IV. ТЕХНИЧЕСКАЯ ЧАСТЬ ДОКУМЕНТАЦИИ

Технические требования
на выполнение работ и оказание услуг по

тиражированию Единой автоматизированной системы отделений почтовой связи (ЕАС ОПС) ФГУП «Почта России».

1. СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Полное наименование системы

Полное наименование: Единая автоматизированная система отделений почтовой связи. Краткое наименование: ЕАС ОПС, Система.

1.2. Заказчик

Федеральное государственное унитарное предприятие «Почта России» (далее - ФГУП «Почта России»).

1.3. Назначение документа

Настоящие технические требования (далее – ТТ) определяют базовые требования Заказчика к выполнению работ и оказанию услуг по тиражированию Единой автоматизированной системы отделений почтовой связи на подразделения филиальной сети ФГУП «Почта России».

1.4. Перечень документов, на основании которых проводятся работы/услуги

Основанием для выполнения работ и оказания услуг по тиражированию ЕАС ОПС являются следующие документы:

- Договор № ____ от «__» _____ 20__ года на оказание услуг по теме «Тиражирование единой автоматизированной системы отделений почтовой связи» (далее «Договор»).
- СТАНДАРТ «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений ФГУП «Почта России" Приложение 2.2 к техническим требованиям.

1.5. Порядок оформления результатов работ/услуг

Порядок оформления и предъявления результатов услуг соответствует требованиям комплекса стандартов и руководящих документов на автоматизированные Системы:

- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные Системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»;
- ГОСТ 34.602-89 «Информационная технология. Техническое задание на создание автоматизированной Системы»;
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные Системы. Термины и определения»;
- ГОСТ 34.601-90 «Информационная технология. Автоматизированные Системы. Стадии создания»;
- РД 50-680-88 «Методические указания. Автоматизированные Системы. Основные положения»;
- РД 50-34.698-90 «Методические указания. Автоматизированные Системы. Требования к содержанию документов»;
- Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;

– ГОСТ Р ИСО/МЭК 12207-99 «Информационная технология. Процессы жизненного цикла программных средств».

Вся отчетная документация должна быть на русском языке.

1.6. Определения, обозначения и сокращения

В Таблице 1 приведены основные обозначения и сокращения, использованные в настоящих Технических требованиях.

Таблица 1. Определения, обозначения и сокращения

Сокращение	Расшифровка
API	Application Programming Interface – Интерфейс программирования приложений (специфицированный программный интерфейс): набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением для использования во внешних по отношению к этому приложению программных продуктах
EMS – ПОЧТА РОССИИ	EMS «Почта России» - филиал ФГУП «Почта России»
ESB	Enterprise Service Bus – сервисная шина предприятия по передаче данных между отдельными узлами
ITSM	IT Service Management, управление ИТ-услугами
АРМ	Автоматизированное рабочее место
АС	Автоматизированная Система
АСЦ	Автоматизированный сортировочный центр
АУП	Аппарат Управления Предприятием
БСО	Бланки строгой отчетности
ГЦМПП	Главный центр магистральных перевозок почты - филиал ФГУП «Почта России»
ЕАС ОПС	Единая автоматизированная система отделений почтовой связи
ЗПО (ГЗПО)	Знаки почтовой оплаты
ИС	Информационные системы
ИТ	Информационные технологии
Ключевой пользователь	занятый по своему прямому функционалу сотрудник структурного подразделения по организации эксплуатации сети почтовой связи Предприятия и производственных технологий, назначенный ответственным за запуск и сопровождение ЕАС ОПС в подразделениях Предприятия. МОПС – мобильное отделение почтовой связи.
ЛВС	Локально-вычислительные сети
МСЦ	Магистральный сортировочный центр

Сокращение	Расшифровка
НСИ	Нормативно – справочная информация
ОПС	Отделение Почтовой Связи
ОСП	Обособленное структурное подразделение
ПБД	Промежуточная база данных
ПК	Персональный компьютер
ПКТ	Почтово-кассовый терминал
ПО	Программное обеспечение
ПП	Программный продукт
Предприятие	ФГУП «Почта России»
ПТК	Производственно-технологический контур
РИМ	Рекламно-информационные материалы
РПО	Регистрируемые почтовые отправления
СКЗИ	Средство криптографической защиты информации
СУБД	Система управления базами данных
ТМЦ	Товарно-материальные ценности
ТС	Терминал самообслуживания
УФПС	Управление федеральной почтовой связи
ФГУП «ПОЧТА РОС-СИИ»	Федеральное государственное унитарное предприятие «Почта России»

2. НАЗНАЧЕНИЕ СИСТЕМЫ

2.1. Назначение системы

Назначение ЕАС ОПС – обеспечение автоматизации операционной деятельности ОПС ФГУП «Почта России».

2.2. Структура ФГУП «Почта России»

Федеральное государственное унитарное предприятие «Почта России» имеет статус федерального почтового оператора, предоставляет услуги почтовой связи на всей территории Российской Федерации, в том числе универсальные услуги почтовой связи по единым социально-ориентированным тарифам, регулируемым государством.

В структуре ФГУП «Почта России» условно можно выделить четыре основных вертикальных уровня управления:

1. Аппарат управления предприятием (АУП);
2. Филиалы (УФПС, ГЦМПП, EMS, АСЦ);
3. Почтамты, магистральные сортировочные центры (МСЦ);
4. Отделения почтовой связи.

2.3. Цель выполнения работ и оказания услуг

Целью выполнения работ и оказания услуг по тиражированию ЕАС ОПС является запуск ЕАС ОПС в отделениях. Поставленная цель должна быть достигнута за счет:

- разработки плана тиражирования и соответствующих организационно-распорядительных документов;
- развертывания ЕАС ОПС в отделениях почтовой связи, Почтамтах и УФПС в соответствии с планом тиражирования;
- обучения пользователей ЕАС ОПС и обеспечения последующей передачи знаний;
- организации эффективных процедур мониторинга этапов процесса тиражирования.

3. ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

3.1. Краткая характеристика объекта автоматизации

Объектами автоматизации являются Филиалы, почтамты и отделения почтовой связи.

ОПС является основным и самым массовым производственным звеном почтовой связи России, основной задачей которого является предоставление населению, организациям, предприятиям и учреждениям услуг почтовой связи и других договорных услуг.

ОПС по специфике организации производственных процессов в почтовой связи обеспечивают начальный (прием услуг) и конечный этап (выдача услуги) в общем технологическом цикле производства почтовых услуг.

3.2. Описание текущей конфигурации ЕАС ОПС

Система ЕАС ОПС создана на базе платформенного решения путем настройки базовой функциональности и разработки новых программных модулей. ЕАС ОПС разработана в трёх конфигурациях, различающихся по своему назначению, в зависимости от использования на иерархических уровнях объекта автоматизации:

- конфигурация уровня ОПС- ОПС;
- конфигурация «Центральный офис» - Почтамт, УФПС;
- конфигурация «Федеральная штаб-квартира» - АУП.

3.2.1. Конфигурация ЕАС ОПС уровня ОПС

Конфигурация ЕАС ОПС уровня ОПС предназначается для инсталляции Системы непосредственно в ОПС и обеспечивает:

- автоматизацию бизнес-процессов по оказанию услуг и продаже товаров в ОПС;
- автоматизацию внутренних хозяйственных операций ОПС;
- поддержание информационного взаимодействия с вышестоящими ИС Заказчика.

Для решения данных задач, в конфигурацию входят следующие компоненты:

- компоненты клиентского ПО;
- компоненты подсистемы синхронизации;
- компоненты интеграции с внешними системами;
- база данных.

Схема компонентов конфигурации ЕАС ОПС уровня ОПС (см. Рисунок 1. Структурная схема компонентов конфигурации ОПС).

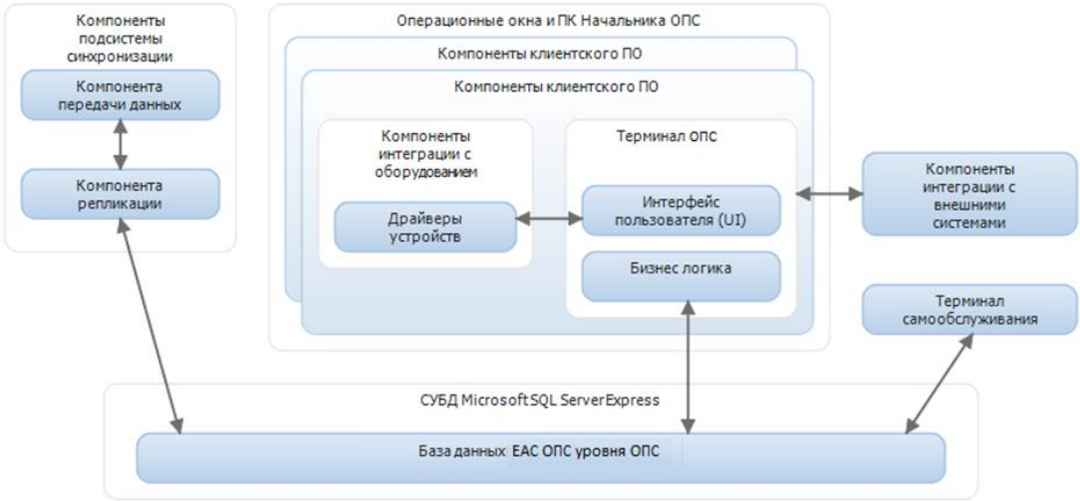


Рисунок 1. Структурная схема компонентов конфигурации ОПС

Клиентское ПО ЕАС ОПС включает в себя функциональные подсистемы ЕАС ОПС реализующие:

- пользовательские интерфейсы;
- бизнес-логику обработки операций (реализация комплексов задач, специально разработанных / адаптированных для работы ОПС);
- интеграции с внешним оборудованием.

Структурная схема функциональных и обеспечивающих подсистем ЕАС ОПС (см. Рисунок 2. Структурная схема компонентов конфигурации ОПС).

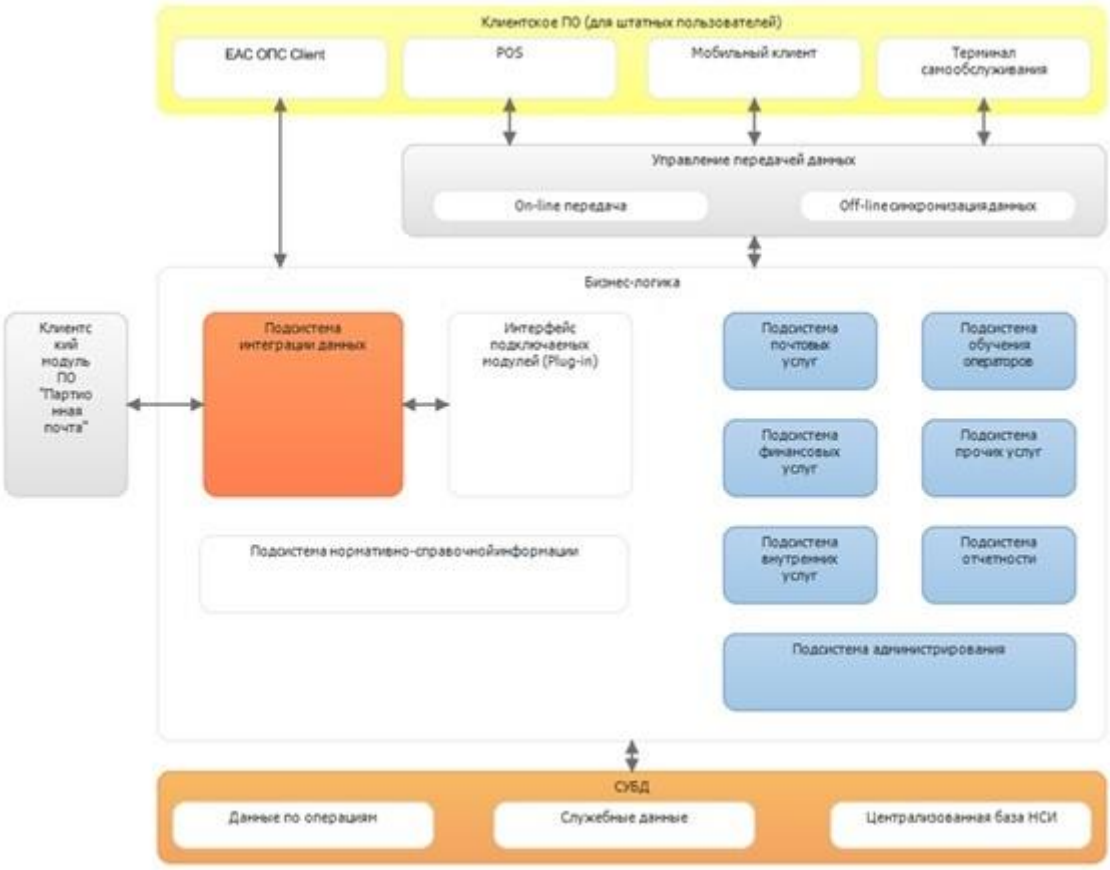


Рисунок 2. Структурная схема компонентов конфигурации ОПС

База данных ЕАС ОПС уровня ОПС представляет собой единую базу данных терминалов в конфигурации ЕАС ОПС уровня ОПС под управлением СУБД, в которой хранятся транзакции, справочники, настройки и служебные данные ОПС.

