнить следующие команды

```
sudo -u postgres psql postgres
CREATE TEXT SEARCH DICTIONARY ispell_ru (
template  =  ispell,
 dictfile  =  ru,
 afffile  =  ru,
 stopwords =  russian
);
CREATE TEXT SEARCH DICTIONARY ispell_en (
  template  = ispell,
  dictfile  = en,
  afffile  = en,
  stopwords = english
);
CREATE TEXT SEARCH CONFIGURATION ru ( COPY = russian );
ALTER TEXT SEARCH CONFIGURATION ru ALTER MAPPING FOR word, hword, hword_part WITH ispell_ru, russian_stem;
ALTER TEXT SEARCH CONFIGURATION ru ALTER MAPPING FOR asciiword, asciihword, hword_asciipart WITH ispell_en, english_stem;
```

22) загрузить в созданную базу резервную копию, скачанную в архиве

```
pg_restore -h localhost -p 5432 -U postgres -d edfs /{путь до резервной копии}/bd-clean.edfs
```

23) настроить imagemagick

```
sudo nano /etc/ImageMagick-6/policy.xml

<policy domain="coder" rights="none" pattern="EPHEMERAL" />
<policy domain="coder" rights="none" pattern="HTTPS" />
<policy domain="coder" rights="none" pattern="MVG" />
<policy domain="coder" rights="none" pattern="MSL" />
<policy domain="coder" rights="none" pattern="TEXT" />
<policy domain="coder" rights="none" pattern="SHOW" />
<policy domain="coder" rights="none" pattern="WIN" />
<policy domain="coder" rights="none" pattern="PLT" />
<policy domain="path" rights="none" pattern="@*" />
<policy domain="coder" rights="write|read" pattern="PDF" />
```

24) установить Крипто-Про 4

ПРИЛОЖЕНИЕ 2

(обязательное)

БАЗОВАЯ УСТАНОВКА И НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА СЕРВЕРЕ КОНВЕРТИРОВАНИЯ ДАННЫХ ДЛЯ ПРЕДПРОСМОТРА

Необходимо выполнить следующие процедуры.

1. Установка пакета офисных приложений не ниже Microsoft Office 2010.

2. Разархивирование файла converter.zip, находящегося в архивной версии программных файлов СЭД, в корень диска.

3. Запуск на исполнение «Выполнить с помощью PowerShell» файл conv.ps1, находящийся в папке /converter/cmd/.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

ПРИЛОЖЕНИЕ 3

(обязательное)

УСТАНОВКА ПРОТОКОЛА SERVER MESSAGE BLOCK

Необходимо выполнить следующие процедуры.

1. Установить на сервере-шлюзе Samba КОМАН:

sudo apt-get install samba

2. Разрешить автостарт сервиса:

sudo systemctl enable smbd

3. Проверить, что сервис запустился:

sudo systemctl status smbd

4. Создать пользователя для доступа к папке:

sudo useradd telegra

5. Назначить пользователю пароль:

sudo passwd telegra

6. Дважды ввести пароль.

7. Создать пользователя в samba:

sudo smbpasswd -a telegra

8. Создать папку, доступ к которой будет иметь ограниченное количество пользователей.

9. Открыть конфигурационный файл samba:

sudo nano /etc/samba/smb.conf

10. Добавить настройку для новой папки в конец файла, закомментить строчки с принтерами (если они не нужны):

[telegram]

comment = Private Folder

path = /var/www/telegram

public = no

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

writable = no

read only = yes

guest ok = no

valid users = admin, telegra

write list = admin, telegra

create mask = 0777

directory mask = 0777

force create mode = 0777

force directory mode = 0777

inherit owner = yes

Примечание:

path = /data/private — использовать новый путь до папки.

writable = no и read only = yes — в данном примере разрешить запись в каталог только некоторым пользователям. Поэтому общие настройки, разрешающие запись в папку, должны быть запрещены.

valid users — список пользователей, которым разрешено подключаться к каталогу. В данном примере разрешения работают для пользователей admin, telegra, а также для всех, кто входит в группу privateusers.

write list — список пользователей, которые имеют доступ к папке на чтение и запись. В данном примере это разрешено только для пользователей admin и telegra.

inherit owner — опция позволяет включить наследование владельца при создании папок и файлов.

Для разрешения полного доступа к каталогу определенным пользователям (без разделения на тех, кто может только читать и тех, кто может также писать в папку) опцию *write list* можно не указывать, а опции *writable* и *read only* оставить как описано выше.

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

11. Создать каталог для новой папки:

sudo mkdir /var/www/telegram

12. Задать права на созданный каталог:

sudo chmod 777 /var/www/telegram

13. Для применения настроек перезапустить samba:

sudo systemctl restart smbd

14. Проверить возможность работы с новым каталогом.