Инсталляция в ОПС в конфигурации ЕАС ОПС уровня ОПС предусматривается в следующих составах:

- сокращенный (см. Рисунок 3. Схема инсталляции Системы в ОПС (сокращенный состав);
- расширенный (см. Рисунок 4. Схема инсталляции Системы в ОПС (расширенный состав).

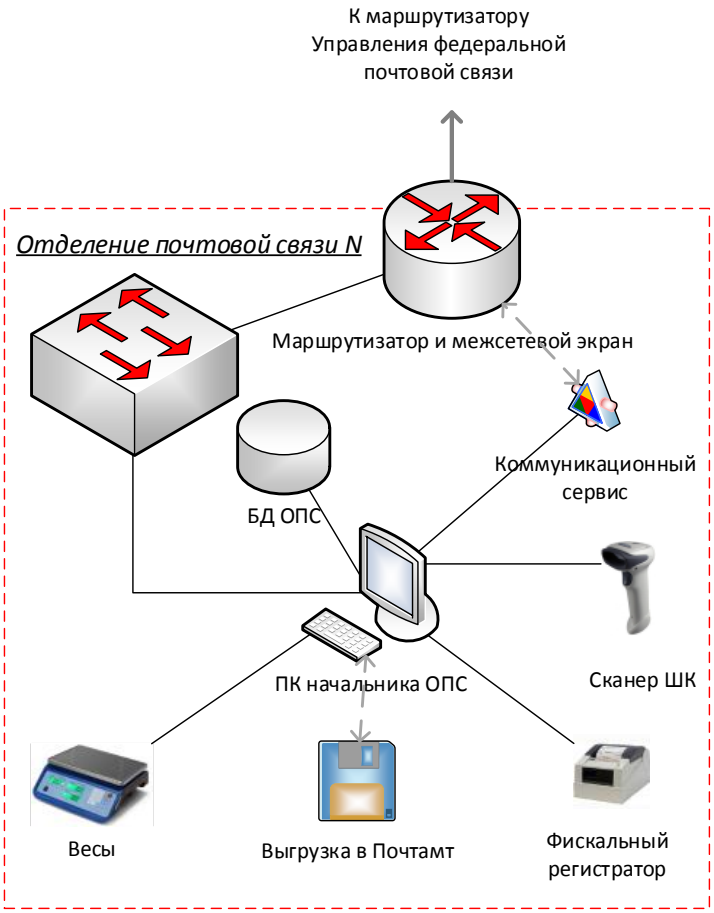


Рисунок 3. Схема инсталляции Системы в ОПС (сокращенный состав)

Сокращенный состав инсталляции поддерживает работу следующих аппаратных средств:

- терминалы ОПС;
- периферийное оборудование;
- коммуникационные сервисы внешних систем;
- сервер базы данных ОПС.

Терминалы ОПС подразделяются на следующие типы, в зависимости от выполняемых задач:

- ПК начальника ОПС;
- почтово-кассовый терминал (ПКТ) операционного окна;
- терминал самообслуживания.

ПК начальника ОПС обеспечивает выполнение следующих задач:

- администрирование, контроль деятельности ОПС;
- обеспечение процессов по ведению внутренней деятельности ОПС;
- синхронизацию баз данных Системы в ОПС и в УПФС.

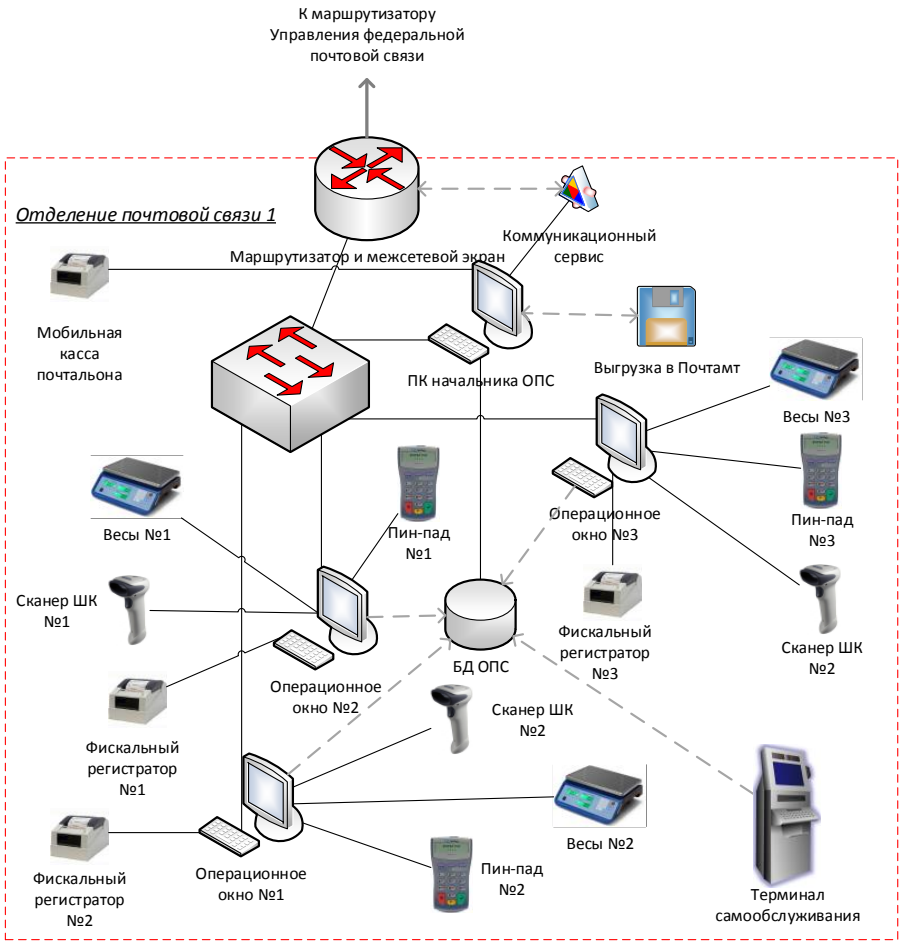


Рисунок 4. Схема инсталляции Системы в ОПС (расширенный состав)

ПК начальника ОПС предполагает также выполнение задач ПКТ операционного окна (при необходимости, в зависимости от количества рабочих мест в ОПС).

ПКТ операционного окна предназначен как для оказания оператором операционного окна фронт-офисных услуг клиентам, так и для обеспечения внутренних процессов (внутренних услуг) по ведению внутренней деятельности.

Терминал самообслуживания предназначен для взаимодействия клиента с ЕАС ОПС без участия оператора.

На ПК начальника ОПС, ПКТ, терминале самообслуживания устанавливаются программные компоненты:

- клиентское ПО системы ЕАС ОПС;
- компоненты подсистемы синхронизации;
- компоненты подсистемы интеграции;
- клиентская часть СКЗИ.

ПК начальника ОПС служит сервером баз данных, который содержит СУБД и базу данных, обеспечивающую доступ, хранение и управление данными инсталляции Системы в ОПС. БД ОПС хранит транзакции, НСИ, настройки и служебную информацию ОПС.

3.2.2. Конфигурация ЕАС ОПС уровня УФПС

Конфигурация ЕАС ОПС уровня УФПС устанавливается в почтамтах и УФПС и предназначена для:

- автоматизации бизнес-процессов УФПС;
- управления нормативно справочной информацией Системы;
- консолидации данных из ОПС (в том числе ввод данных за немеханизированные ОПС);

- формирования оперативной отчетности;
- получение данных в виде журналов регистрации событий;
- регистрация действий операторов;
- формирование консолидированной отчетности по операциям подчиненных подразделений.

Для покрытия данных задач, в конфигурацию входят следующие составные части:

- компоненты клиентского ПО;
- компоненты бизнес-логики;
- база данных ЕАС ОПС;
- компоненты подсистемы синхронизации.

Структурная схема компонентов конфигурации ЕАС ОПС уровня УФПС (см. Рисунок 5. Структурная схема компонентов конфигурации ЕАС ОПС уровня УФПС).

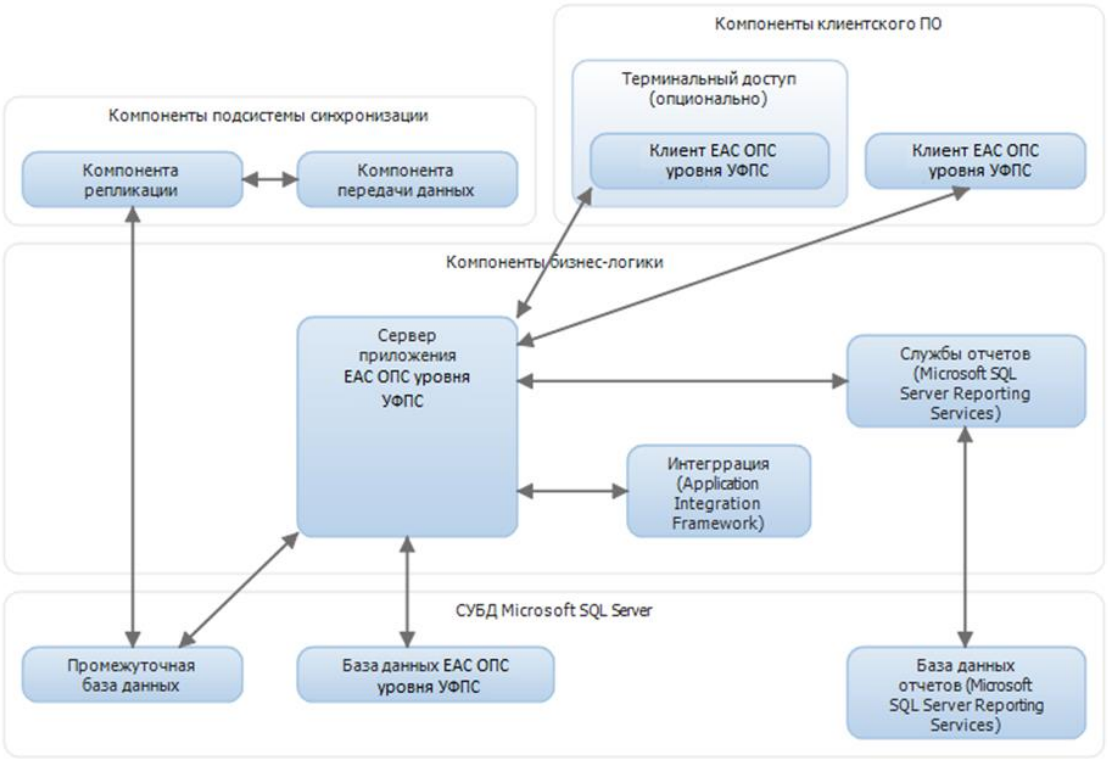


Рисунок 5. Структурная схема компонентов конфигурации ЕАС ОПС уровня УФПС

В ЕАС ОПС представлены следующие компоненты конфигурации ЕАС ОПС уровня УФПС: клиент ЕАС ОПС, сервер приложения ЕАС ОПС, служба отчетов, интеграция с внешними приложениями с использованием интеграционной БД, БД ЕАС ОПС уровня УФПС, БД подсистемы формирования отчетности, промежуточная база данных, компоненты подсистемы синхронизации.

Клиент ЕАС ОПС является 32-х битным Windows-приложением, совместимым с операционной системой MS Windows 7 и выше приложением и предоставляет пользователям интерфейс к данным, к функциональности ЕАС ОПС уровня УФПС.

Сервер приложения ЕАС ОПС уровня УФПС обеспечивает:

- выполнение бизнес-логики ЕАС ОПС уровня УФПС;
- совместный доступ к бизнес-логике и базе данных ЕАС ОПС уровня УФПС;
- интерфейс к базе данных ЕАС ОПС уровня УФПС для формирования оперативных отчетов с использованием службы отчетов Microsoft Reporting Services.

База данных ЕАС ОПС уровня УФПС управляется в среде СУБД, в которой хранятся транзакции, справочники, настройки и служебные данные ЕАС ОПС уровня УФПС.

Платформенным решением поддерживаются версии и редакции СУБД для конфигурации ЕАС ОПС уровня УФПС:

- Microsoft SQL Server 2012, Standard Edition, Enterprise Edition или Business Intelligence Edition;
- Microsoft SQL Server 2008 R2, Standard Edition, Enterprise Edition или Datacenter Edition;
- Microsoft SQL Server 2008, Standard Edition or Enterprise Edition, Service Pack 1.
- Для ЕАС ОПС выбор версии и редакции СУБД производится в соответствие стандарту.

Компоненты подсистемы синхронизации обеспечивают обмен данными между конфигурацией ЕАС ОПС уровня УФПС и конфигурациями ЕАС ОПС уровня ОПС и конфигурациями ЕАС ОПС уровня АУП. Работа компонентов подсистемы синхронизации обеспечивает сбор, передачу и консолидацию операционных данных уровня ОПС.

В задачи инсталляции для Почтамта входит ввод информации за подведомственные немеханизированные ОПС; загрузка/выгрузка информации с/на внешние носители для обеспечения информационного взаимодействия с ОПС без каналов связи или взаимодействия с ОПС с каналами связи в случае их недоступности; получение отчетности по операциям, совершенным подчиненными данному Почтамту ОПС. Инсталляция для Почтамтов разработана на основе конфигурации ЕАС ОПС уровня УФПС платформенного решения (в части операций по подготовке и обработке внешних носителей и получения отчетности).

В задачи инсталляции ЕАС ОПС для УФПС входит управление региональным объемом нормативно-справочной информации, а также получение консолидированной отчетности по операциям подчиненных Почтамтов \ ОПС. Для автоматизации процессов УФПС используется полный набор компонентов конфигурации ЕАС ОПС уровня УФПС.

Схема инсталляции ЕАС ОПС в УФПС на основе конфигурации ЕАС ОПС уровня УФПС (см. Рисунок 7. Схема инсталляции ЕАС ОПС в УФПС).

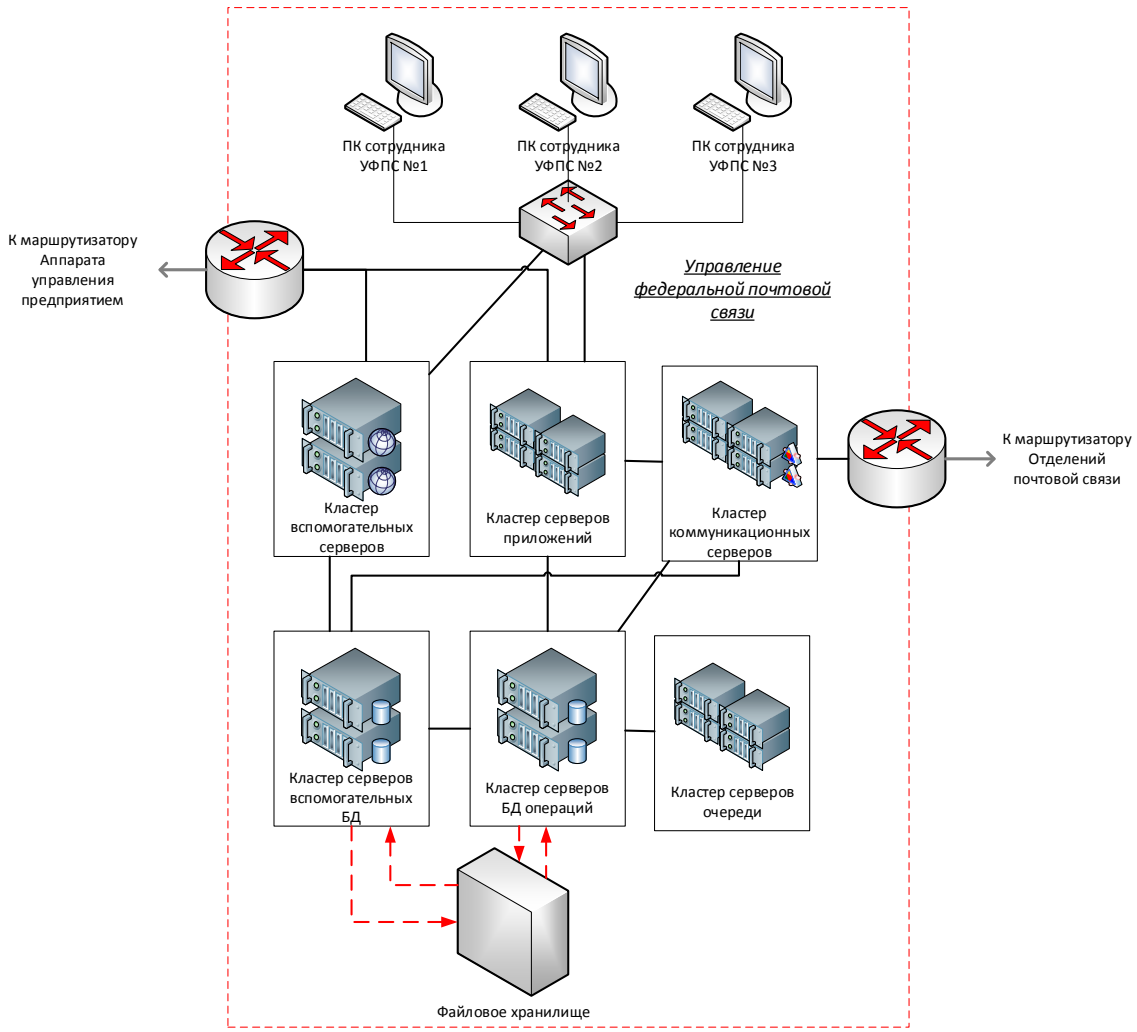


Рисунок 7. Схема инсталляции ЕАС ОПС в УФПС

Инсталляция системы ЕАС ОПС в УФПС базируется на наборе компонентов конфигурации ЕАС ОПС уровня УФПС и обеспечивает поддержку работы следующих аппаратных средств:

- ПК работников;
- кластер серверов приложений;
- кластер серверов очереди;
- кластер коммуникационных серверов;
- кластер серверов БД операций;
- кластер вспомогательных серверов;
- кластер серверов вспомогательных БД;
- файловое хранилище.

На ПК работников устанавливается клиентское ПО инсталляции ЕАС ОПС в УФПС. Клиентское ПО обеспечивает доступ пользователя к компонентам инсталляции ЕАС ОПС в УФПС посредством взаимодействия с сервером приложений ЕАС ОПС, установленным в кластере серверов приложений. Для связи с сервером приложений используется прямое подключение на базе RPC технологии.

Кластер серверов приложений является ключевым аппаратным компонентом инсталляции ЕАС ОПС в УФПС, в котором установлен набор программных компонентов - служб «Сервер приложения ЕАС ОПС». Набор служб ЕАС ОПС работает в виде программного кластера, обеспечивающего реализацию расчетно-вычислительных задач приложения как единая система для пользователя.

Все службы ЕАС ОПС в программном кластере работают с единым хранилищем модели приложения и единой БД операций конфигурации ЕАС ОПС уровня УФПС. Кластер серверов приложений является поставщиком данных и бизнес логики для клиентского ПО, а также поставщиком данных для компонентов репликации подсистемы синхронизации, которые работают на кластере серверов вспомогательных БД.

В кластере серверов очереди, аналогично кластеру серверов приложений, установлен набор программных компонент - служб ЕАС ОПС. С точки зрения функционального назначения, службы ЕАС ОПС кластера серверов очереди выполняют пакетную обработку расчетно-вычислительных задач служб ЕАС ОПС, работающих в кластере серверов приложений. Пакетная обработка представляет из себя асинхронный, не интерактивный серверный процесс, позволяющий обрабатывать множество параллельных задач в рамках одного пакета, на нескольких пакетных службах AOS. Пакетная обработка не является интерактивным процессом и не взаимодействует с клиентским ПО.

В кластере коммуникационных серверов установлены компоненты передачи данных подсистемы синхронизации в конфигурации ЕАС ОПС уровня УФПС для обеспечения двустороннего обмена данными с инсталляциями ЕАС ОПС в ОПС.

Кластер серверов БД операций отвечает за обеспечение доступа, хранения и управление данными инсталляции ЕАС ОПС в УФПС. На кластере серверов БД устанавливается СУБД с развернутыми:

- БД операций УФПС;
- БД модели приложения конфигурации ЕАС ОПС уровня УФПС.

БД операций УФПС хранит транзакции, НСИ, настройки и служебную информацию подразделения УФПС. БД модели приложения содержит все объекты приложения УФПС. Модификации также сохраняются в БД модели приложения.

В кластере вспомогательных серверов установлены компоненты мониторинга и средства визуализации панелей состояния, необходимые для работы ролевых центров платформы. Данные компоненты обеспечивают визуализацию контрольных функций Системы, обеспечивая тем самым вывод информации по состоянию информационного обмена на участках УФПС-ОПС и АУП-УФПС, а также вывод информации по данным журналов ЕАС ОПС, которые поступают с уровня отделений связи.

Кластер серверов вспомогательных БД служит для хранения дополнительной информации, которая напрямую не связана с осуществлением операций в отделениях почтовой связи, но необходима для мониторинга состояния процессов и обеспечения работы вспомогательных функций Системы. К такой информации относятся данные журналов ЕАС ОПС (системные журналы, журналы действий пользователей и журналы рисковых операций[1]).

Система хранения данных обеспечивает хранение совокупной информации, обрабатываемой компонентами инсталляции уровня УФПС, на файловом уровне. Система хранения данных подключается к кластеру серверов БД операций и к кластеру серверов вспомогательных БД по высокоскоростным интерфейсам. Внутренними средствами MS SQL Server обеспечивается выполнение планов мониторинга целостности информации и резервного копирования.

3.2.3. Конфигурация ЕАС ОПС уровня АУП

Конфигурация ЕАС ОПС уровня АУП предназначена для инсталляции Системы в АУП и обеспечивает выполнение следующих задач:

---

[1] Журнал рисковых операций содержит информацию об операциях соотв. определенным критериям, например, операции с клиентами, подозревающимися в экстремистской деятельности. Журналирование осуществляется внутренней функциональностью приложения ЕАС ОПС уровня ОПС.

- управление нормативно справочной информацией Системы;
- получение данных в виде журналов регистрации событий всех ОПС;
- регистрация действий операторов;
- формирование консолидированной отчетности по операциям подчиненных подразделений.

Для покрытия этих задач, в конфигурацию входят следующие составные части:

- компоненты клиентского ПО;
- компоненты бизнес-логики;
- база данных ЕАС ОПС уровня АУП.

Схема компонентов конфигурации ЕАС ОПС уровня АУП (см. Рисунок 8. Структурная схема компонентов конфигурации ЕАС ОПС уровня АУП.

На данной схеме представлены компоненты конфигурации ЕАС ОПС уровня АУП:

- клиент ЕАС ОПС;
- сервер приложения ЕАС ОПС уровня АУП;
- компоненты интеграции с внешними ИС;
- БД ЕАС ОПС уровня АУП.

Клиент ЕАС ОПС уровня АУП аналогичен клиенту ЕАС ОПС уровня УФПС и предоставляет пользователям доступ к данным и к функциональности ЕАС ОПС уровня АУП.

Сервер приложения ЕАС ОПС уровня АУП, решает те же задачи, что и сервер приложения ЕАС ОПС уровня УФПС и выполняет те же функции.

Интеграция с внешними приложениями решает те же задачи, что и интеграция с внешними приложениями конфигурации ЕАС ОПС уровня УФПС и выполняет те же функции.

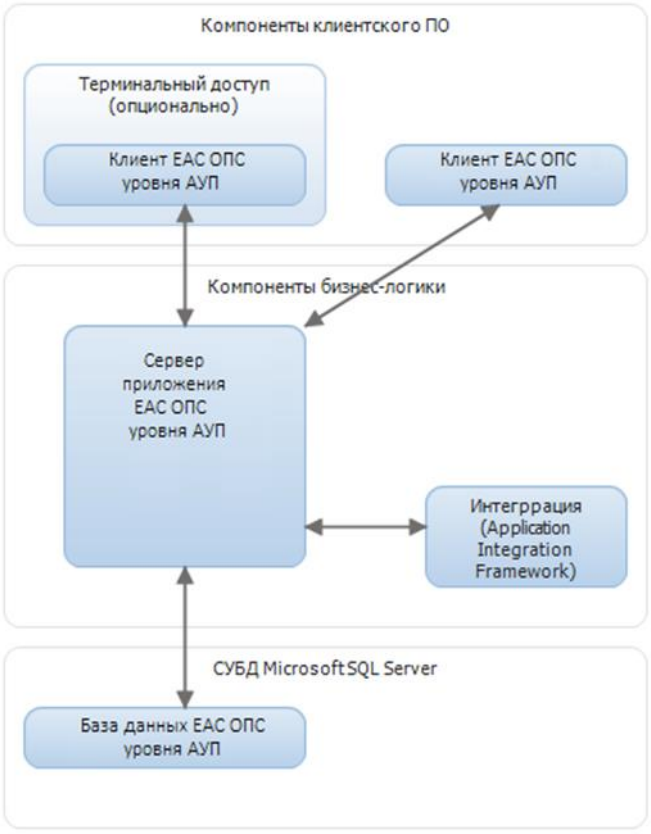


Рисунок 8. Структурная схема компонентов конфигурации ЕАС ОПС уровня АУП

База данных ЕАС ОПС уровня АУП с технической точки зрения аналогична базе данных конфигурации ЕАС ОПС уровня УФПС и хранит транзакции, справочники, настройки и служебные данные конфигурации ЕАС ОПС уровня УФПС.

Схема инсталляции ЕАС ОПС в АУП на основе конфигурации ЕАС ОПС уровня АУП (см. Рисунок 9. Схема инсталляции ЕАС ОПС в АУП).