15. На сервере СЭД добавить строку в конец файла fstab, меняя password на созданный пароль:

sudo nano /etc/fstab

//192.168.123.103/telegram/storage/outbox /var/www/sed-citis/storage/exchange/telegram/outbox cifs user=telegra,pass=password,iocharset=utf8,noperm,uid=www-data,gid=www-data,dir_mode=0777,file_mode=0777,auto 0 0

16. Далее монтировать:

sudo mount -a

17. Если ошибка: *mount error(95): Operation not supported*,

то необходимо изменить строку:

sudo nano /etc/fstab

//192.168.123.103/telegram/storage/outbox /var/www/sed-citis/storage/exchange/telegram/outbox cifs user=telegra,pass=password,iocharset=utf8,vers=2.0,noperm,uid=www-data,gid=www-data,dir_mode=0777,file_mode=0777,auto 0 0

ПРИЛОЖЕНИЕ 4

(обязательное)

СОЗДАНИЕ SSL СЕРТИФИКАТА ДЛЯ САЙТА

Сайт, для которого необходимо создать SSL сертификат, должен уже быть доступен без HTTPS на порту 80. Поэтому его виртуальный хост Apache должен уже быть настроен.

Ниже будет показано, как получать сертификат для сайта *edu.citis.ru*.

1. Для примера нужно создать такой виртуальный хост:

sudo nano /etc/apache2/sites-available/edu-citis-ru.conf

*<VirtualHost *:80>*

ServerName edu.citis.ru

ServerAlias www.edu.citis.ru

ServerAdmin webmaster@localhost

DocumentRoot /var/www/

ErrorLog ${APACHE_LOG_DIR}/error.log

CustomLog ${APACHE_LOG_DIR}/access.log combined

RewriteEngine on

RewriteCond %{SERVER_NAME} =edu.citis.ru [OR]

RewriteCond %{SERVER_NAME} =www.edu.citis.ru

RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]

</VirtualHost>

2. Выйти, сохраняя изменения.

3. Клиент Lets Encrypt называется Certbot. Он доступен в официальных репозиториях. Для установки следует выполнить команды:

sudo apt install certbot python-certbot-apache

4. Если последний пакет не будет найден, необходимо установить *python3-certbot-apache*.

5. Сгенерировать сертификат:

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

sudo certbot certonly --apache -d edu.citis.ru -d www.edu.citis.ru

6. При первом запуске утилита предложит указать *E-mail* адрес для отправки уведомления о необходимости обновить сертификат и новости, а также попросит принять лицензионное соглашение.

7. Появится окно с вопросом о возможности передать ваш адрес их партнёрам. Ответить *No*. Только после этого начнётся генерация сертификата.

8. Программа сообщит, что сертификат сохранён в папке */etc/letsencrypt/live/edu.citis.ru/* и его можно использовать.

9. Папка */etc/letsencrypt/live/edu.citis.ru* будет содержать четыре файла:

cert.pem - файл сертификата, его необходимо прописать в параметре *SSLCertificateFile*;

chain.pem - файл цепочки сертификата, обычно прописывается в параметре *SSLCertificateChainFile*;

privkey.pem - приватный ключ сертификата, должен быть прописан в *SSLCertificateKeyFile*;

fullchain.pem - в нём объединено содержимое *cert.pem* и *chain.pem*, можно использовать вместо этих обоих файлов.

Необходимо сгенерированные файлы перенести в другую папку (до текущей папки нет доступа у апача):

sudo mkdir /etc/apache/ssl

sudo mv /etc/letsencrypt/live/edu.citis.ru/ /etc/apache/ssl/**

Для обычного сайта виртуальный хост существует.

10. Далее необходимо создать виртуальный хост для SSL версии. Для этого кроме стандартных настроек нужно добавить четыре параметра.

SSLEngine on

SSLCertificateFile /путь/к/сертификату.pem

SSLCertificateChainFile /путь/к/сертификату/цепочки.pem

SSLCertificateKeyFile /путь/к/приватному/ключу.pem

Например:

Порядковый номер изменения	*Подпись лица*	*Дата внесения изменений*

sudo nano /etc/apache2/sites-available/edu-citis-ru-ssl.conf

*<VirtualHost *:443>*

ServerName edu.citis.ru

ServerAlias www.edu.citis.ru

ServerAdmin webmaster@localhost

DocumentRoot /var/www/

ErrorLog ${APACHE_LOG_DIR}/error.log

CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on

SSLCertificateFile /etc/letsencrypt/live/edu.citis.ru/cert.pem

SSLCertificateChainFile /etc/letsencrypt/live/edu.citis.ru/chain.pem

SSLCertificateKeyFile /etc/letsencrypt/live/edu.citis.ru/privkey.pem

</VirtualHost>

Данной конфигурации достаточно для начала функционирования.

11. Затем необходимо активировать виртуальный хост:

sudo a2ensite edu-citis-ru-ssl

12. Обязательно следует включить модуль для поддержки SSL:

sudo a2enmod ssl

13. Далее следует проверить работоспособность, открыв домен в браузере.

14. Чтобы добавить больше безопасности, можно указать, какие протоколы SSL следует использовать. Например, для того чтобы отключить SSLv2 и SSLv3, а также TLS ниже 1.2 следует добавить:

sudo nano /etc/apache2/sites-available/edu-citis-ru-ssl.conf

SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в документе*	*№ Документа*	*Входящий № сопроводительного документа и дата*	*Подпись*	*Дата*
	измененных	*замененных*	*новых*	*аннулированных*					