Инсталляция состоит из следующих аппаратных компонентов:

- ПК сотрудника;
- кластер серверов приложений;
- кластер серверов БД операций;
- кластер вспомогательных серверов;
- кластер серверов вспомогательных БД;
- файловое хранилище.

На ПК работников устанавливается клиентское ПО инсталляции ЕАС ОПС в АУП. Клиентское ПО инсталляции выполняет те же функции, что и клиентское ПО инсталляции УФПС.

Кластер серверов приложений является ключевым аппаратным компонентом конфигурации ЕАС ОПС уровня АУП, в котором установлен набор программных компонент - служб сервера приложений. Набор служб ЕАС ОПС уровня АУП работает в виде программного кластера, обеспечивающего реализацию расчетно-вычислительных задач приложения как единая система для пользователя.

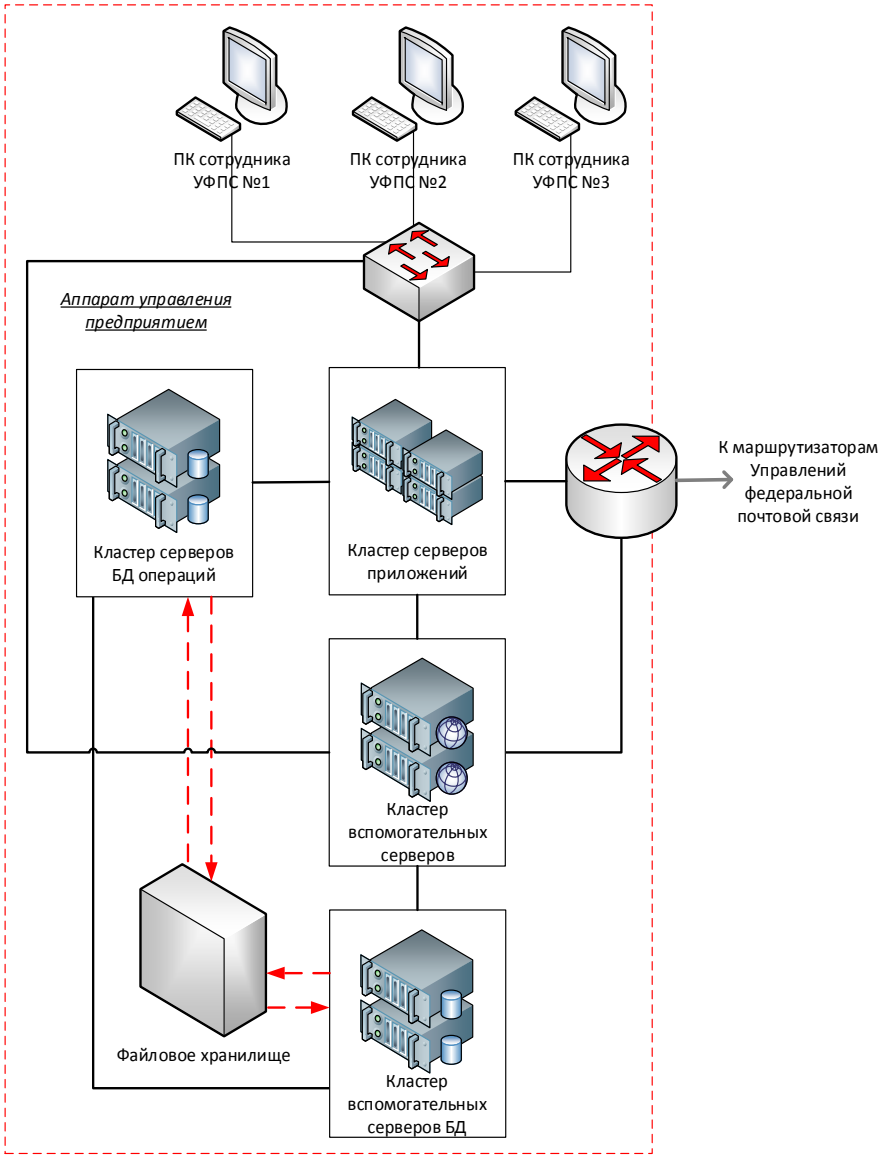


Рисунок 9. Схема инсталляции ЕАС ОПС в АУП

Все службы ЕАС ОПС уровня АУП в программном кластере работают с единым хранилищем модели приложения и единой БД операций конфигурации ЕАС ОПС уровня АУП, являясь поставщиком данных и бизнес логики для клиентского ПО.

Кластер серверов БД выполняет те же функции, что и кластер серверов БД УФПС.

Кластер вспомогательных серверов выполняет те же функции, что и кластер вспомогательных серверов УФПС.

Кластер серверов вспомогательных БД выполняет те же функции, что и кластер серверов вспомогательных БД УФПС.

Файловое хранилище выполняет те же функции, что и файловое хранилище УФПС.

3.2.4. Состав функциональных и обеспечивающих подсистем ЕАС ОПС

ЕАС ОПС включает в себя следующие функциональные подсистемы и комплексы задач:

– подсистема почтовых услуг:
  - комплекс задач оформления приёма РПО;

- комплекс задач оформления вручения (доставки), досыла и возврата РПО;
- комплекс задач по обработке исходящих РПО и емкостей;
- комплекс задач по обработке входящих РПО и емкостей;
- комплекс задач по оформлению партионного приёма РПО путем использования электронного списка;
- комплекс задач по оформлению партионного приёма РПО путем использования бумажного списка;
- комплекс задач по обеспечению адресного хранения РПО;

– подсистема финансовых услуг:
- комплекс задач по оформлению приёма \ выплаты почтовых денежных переводов;
- комплекс задач по оформлению приёма \ выплаты срочных безадресных переводов «Форсаж»;
- комплекс задач по оформлению приёма \ выплаты денежных переводов Western Union;
- комплекс задач по оформлению выплаты пенсий и пособий;
- комплекс задач по оформлению приёма платежей;
- комплекс задач по оформлению услуг страхования;
- комплекс задач по оформлению услуг по брокерскому обслуживанию;
- комплекс задач по оформлению услуг по банковским вкладам;
- комплекс задач по оформлению услуг по банковским картам;
- комплекс задач по оформлению услуг по кредитам / минизаймам;
- комплекс задач по оформлению виртуальных карт оплаты;

– подсистема внутренних услуг:
- комплекс задач по учёту оказанных услуг;
- комплекс задач по учету планов реализации услуг;
- комплекс задач по учету денежных средств;
- комплекс задач по учету ТМЦ, ГЗПО, БСО, НСПУ, ППО, материалов для собственных нужд;
- комплекс задач по формированию и ведению табеля учета рабочего времени;
- комплекс задач учета выработки персонала ОПС;
- комплекс задач оформления операций открытия и закрытия операционной смены.

– подсистема прочих услуг:
- комплекс задач по оформлению подписки на периодические печатные издания;
- комплекс задач по оформлению услуг по распространению рекламно-информационных материалов;
- комплекс задач по реализации проездных билетов и транспортных карт;
- комплекс задач по реализации (в том числе возврат) авиабилетов;
- комплекс задач по реализации (в том числе возврат) жд-билетов;
- комплекс задач по реализации лотерейных билетов;
- комплекс задач по оформлению услуг телеграфной связи;
- комплекс задач по оформлению услуг междугородней и международной связи;
- комплекс задач по оформлению заказов на услуги «Поздравление почтой»;
- комплекс задач по оформлению розничных торговых операций;
- комплекс задач по учету абонирования ячеек абонентного почтового ящика;
- комплекс задач по оформлению филателистического абонемента;

– подсистема формирования отчетности:
- Отчет «Дневник ф.130»;
- Кассовая справка ф. МС-42;
- Отчёт по весу и количеству почтовых отправлений;
- Отчёт ф. 2а-п;
- Отчет ф. 2б-п;
- Отчет по почтовым переводам;
- Отчет по сомнительным операциям;
- Отчет по почтовым отправлениям;
- Отчет по операциям сотрудников;
- Отчет по оказанным услугам / реализованным ТМЦ;
- Отчеты по пенсиям и пособиям;

- Справка по движению РПО на участке / в ОПС;
- Отчет о платежах в пользу третьих лиц.

ЕАС ОПС также включает в себя следующие обеспечивающие подсистемы:

- подсистема обучения операторов;
- подсистема формирования и ведения НСИ;
- подсистема администрирования;
- подсистема интеграции данных;
- подсистема синхронизации данных.

3.2.5. Организация взаимодействия Системы со смежными системами

3.2.5.1. Схема информационного взаимодействия между инсталляциями ЕАС ОПС

Эксплуатация Системы предполагает множественные инсталляции для ОПС (конфигурации ЕАС ОПС уровня ОПС), множественные инсталляции для Почтамтов (доступ в конфигурацию ЕАС ОПС уровня УФПС), а также множественные инсталляции для УФПС (конфигурации ЕАС ОПС уровня УФПС). Инсталляция в АУП предполагает единичное развертывание конфигурации ЕАС ОПС уровня АУП.

Инсталляция каждого вида устанавливается на выделенный набор аппаратных средств и обеспечивает выполнение автоматизируемых функций конкретного объекта автоматизации. Каждая инсталляция обеспечивает прием и передачу информации в другие инсталляции. Схема полностью развёрнутой системы ЕАС ОПС и информационного взаимодействия инсталляций (см. Рисунок 10. Схема взаимодействия инсталляций в рамках ЕАС ОПС).

Организация информационного взаимодействия между компонентами Системы разных уровней обеспечивается подсистемами синхронизации данных и формирования отчётности, которые разработаны на основе платформенного решения.

Информационный обмен механизированных ОПС с УФПС и Почтамтом может производиться как по сетевой схеме, при наличии каналов связи, так и по бессетевой схеме, когда информация передается пакетами на внешних носителях. Информационный обмен осуществляется компонентами подсистемы синхронизации, которые обеспечивают гарантированную доставку данных.

Сетевая схема обмена данными предполагается для ОПС, подключенных к каналам связи. Она предусматривает контроль доступности канала связи для обмена данными и работу с накоплением данных на уровне ОПС в случае неработоспособности канала связи с последующей синхронизацией данных по сети после восстановления работоспособности канала. В случае временной недоступности канала связи подсистема синхронизации ЕАС ОПС обеспечивает:

- локальную буферизацию данных для последующего обмена с подразделением-получателем;
- периодический контроль доступности канала связи;
- передачу буферизированных данных в подразделение-получатель;

– загрузку данных, принятых из подразделения-отправителя.

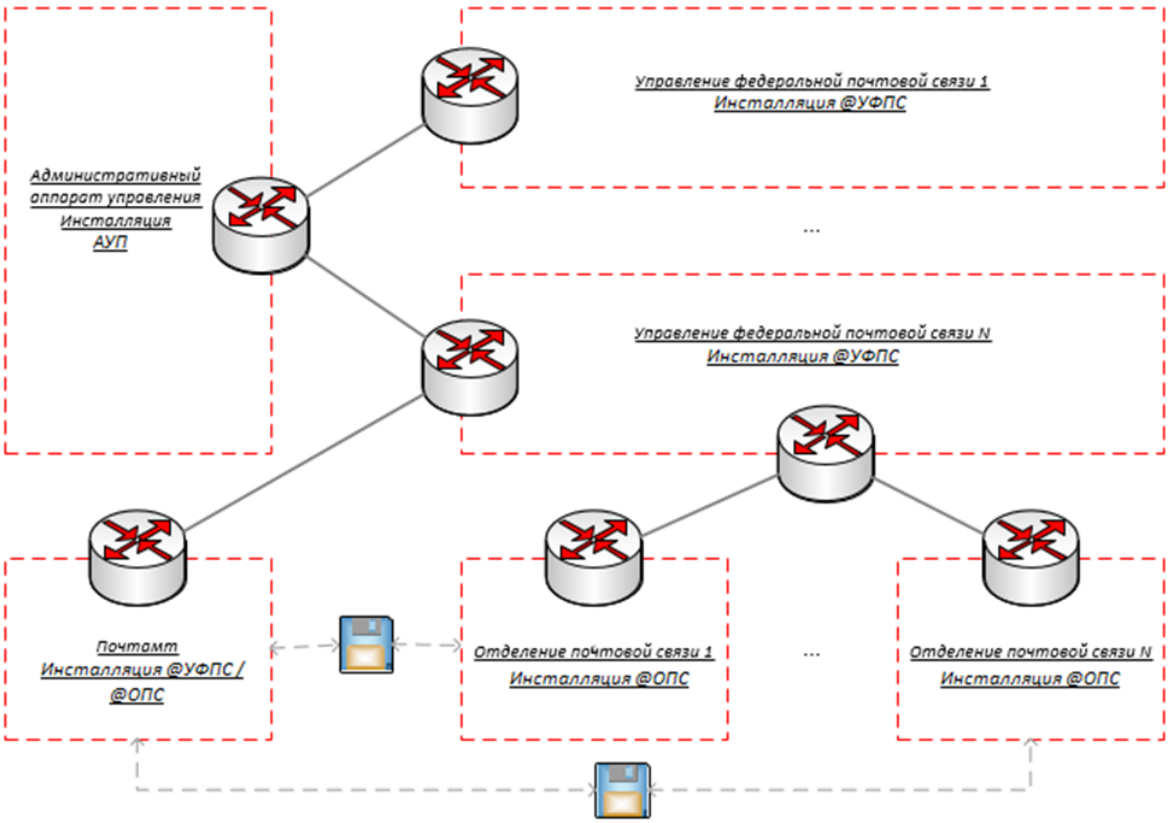


Рисунок 10. Схема взаимодействия инсталляций в рамках ЕАС ОПС

Сетевая схема обмена данными предполагается для ОПС, подключенных к каналам связи. Она предусматривает контроль доступности канала связи для обмена данными и работу с накоплением данных на уровне ОПС в случае неработоспособности канала связи с последующей синхронизацией данных по сети после восстановления работоспособности канала. В случае временной недоступности канала связи подсистема синхронизации ЕАС ОПС обеспечивает:

– локальную буферизацию данных для последующего обмена с подразделением - получателем;
– периодический контроль доступности канала связи;
– передачу буферизированных данных в подразделение-получатель;
– загрузку данных, принятых из подразделения-отправителя.

В случае долговременной недоступности канала связи подсистема синхронизации ЕАС ОПС обеспечивает бессетевую схему обмена.

Бессетевая схема обмена предполагается для ОПС, не подключенных к каналам связи, а также для обеспечения информационного обмена с отделениями связи, испытывающими длительные перебои в работоспособности каналов. Бессетевой обмен обеспечивает выгрузку новой и изменившейся с момента последнего успешного обмена информации на внешний носитель с последующей загрузкой и применением изменений в подразделении-получателе. Бессетевой обмен производится в две стадии:

– на первой стадии производится подготовка данных на внешних носителях на уровнях ОПС и УФПС, причем подготовка внешних носителей с набором информации уровня УФПС готовится работниками Почтамта. Информационная выгрузка уровня УФПС содержит данные конфигурации ЕАС ОПС, а также набор нормативно справочной информации, необходимый для работы подчиненных ОПС. Информационная выгрузка уровня ОПС содержит служебные данные конфигурации, набор данных по со-

вершенным операциям с момента последнего успешного обмена, а также данные журналов регистрации событий . После подготовки внешних носителей, они должны доставляться в соответствующие места назначения;
- на второй стадии производится загрузка информации со внешнего носителя в базу данных соответствующей инсталляции. Причем загрузку с уровня ОПС должны загружать работниками Почтамта, которые должны подключаться к инсталляции УФПС по каналам связи.

При наличии в составе подчинённых подразделений Почтамта немеханизированных ОПС, на Почтамте устанавливается инсталляция, основанная на конфигурации ЕАС ОПС уровня ОПС, в задачи которой входят:

- выполнение функций по вводу данных за немеханизированные отделения связи;
- выполнение функций по поддержке сетевого обмена с вышестоящим УФПС.

Предполагается наличие непрерывной связи от Почтамта до УФПС и выше.

3.2.5.2. Модели интеграции с внешними интеграционными системами

Система поддерживает несколько моделей интеграции с внешними ИС в зависимости от назначения и поддержки режима работы с использованием сетевого или бессетевого обмена:

- интеграция на уровне «ОПС» – используется для интеграции с системами, требующими предварительного (до регистрации операции в ЕАС ОПС) обмена данными в режиме реального времени (либо файловый обмен), а также с ИС, которые не допускают разрыва во времени регистрации операций в ЕАС ОПС и в процессинге (например, операции по обслуживанию банковских карт);
- интеграция на уровне «УФПС» - используется для периодического обмена информацией по совершенным в Системе операциям (зарегистрированным в базе данных ЕАС ОПС), либо для интеграции данных, загруженных в результате бессетевого обмена с отделениями связи;
- совмещенная модель интеграции «ОПС / УФПС» - используется в случае, если внешняя система поддерживает как периодический обмен информацией, так и обмен в режиме реального времени. Использование того или иного режима определяется выполняемой задачей;
- интеграция на уровнях «Почтамт» и «АУП» не предусматривается.

При работе функциональности интеграции на уровне «ОПС», Система обращается напрямую к интерфейсу внешней ИС и производит одну или несколько сессий обмена информацией «Запрос-Ответ» для получения и обработки предварительной информации.

После окончания предварительного обмена данными, Система регистрирует операцию в базе данных с одновременным фиксированием операции во внешней ИС. После осуществления операции, данные из ОПС передаются в УФПС средствами подсистемы синхронизации данных через сетевой или бессетевой обмен.

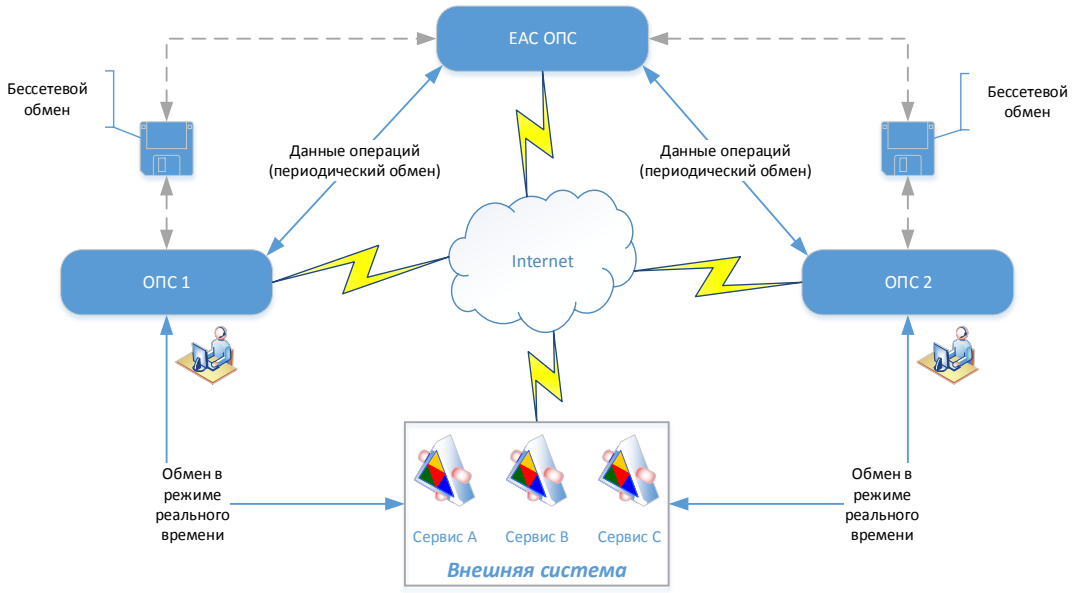
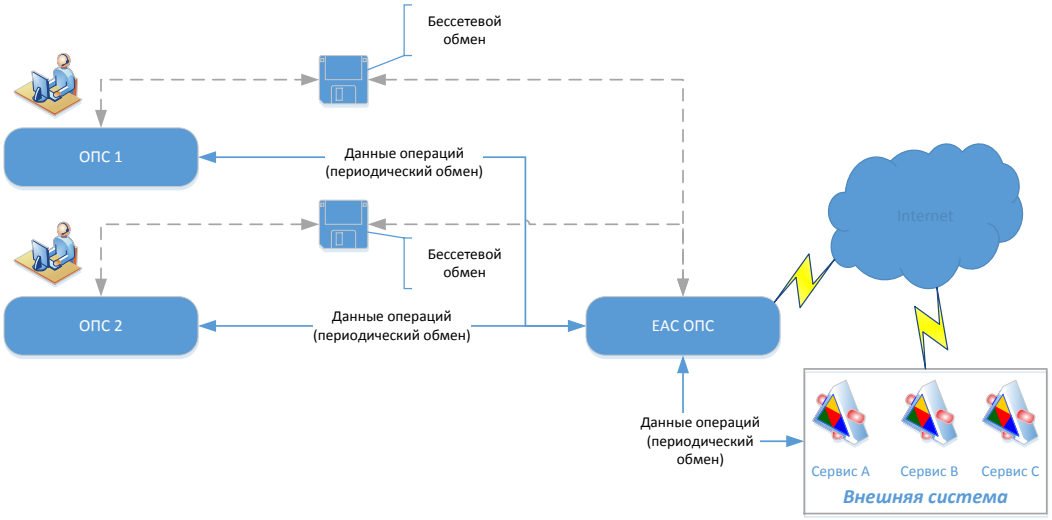


Рисунок 11. Структурная схема интеграции на уровне ОПС

При работе функциональности интеграции на уровне «УФПС» Система инициирует периодические сессии обмена информацией с интерфейсом внешней системы. Передаче подлежат только данные зафиксированных транзакций, поступивших из ОПС посредством подсистемы синхронизации данных (см. Рисунок 12. Структурная схема интеграции на уровне УФПС). Обмен данными инициируется на периодической основе по таймеру или посредством вызова из административной формы Системы. Работа подсистемы интеграции на уровне УФПС в режиме реального времени не предусматривается.

Рисунок 12. Структурная схема интеграции на уровне УФПС



При работе совмещенной модели функциональности интеграции на уровне «ОПС / УФПС» (см. Рисунок 13. Структурная схема совмещенного режима интеграции на уровне ОПС \ УФПС) Система работает в зависимости от логики обработки конкретной операции и от её требований к режиму обработки:

– для обработки в режиме реального времени Система обращается напрямую к интерфейсу внешней системы и производит одну или несколько сессий обмена информацией «Запрос-Ответ» для получения и обработки предварительной информации. После окончания предварительного обмена данными, Система регистрирует операцию в базе данных с одновременным фиксированием операции во внешней системе. После

осуществления операции, данные из ОПС передаются в УФПС средствами подсистемы синхронизации данных через сетевой или бессетевой обмен;

– для обработки в режиме периодического обмена, Система инициирует периодические сессии обмена информацией с интерфейсом внешней системы. Передаче подлежат только данные зарегистрированных транзакций, поступивших из ОПС посредством подсистемы синхронизации данных. Обмен данными инициируется на периодической основе по таймеру или посредством вызова функции из подсистемы администрирования ЕАС ОПС.

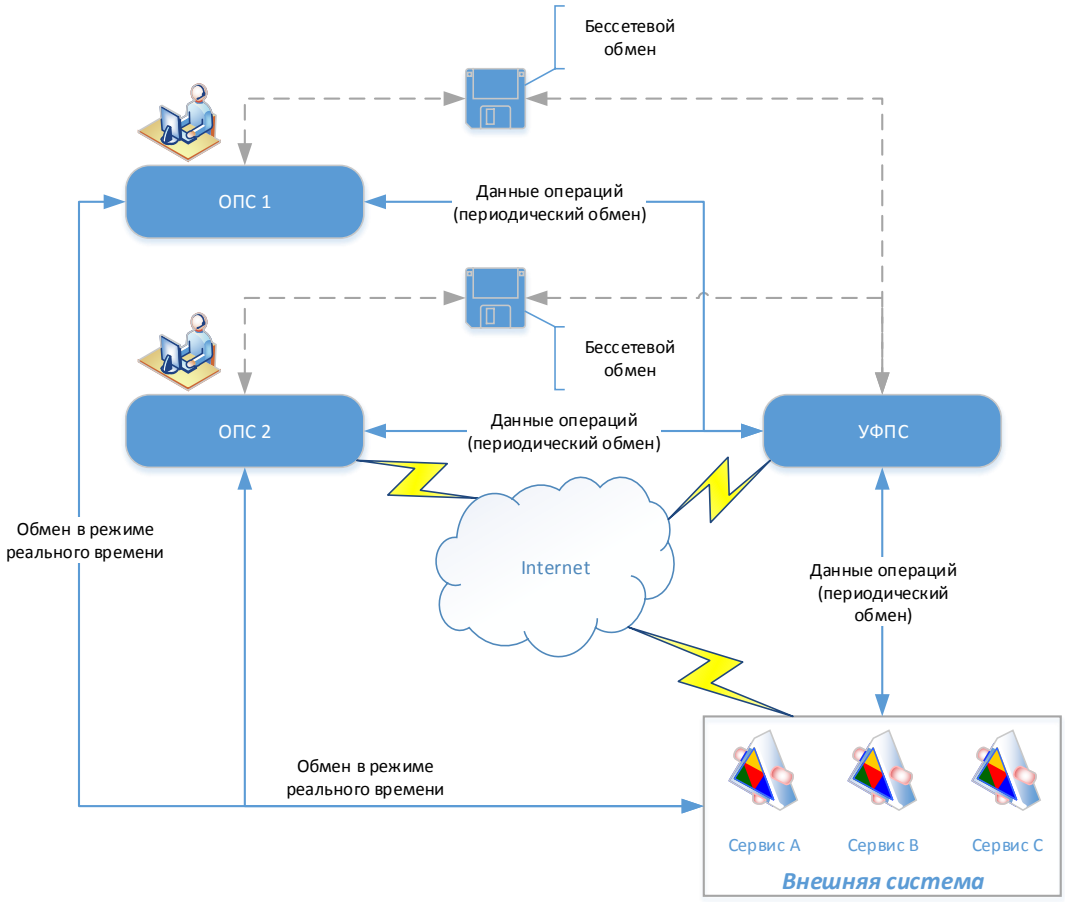


Рисунок 13. Структурная схема совмещенного режима интеграции на уровне ОПС \ УФПС

3.2.5.3. Технологии интеграции с внешними информационными системами

Информационное взаимодействие с внешними ИС обеспечивается посредством средств передачи данных между интерфейсами ввода / вывода ЕАС ОПС, представленных ниже:

– файловый обмен - используется для одностороннего периодического обмена данными по зарегистрированным операциям либо для обмена данными НСИ. Данный вид интеграции преимущественно используется для интеграции с другими фронт-офисными системами на уровне ОПС, хотя может использоваться и для интеграции с учетными системами на региональном уровне (УФПС);

– прямой доступ к базе данных по технологии ADO.NET - используется для доступа к внешним базам данных НСИ либо для интеграции с внешними ИС через промежуточную базу данных. Данный вид интеграции используется преимущественно для доступа к справочным базам, предоставленным сторонними источниками (не использующими ЕАС ОПС) на уровне отделения почтовой связи, а также для периодической загрузки централизованных справочников (например, справочник эталонных индексов) на региональном уровне (УФПС);

– сервисно-ориентированная интеграция - используется в случае наличия требований к обмену данными в режиме реального времени. Используется как при интеграции с

внешними процессинговыми системами на уровне ОПС, так и при периодическом обмене данными с процессинговыми системами по операциям, полученным из ОПС без каналов связи, на уровне УФПС;

– встраивание подключаемых модулей – основной механизм реализации бизнес функционала сторонних поставщиков, используется в случае отсутствия технической возможности информационного взаимодействия иными способами. Данный вид интеграции применяется, как правило, если внешняя система имеет закрытую архитектуру интеграционных интерфейсов, либо предъявляет повышенные требования к защите информации при взаимодействии с ней.

4. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ И ОКАЗАНИЮ УСЛУГ

4.1. Требования к выполнению работ и оказанию услуг по тиражированию ЕАС ОПС

4.1.1. Тиражирование ЕАС ОПС

Работы и услуги по тиражированию ЕАС ОПС должны быть оказаны в следующих регионах и филиалах ФГУП «Почта России»:

- Центральный ФО:
  - УФПС Белгородской области;
  - УФПС Брянской области;
  - УФПС Владимирской области;
  - УФПС Воронежской области;
  - УФПС г. Москвы;
  - УФПС Ивановской области;
  - УФПС Калужской области;
  - УФПС Костромской области;
  - УФПС Курской области;
  - УФПС Липецкой области;
  - УФПС Московской области;
  - УФПС Орловской области;
  - УФПС Рязанской области;
  - УФПС Смоленской области;
  - УФПС Тамбовской области;
  - УФПС Тверской области;
  - УФПС Тульской области;
  - УФПС Ярославской области.
- Южный ФО:
  - УФПС Астраханской области;
  - УФПС Волгоградской области;
  - УФПС Краснодарского края;
  - УФПС Республики Адыгея;
  - УФПС Республики Калмыкия;
  - УФПС Ростовской области.
- Уральский ФО:
  - УФПС Курганской области;
  - УФПС Свердловской области;
  - УФПС Тюменской области;
  - УФПС Ханты-Мансийского автономного округа – Югры;
  - УФПС Челябинской области;
  - УФПС Ямало-Ненецкого автономного округа.
- Сибирский ФО:
  - УФПС Алтайского края;
  - УФПС Забайкальского края;
  - УФПС Иркутской области;
  - УФПС Кемеровской области;
  - УФПС Красноярского края;
  - УФПС Новосибирской области;

- УФПС Омской области;
- УФПС Республики Алтай;
- УФПС Республики Бурятия;
- УФПС Республики Тыва;
- УФПС Республики Хакасия;
- УФПС Томской области.

– Северо-Кавказский ФО:
- УФПС Кабардино-Балкарской Республики;
- УФПС Карачаево-Черкесской Республики;
- УФПС Республики Дагестан;
- УФПС Республики Ингушетия;
- УФПС Республики Северная Осетия — Алания;
- УФПС Ставропольского края;
- УФПС Чеченской Республики.

– Северо-Западный ФО:
- УФПС Архангельской области;
- УФПС Вологодской области;
- УФПС Калининградской области;
- УФПС Мурманской области;
- УФПС Ненецкого автономного округа;
- УФПС Новгородской области;
- УФПС Псковской области;
- УФПС Республики Карелия;
- УФПС Республики Коми;
- УФПС Санкт-Петербурга и Ленинградской области.

– Приволжский ФО:
- УФПС «Татарстан почтасы»;
- УФПС Кировской области;
- УФПС Нижегородской области;
- УФПС Оренбургской области;
- УФПС Пензенской области;
- УФПС Пермского края;
- УФПС Республики Башкортостан;
- УФПС Республики Марий Эл;
- УФПС Республики Мордовия;
- УФПС Самарской области;
- УФПС Саратовской области;
- УФПС Удмуртской Республики;
- УФПС Ульяновской области;
- УФПС Чувашской Республики.

– Дальневосточный ФО:
- УФПС Амурской области;
- УФПС Еврейской автономной области;
- УФПС Камчатского края;
- УФПС Магаданской области;
- УФПС Приморского края;
- УФПС Республики Саха (Якутия);
- УФПС Сахалинской области;
- УФПС Хабаровского края;
- УФПС Чукотского автономного округа.

Плановые количественные характеристики:

№	Наименование	Единица измерения	Кол-во (шт.)
1.	Подготовка к тиражированию	УФПС	**25**
2.	Подготовка инфраструктуры для запуска функциональности ЕАС ОПС уровня УФПС	УФПС	**25**
3.	Настройка ЕАС ОПС уровня УФПС	УФПС	**25**
4.	Формирование реплик ЕАС ОПС уровня ОПС	ОПС	**24600**
5.	Установка ЕАС ОПС на АРМ отделений почтовой связи (выполняется на уровне УФПС)	ОПС	**24600**
6.	Работы в отделении почтовой связи	ОПС	**24600**
7.	Обучение ключевых пользователей ЕАС ОПС (специалисты УФПС/Почтамтов)	УФПС	**25**

Состав группы обучающихся определяется Заказчиком. Численность группы ключевых пользователей для обучения не может превышать 30 (тридцать) человек.Объем работ и услуг по тиражированию, включающий в себя поименованный список УФПС, Почтамтов, ОПС, состав работ/услуг по тиражированию, а также результаты по каждому виду работ/услуг определяются в соответствии с п.п. 2.3, 2.4 Договора.

4.2. Организационные требования

Отчетные документы о результатах работ и услуг по тиражированию ЕАС ОПС предоставляются в двух экземплярах на бумажном и электронном носителях (компакт-диск) в формате MS Word.

В бумажном виде и на компакт-дисках документация передается Заказчику после согласования результатов выполненных работ и оказанных услуг. Бумажные версии документов должны быть сброшюрованы.

5. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ И УСЛУГ

5.1. Требования к составу и содержанию организационно-подготовительных работ

На данном этапе выполняются следующие работы:

- формирование и утверждение организационной структуры Проекта;
- выпуск Заказчиком приказа о начале проекта и формировании рабочей группы Проекта;
- проведение встречи, открывающей проект.

5.2. Требования к составу и содержанию работ и услуг по тиражированию ЕАС ОПС

Перечень работ и услуг по тиражированию ЕАС ОПС включает в себя услуги:

- подготовку к тиражированию;
- подготовку инфраструктуры для запуска функциональности ЕАС ОПС уровня УФПС;
- настройку ЕАС ОПС уровня УФПС;
- формирование реплик ЕАС ОПС уровня ОПС;
- установку ЕАС ОПС на АРМ отделений почтовой связи;
- работы в отделении почтовой связи;
- обучение ключевых пользователей ЕАС ОПС;
- поддержку начального периода эксплуатации Системы с присутствием специалистов в УФПС.

В рамках тиражирования Заказчику необходимо обеспечить выполнение следующих мероприятий:

- определить сотрудников, входящих в состав рабочей группы УФПС;
- обеспечить выделение, оснащение учебных классов, а также помещений для настройки компьютеров ОПС участвующих в тиражировании;
- обеспечить необходимое серверное оборудование УФПС и АУП;
- обеспечить пользователей Системы в УФПС и ОПС вычислительной техникой, ЛВС, программным обеспечением в сроки в соответствии с согласованным планом тиражирования и требованиями к технической инфраструктуре и системному ПО при внедрении Системы;
- провести обучение пользователей силами ключевых пользователей;
- провести функциональное тестирование бизнес-процессов перед развертыванием Системы в филиале;
- обеспечить доставку сотрудников Исполнителя, вычислительной техники в ОПС на собственном транспорте. Также Заказчик обеспечивает доставку сотрудников Исполнителя в почтамт после завершения установки Системы в ОПС;

В рамках тиражирования Исполнителю необходимо обеспечить работоспособность системы и выполнить следующие мероприятия:

- провести обследование филиала;
- провести установку, настройку и тестирование ЕАС ОПС уровня УФПС;
- провести настройку ЕАС ОПС уровня ОПС и сформировать реплики;
- провести обучение и аттестацию ключевых пользователей;
- предоставить будущим пользователям ЕАС ОПС доступ к Системе;
- провести установку ЕАС ОПС на рабочие места будущих пользователей;
- провести проверку работоспособности подключенного оборудования к рабочим станциям пользователей ЕАС ОПС;

- обеспечить поддержку начального периода эксплуатации Системы;
- адаптировать имеющуюся методологию
- обеспечить мониторинг хода тиражирования.

5.3. Требования в части предоставления технологии тиражирования

Учитывая высокую сложность тиражирования с учетом функционального объема тиражируемого продукта, территориального распределения Заказчика, календарного плана тиражирования, необходимым условием является предоставление Исполнителем до начала срока выполнения работ и оказания услуг по заявкам следующих документов:

- Технология тиражирования:
  - Подходы к организации выполнения работ по тиражированию;
  - Организационно-административные мероприятия по подготовке к тиражированию;
  - Подход к организации рабочих групп по тиражированию;
  - Подход к обучению;
  - Подход к обеспечению ОПС техникой с учетом:
    - наличия устаревшей техники не подлежащей модернизации;
    - возможности частичной модернизации техники;
    - наличие различного периферийного оборудования – сканеров, весов, фискальных регистраторов (без возможности замены), пин-падов;
    - требований к массовой подготовке техники с учетом запуска значительного количества отделений в день (~100-200) в рамках Календарного плана.
  - Подход к организации технической и методологической поддержки;
  - Подход к мониторингу процесса тиражирования;
  - Подход к переносу данных и справочников;
  - Типовой шаблон плана работ по тиражированию с учетом настоящих требований к составу и содержанию работ (формат MS Project) с указанием названия, длительности задач и их исполнителей по ролям, результатов работ;
  - Список рисков проекта тиражирования, а также перечень мероприятий по управлению рисками.
- Расчет требуемого количества специалистов с указанием ролей для проведения тиражирования по следующим направлениям:
  - Запуск УФПС;
  - Запуск ОПС в рамках УФПС;
  - Поддержка запуска.

Расчет должен быть выполнен на весь срок проекта в соответствии с календарным планом.

5.4. Результаты выполнения работ и оказания услуг

Результаты оказания услуг представлены в Приложении 2.1 к техническим требованиям.

6. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

Услуги по тиражированию ЕАС ОПС должны быть оказаны с соблюдением требований Федерального законодательства, нормативно-правовых актов регуляторов и локально-правовых актов Предприятия в области защиты персональных данных и конфиденциальной информации.

Приложение № 2.1

к техническим требованиям

ОПИСАНИЕ РАБОТ И УСЛУГ ПО ТИРАЖИРОВАНИЮ

№	Работа/Услуга	Исполнитель	Заказчик	Результаты работ/услуг для приемки
1.	Подготовка к тиражированию	– Определение состава рабочей группы для запуска УФПС – Формирование группы специалистов для запуска и сопровождения Системы на каждый УФПС – Проверка достаточности и целостности данных, представленных в опросных листах для целей настройки Системы – Систематизация, анализ, уточнение и согласование данных опросных листов	– Обучение филиала изменениям в технологических процессах – Разработка и утверждение плана тиражирования – Миграция с СКЗИ Верба на Валидата – Определение состава рабочей группы УФПС – Формирование группы «ключевых» пользователей УФПС и Почтамта и инженеров для запуска ЕАС ОПС – Заполнение опросных листов – Подготовка учебных классов и помещений для настройки компьютеров для отправки в ОПС в филиалах/почтамтах (например, наличие доступа в Интернет, наличие достаточной мощности электропитания, наличие локальной вычислительной сети) – Обеспечение необходимого серверного оборудования УФПС и АУП – Обеспечение необходимого пользовательского и периферийного оборудования на уровне ОПС	**Отчетный документ**: «Протокол подготовки к тиражированию». **Ответственный подписант/подразделение Заказчика**: Ответственный сотрудник АУП

			– Организация доступа к веб-порталу службы технической поддержки	
2.	Подготовка инфраструктуры для запуска функциональности ЕАС ОПС уровня УФПС	– Развертывание серверных компонент ЕАС ОПС уровня УФПС в составе: - Подсистема почтовых услуг - Подсистема финансовых услуг - Подсистема внутренних услуг - Подсистема прочих услуг - Подсистема обучения - Подсистема отчетности - Подсистема администрирования - Подсистема формирования и ведения НСИ - Подсистема синхронизации данных - Подсистема интеграции данных – Настройка серверных компонент внешних подключаемых модулей ЕАС ОПС в составе (но не ограничиваясь) следующих модулей (где это необходимо): - Прием коммунальных платежей PostPay; - Прием коммунальных платежей Банк Москвы; - Прием коммунальных платежей ИС Прием коммунальных платежей Санкт-Петербурга; - Выплата пенсий Банк Москвы; - Выплата пенсий Банк Открытие; - Реализация ж/д билетов; - Реализация онлайн лотерей; - Реализация почтово-банковских и страховых услуг; - Прием переводов Western Union; - Прием моментальных платежей.	– Подготовка серверной инфраструктуры уровня УФПС: - организация виртуальных серверов; - предоставление систем хранения; - организация доступа между серверами, - размещение в КСПД; - настройка маршрутизации; - Настройка каналов связи между уровнями (АУП, УФПС, ОПС). – Формирование и исполнение заявки на настройку портов обмена при интеграции с ПБД. – Настройка серверных компонент внешних подключаемых модулей ЕАС ОПС в составе следующих модулей, а также встроенных в процессе развития Системы (где это необходимо): - Прием коммунальных платежей PostPay; - Прием коммунальных платежей Банк Москвы; - Прием коммунальных платежей ИС Прием коммунальных платежей Санкт-Петербурга; - Выплата пенсий Банк Москвы;	**Отчетный документ**: «Протокол развертывания и настройки инфраструктуры». **Ответственный подписант/подразделение Заказчика**: Ответственный сотрудник АУП

			- Выплата пенсий Банк Открытие; - Реализация ж/д билетов; - Реализация онлайн лотерей; - Реализация почтово-банковских и страховых услуг; - Прием переводов Western Union. - Прием моментальных платежей.	
3.	Настройка ЕАС ОПС уровня УФПС	– Настройка синхронизации ЕАС ОПС уровня УФПС и уровня АУП. – Настройка Подсистемы синхронизации УФПС – ОПС. – Настройка доступа к ЕАС ОПС сотрудников УФПС и Почтамта. – Внесение региональных настроек по услуге «Выплата пенсий». – Настройка интеграции, подготовка интеграционных шлюзов на уровне УФПС. – Получение и загрузка справочников из внешних систем (ИС Подписка, 1С ЗУП и 1С АСКУ). – Подготовительные работы на виртуальном ОПС: - Настройка ЕАС ОПС в соответствии с заполненным опросным листом по Виртуальному ОПС (например, план направлений, региональные тарифы, профили рабочих мест ОПС); - Формирование реплики ЕАС ОПС уровня ОПС для Виртуального ОПС; – Запуск Виртуального ОПС: – **Контроль перед инсталляцией (Осуществление проверки в соответствии с Чек листом)**	– Настройка интеграционных интерфейсов со стороны: - 1С ЗУП; - 1С АСКУ; - ИС Подписка. – Выверка данных в 1С для передачи в ЕАС ОПС. – Организация тестового обмена для механизма интеграции с 1С: - 1С ЗУП; - 1С АСКУ; - ИС Подписка. – Настройка интеграции на стороне ОАСУ РПО. – Инициация передачи справочников из ИС Подписка, 1С ЗУП и 1С АСКУ. – Подготовительные работы на виртуальном ОПС: - Подготовка виртуального ОПС в составе 2-х рабочих мест (начальник ОПС, оператор ОПС); - Предоставление необходимых сертификатов; - Ввод ключа безопасности;	**Отчетный документ**: «Протокол развертывания и настройки ЕАС ОПС уровня УФПС». **Ответственный подписант/подразделение Заказчика**: Ответственный сотрудник УФПС/АУП

		- Проверка соответствия схемы ПК опросному листу и настройкам в ЕАС уровня УФПС - Проверка системного ПО - Проверка компьютера начальника (установлена СУБД SQL согласно необходимой конфигурации) - Проверка наличия и правильного подключения периферийного оборудования (на всех ПК) - Состав подключенного периферийного оборудования соответствует заявленному - Проверка корректного подключения ФР к ПК - Проверка корректного подключения весов к ПК - Проверка корректного подключения Пинпада к ПК - Проверка корректного подключения Сканера к ПК - Проверка готовности транспорта ETM - Проверка наличия перечня пунктов СБП для ОПС - Проверка наличия перечня пользовательских профилей для WU - Проверка установленных сертификатов WU - Проверка установленных сертификатов СК - Проверка установленного ПО Почта Финанс - Проверка интеграционных шлюзов уровня ОПС (ЗПТО, АСУ РПО, ЦХДПА, Форсаж) – **Инсталляция ЕАС ОПС** - Инсталлирование ЕАС ОПС - Формирование реплики на флеш носителе - Импорт реплики - Запуск ЕАС ОПС	- Установка системного ПО; - Настройка пункта СБП; - Установка сертификата Western Union; - Установка сертификата «Свободная касса» - Загрузка тестовых данных из внешних систем (1С ЗУП, 1С АСКУ, ИС Подписка)	

		– **Проведение проверочных работ на инсталляции** - Проверка, что транспорт отключен автоматический транспорт УФПС-ОПС - Обмен данными с 1С (Работники, Номенклатуры, Контрагенты, Договора, Остаток ТМЦ) в офлайн режиме, только в сторону ОПС - Обмен данными ЕАС УФПС -> ЕАС ОПС) в офлайн режиме, только в сторону ОПС - Проверка ДДС. Прием денежных средств в ОПС. Подкрепление кассы - Функционал ЕАС ОПС: Почтовые услуги ▪ Прием РПО ▪ Проверка тарификации по направлениям ▪ Тарифы на дополнительные услуги ▪ Проверить работу ЦХДПА ▪ Проверить регистрацию входящей почты - Функционал ЕАС ОПС: ДУ ▪ Мигрировать данные из ИС "ОПС-Почтовые отправления" (ДУ) ▪ Провести сравнение мигрируемых данных из ДУ (ИС "ОПС-Почтовые отправления") - Функционал ЕАС ОПС: Работа с ТМЦ ▪ Проверка прихода ТМЦ по журналу. Печать ценников ▪ Проверка остатка на складе (с использование формы и отчета о движении ТМЦ) ▪ Проверка продажи ТМЦ, без оплаты - Функционал ЕАС ОПС: Финансовые услуги ▪ Проверка справочников по соц.выплатам		

		▪ Проверка справочников по пенсиям ▪ Проверка выплаты пенсий и соц.выплатам, без оплаты - Переводы ▪ Проверка прием перевода Форсаж, без получения денежных средств. (Без проверки выплаты) ▪ Проверка работы Вестерн Юнион. Проверка авторизации и открытия окна для работы - Функционал ЕАС ОПС: Платежи в пользу третьих лиц ▪ Проверка приема коммунальных платежей в модуле ЕАС POSTPAY. Проверка авторизации и открытия окна для работы ▪ Проверка приема коммунальных платежей через модуль Свободной кассы. Проверка открытия окна для работы ▪ Проверка предоставления банковских страховых услуг через Почта финанс (АРФУ). Проверка открытия окна для работы - Функционал ЕАС ОПС: Прочие услуги ▪ Проверка тарифов на абонирование почтовых ячеек - Подписка ▪ Проверка НСИ из ИС "Подписка" ▪ Проверка оформления подписки, без оплаты ▪ Устранение выявленных расхождений		
4.	Формирование реплик ЕАС ОПС уровня ОПС	– Настройка ЕАС ОПС в соответствии с заполненными опросными листами (например,	– Предоставление опросных листов в соответствии с планом тиражирования	**Отчетный документ**: «Протокол приемки реплик ЕАС ОПС уровня ОПС».

		план направлений, региональные тарифы, профили рабочих мест ОПС); – Формирование реплики ЕАС ОПС уровня ОПС для каждого ОПС очереди тиражирования; – Предоставление УФПС набора сформированных реплик.	– Получение и проверка комплектности набора реплик ЕАС ОПС уровня ОПС в соответствии с очередью тиражирования.	**Ответственный подписант/подразделение Заказчика**: Заместитель руководителя рабочей группы ЕАС ОПС в УФПС
5.	Установка ЕАС ОПС на АРМ отделений почтовой связи (выполняется на уровне УФПС/почтамт)	– Установка системного ПО; – Настройка драйверов периферийного оборудования; – Установка ЕАС ОПС уровня ОПС; – Настройка пункта СБП; – Установка сертификата Western Union; – Установка сертификата «Свободная касса»; – Настройка интеграционных шлюзов уровня ОПС (ЕСПП, ОАСУ РПО, ЦХДПА, Форсаж); – Восстановление пункта ЕСПП; – Консультации в ходе проверки работоспособности; – Проверка готовности к установке ЕАС ОПС по чек-листу; – Получение и загрузка остатков ТМЦ на каждое ОПС; – Настройка ролей для пользователей ОПС.	– Проверка соответствия конфигурации ПК опросному листу и настройкам на уровне УФПС; – Проверка наличия и корректного подключения периферийного оборудования; – Проверка наличия перечня пунктов СБП для ОПС; – Проверка готовности инфраструктуры СКЗИ «Валидата»; – Проверка наличия перечня пользовательских профилей для Western Union; – Проверка установленных сертификатов Western Union; – Установка и настройка крипто-сервера Валидата; – Установка СКЗИ Валидата; – Проверка установленных сертификатов Свободная касса; – Проверка интеграционных шлюзов уровня ОПС (ЕСПП, ОАСУ РПО, ЦХДПА, Форсаж); – Заказ диска восстановления ЕСПП; – Инициация загрузки данных по актуальным остаткам ТМЦ из 1С АСКУ;	**Отчетный документ**: «Протокол установки ЕАС ОПС на АРМ отделений почтовой связи». **Ответственный подписант/подразделение Заказчика**: Заместитель руководителя рабочей группы ЕАС ОПС в УФПС

			– Обеспечение готовности ОПС к установке системы по чек-листу; – Проверка работоспособности системы в ОПС, подписание протокола выходного контроля.	
6.	Работы в отделении почтовой связи	– Установка АРМ на рабочие места, подключение к ЛВС и сети электропитания; – Миграция данных из заменяемых систем (ИС Доставочный участок); – Проверка работоспособности системы (прием РПО, продажа ТМЦ, прием платежей, выплата пенсий, прием и выплата переводов).	– Доставка АРМ в ОПС; – Контроль работоспособности системы на уровне ОПС; – Проведение работ с локальными настройками АРМ; – Подписание чек-листа на работоспособность системы; – Сверка остатков.	**Отчетные документы**: – «Протокол выполнения работ в отделениях почтовой связи»; – «Протокол выходного контроля» Приложение № 5 к Договору. **Ответственный подписант/подразделение Заказчика**: Начальник ОПС
7.	Обучение пользователей ЕАС ОПС	– Установка ЕАС ОПС в учебных классах; – Проведение обучения «ключевых» пользователей, разбор типовых инцидентов; – Аттестация «ключевых» пользователей.	– Проведение обучения пользователей силами «ключевых» пользователей	**Отчетный документ**: «Протокол обучения пользователей». **Ответственный подписант/подразделение Заказчика**: Руководитель рабочей группы ЕАС ОПС в УФПС
8.	Поддержка начального периода эксплуатации Системы	– Техническое сопровождение «ключевых» пользователей почтамтов и УФПС очереди тиражирования: - Организация постоянной линии поддержки пользователей 18х7; - Создание регламентов взаимодействия участников процесса сопровождения Системы; - Организация поддержки пользователей Системы; - Организация поддержки компонентов Системы; - Создание системы отчетности по сопровождению.	– Операции в рамках эксплуатации системы; – Поддержка пользователей «ключевыми» пользователями; – Предоставление Исполнителю помещения на территории УФПС для оказания поддержки.	**Отчетный документ**: «Протокол завершения технического сопровождения ключевых пользователей». **Ответственный подписант/подразделение Заказчика**: Руководитель проекта от АУП

Приложение № 2.2
к техническим требованиям

СТАНДАРТ
«Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений ФГУП «Почта России»

(редакция № 1)

Москва, 2016

Оглавление

1. Термины и определения

В настоящем Стандарте «Обеспечение информационной безопасности при разработке или модернизации информационных систем или приложений ФГУП «Почта России» (далее – Стандарт) используются следующие термины и определения.

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Внешний интерфейс		сервис, через который осуществляется непосредственное взаимодействие с внешними пользователями
Внутренний интерфейс		сервис, через который осуществляется непосредственное взаимодействие с внутренними пользователями и/или администраторами
Департамент информационной безопасности	ДИБ	Департамент информационной безопасности Блока по корпоративной безопасности ФГУП «Почта России»
Информационная безопасность	ИБ	состояние защищенности информации (данных) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации, и характеризуемое способностью обеспечивать конфиденциальность, целостность и доступность информации при ее хранении, обработке и передаче на заданном владельцем уровне
Информационная система		совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационная система персональных данных	ИСПДн	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Компонент системы		компонентом системы является любое сетевое устройство, сервер или приложение, входящее в состав информационной системы или подключенное к среде передачи данных
Минимально необходимые права доступа		набор прав доступа в информационные системы, позволяющие выполнять в информационных системах операции, определяемые должностными обязанностями работника, и не превышающие их
Модель угроз		Документ, в котором определяются актуальные для Системы угрозы информационной безопасности
Несанкционированный доступ	НСД	нарушение регламентированного порядка доступа к объекту защиты
Обфускация		приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции
Операционная Система	ОС	комплекс программ, обеспечивающий управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных задач и утилит
Персональные данные	ПДн	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Система		прикладные системы и приложения, используемые на Предприятии

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Система управления базами данных	СУБД	совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных
Соль		это строка случайных данных, которая подается на вход хеш-функции вместе с исходными данными
Пользователь		лицо, участвующее в функционировании информационной системы
Права доступа пользователя		совокупность правил, регламентирующих порядок и условия доступа пользователя к информации и её носителям, установленных нормативными документами или владельцем информационного актива (ресурса)
Предприятие		ФГУП «Почта России»
Угроза информационной безопасности		совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информационным активам, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий при их обработке в информационной системе
Хэш-функция		функция, реализующая алгоритм преобразования массива входных данных произвольной длины в выходную строку фиксированной длины
Active Directory	AD	
Application		прикладная компьютерная программа или комплекс программ
Completely Automated Public Turing test to tell Computers and Humans Apart	CAPTCHA	компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером
Clickjaking		тип атаки на web-приложения, заключающийся во внедрении web-приложения в iframe с последующим сокрытием последнего на вредоносном сайте с целью выполнения действий от имени пользователя в контексте уязвимого приложения
Cookies		небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя
Content management system	CMS	информационная система или программа для обеспечения и организации совместного процесса создания, редактирования и управления контентом web-приложения
Demilitarized zone	DMZ	отдельный сегмент сети, изолированный от основных сегментов сети с помощью межсетевого экрана
Domain Name System	DNS	служба доменных имён. Представляет собой распределённую, иерархическую базу данных для хранения имён сетей и компьютеров. Также предоставляет функционал по преобразованию строчных имен в числовые IP-адреса
Fully Qualified Domain Name	FQDN	точное обозначение имени оборудования в рамках службы DNS
File Transfer Protocol	FTP	протокол для передачи данных. Обеспечивает передачу данных из файловой системы сервера в локальную файловую систему клиента и наоборот
File Transfer Protocol over SSL	FTPS	дополнение к протоколу FTP, позволяющее передавать его данные поверх протокола TLS/SSL

Наименование термина	Сокращение	Определение термина (расшифровка сокращения)
Identity Manager	IDM	централизованная система, используемая для управления данными пользователей и для синхронизации между несколькими основными пользовательскими хранилищами информации, которые используются для хранения параметров и идентификационной информации
Kerberos		сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними
NT LAN Manager	NTLM	протоколом сетевой аутентификации, разработанный Microsoft для Windows NT
Network Time Protocol	NTP	протокол сетевого времени. Протокол, с помощью которого производится синхронизация системного времени компьютера с временем NTP-сервера
Secure copy	SCP	протокол копирования файлов, использующий в качестве транспорта протокол SSH
Secure Multipurpose Internet Mail Extensions	S/MIME	набор стандартов описывающих безопасную передачу различных типов данных посредством электронной почты и других средств
Service Level Agreement	SLA	соглашение об уровне предоставления услуги
SSH File Transfer Protocol	SFTP	протокол, предназначенный для обмена и управления данными поверх какого-либо криптографического протокола (обычно SSH)
Structured Query Language	SQL	структурированный язык запросов. Специализированный информационно-логический язык, используемый для работы с данными в реляционных СУБД
Secure Shell	SSH	протокол, позволяющий передавать данные и производить удалённое управление операционной системой по защищенному каналу
Transport Layer Security	TLS	криптографический протокол, обеспечивающий конфиденциальность и целостность данных при их передаче по сети
Uniform Resource Locator	URL	универсальный указатель ресурса
Virtual Private Network	VPN	виртуальная частная сеть. Логическая сеть, создаваемая поверх другой сети, и использующаяся для безопасной пересылки данных
Web-приложение		клиент-серверная Система, в которой клиентом выступает браузер, а сервером — веб-сервер

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящий Стандарт разработан с целью унификации требований по информационной безопасности, предъявляемых к новым или модернизируемым информационным системам и приложениям Предприятия, обеспечения конфиденциальности, целостности и доступности обрабатываемой в них информации с учетом исполнения требований законодательства Российской Федерации, семейства стандартов ISO/IEC 27000, локальных нормативных документов Предприятия.

Требования настоящего Стандарта распространяются на все подразделения Предприятия, осуществляющие деятельность по разработке, модернизации и эксплуатации информационных систем и приложений.

Подразделением, ответственным за координацию и контроль исполнения настоящего Стандарта является Департамент информационной безопасности.

Отступление от требований настоящего Стандарта осуществляется по согласованию с Департаментом информационной безопасности.

Настоящий Стандарт подлежит пересмотру и актуализации (в случае необходимости) не реже 1 раза в три года, а также в случае изменения законодательства в области информационной безопасности, касающихся положений данного Стандарта.

Актуальная версия Стандарта размещается на корпоративном портале или может быть предоставлена по электронной почте по соответствующему запросу в Департамент информационной безопасности.

3. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

3.1 Работы по обеспечению ИБ должны проводиться на всех этапах жизненного цикла Системы.

3.2 Работники Департамента информационной безопасности должны включаться в состав комиссии (проектной команды) по разработке или модернизации Системы.

3.3 Требования настоящего Стандарта должны в обязательном порядке включаться в технические задания на разработку или модернизацию Системы.

3.4 Объем требований по обеспечению ИБ, включаемый в техническое задание на разработку или модернизацию Системы, определяется в рамках процесса его согласования с Департаментом информационной безопасности. Исключение требований данного Стандарта из технического задания возможно с учетом обоснования такой потребности и его согласования с Департаментом информационной безопасности.

3.5 В рамках работ по созданию или модернизации Системы Департамент информационной безопасности должен провести ее испытания по проверке исполнения требований настоящего Стандарта, а также отсутствия уязвимостей Системы.

3.6 Ввод Системы в эксплуатацию (опытную/промышленную) возможен после успешного прохождения испытаний Системы и получения положительного заключения о ее соответствии требованиям информационной безопасности.

4. ТРЕБОВАНИЯ К РАЗРАБАТЫВАЕМЫМ ИЛИ МОДЕРНИЗИРУЕМЫМ СИСТЕМАМ

4.1. Общие требования

4.1.1. Конфиденциальные данные, хранящиеся и передающиеся внутри корпоративной сети, должны быть защищены с использованием криптографически стойких алгоритмов шифрования. Перечень криптографически стойких

алгоритмов шифрования и хеширования утверждается заместителем генерального директора по корпоративной безопасности, размещается на корпоративном портале совместно с настоящим Стандартом и может быть предоставлен Департаментом информационной безопасности по электронной почте по запросу.

4.1.2. Данные, содержащие коммерческую тайну, персональные данные, тайну связи и иную информацию, обеспечение конфиденциальности которой определяется законодательством Российской Федерации, при передаче по сетям общего пользования должны защищаться с использованием средств криптографической защиты информации, имеющих сертификат соответствия ФСБ России.

4.1.3. Система и ее компоненты, расположенные в DMZ, не должны хранить информацию конфиденциального характера Предприятия.

4.1.4. Тестовые и учебные экземпляры Системы не должны содержать реальных данных конфиденциального характера либо должны содержать их в обезличенном виде.

4.1.5. Должна осуществляться проверка/валидация любых входных данных на длину, допустимые символы, кодировку, полноту данных (наличие обязательных параметров). Проверка должна осуществляться до процесса их обработки в Системе и передачи во внешние компоненты.

4.1.6. Внешние интерфейсы Системы, предоставляющие доступ из общедоступных сетей клиентам Предприятия, и внутренние интерфейсы Систем, работающие с привилегированными пользователями (внутренние пользователи и/или администраторы), должны быть разделены.

4.1.7. Возможность управления сервисами безопасности, в том числе отключения, подключения, модификации режима аутентификации, авторизации, аудита и т.п., должна быть доступна только администратору Системы.

4.2.Требования к аутентификации и авторизации

4.2.1. Доступ к ресурсам Системы должен предоставляться только после успешного прохождения процесса аутентификации пользователя и последующей его авторизации.

4.2.2. Доступ к ресурсам Системы должен подразделяется на пользовательский, административный, технологический и должен быть реализован на основе ролей с учетом принципов разделения обязанностей и минимизации полномочий. В Системе необходимо наличие средств управления ролями: создание новых, редактирование, удаление.

4.2.3. Управление доступом к Системе должно осуществляться на основании групповой или ролевой моделей.

4.2.4. Внешние и внутренние пользователи должны проходить аутентификацию во внешней и внутренней системе аутентификации соответственно. Внешняя и внутренняя системы аутентификации должны быть разделены.

4.2.5. Внутренняя система аутентификации должна взаимодействовать с AD Предприятия или непосредственно интегрироваться с системой AD Предприятия или корпоративной IDM.

4.2.6. Для каждого пользователя необходимо использовать следующие основные атрибуты безопасности: идентификатор пользователя, аутентификационная информация (например, пароль), права доступ к объекту защиты (роль).

4.2.7. Для каждого пользователя необходимо использовать уникальную учетную запись, сформированную в соответствии с принятыми на Предприятии правилами именования.

4.2.8. Использование групповых учетных записей запрещено.

4.2.9. В Системе и ее компонентах должны отсутствовать жестко запрограммированные учетные записи.

4.2.10. Все неиспользуемые учетные записи (установленные по умолчанию, тестовые, сервисные) для штатной работы Системы и ее компонентов должны быть удалены или заблокированы.

4.2.11. В качестве механизмов аутентификации пользователей Системы могут быть использованы:

– пароли;

– средства двухфакторной аутентификации (USB-токен, смарт-карта и т.п.);

– средства биометрической аутентификации.

4.2.12. Восстановление пароля должно производиться только путем его смены.

4.2.13. В процессе аутентификации проверка введенной информации (логина и пароля) должна осуществляется только после полного ее ввода. В случае обнаружения ошибки Система не должна уточнять, какие именно данные введены неправильно. Пароль не должен отображаться при вводе.

4.2.14. Проверка/валидация учетных данных пользователя должна проводиться на стороне серверных компонентов Системы.

4.2.15. Компоненты Системы с повышенными требованиями к обеспечению информационной безопасности в случае сетевого взаимодействия, например, при передаче по сети финансовых операций, должны проходить процедуру взаимной аутентификации.

4.2.16. Подсистема аутентификации Системы должна обеспечивать возможность настройки парольной политики в части:

– самостоятельной смены пароля пользователем при первом входе в Систему, а также в любое время по его усмотрению;

– отключения администратором функции смены паролей у отдельных пользователей;

– установки парольной политики для всех пользователей, группы пользователей или отдельно для каждой учетной записи в соответствии с локальными нормативными документами Предприятия;

– принудительной смены пароля пользователем через установленный промежуток времени;

– заблаговременного оповещения пользователей о необходимости смены пароля (посредством сообщений/подсказок или почтовых рассылок на электронные адреса пользователей);

– блокировки учётной записи на заранее определенный срок после заданного количества неудачных попыток аутентификации;

– установки срока длительности простоя пользовательской сессии, после которого сессия должна принудительно завершаться;

– ограничения множественного входа в систему под одной учетной записью пользователя.

Дополнительно для внутренних пользователей подсистема аутентификации Системы должна осуществлять:

– автоматическую блокировку учётной записи пользователя в случае, если пароль не был изменён до установленной даты;

– хранение истории паролей пользователей как минимум за последние 12 месяцев для предотвращения повторного их использования.

4.2.17. Механизмы авторизации пользователей Систем должны поддерживать возможность разделения доступа к данным и функциям внутри Системы.

4.2.18. Все действия в Системах, включая их администрирование и штатную эксплуатацию, должны производиться с использованием учетных записей, наделенных минимально необходимыми привилегиями.

4.2.19. В Системах пароли должны храниться и передаваться только в зашифрованном виде. При хранении и передаче должны использоваться стойкие криптографические алгоритмы или алгоритмы хеширования, определенные в соответствии с пунктом 4.1.1.

4.2.20. Процесс аутентификации и авторизации должен быть устойчив к сетевым угрозам (пассивному и активному прослушиванию сети, подбору паролей и т.п.).

4.3.Требования к сетевому взаимодействию

4.3.1. Сетевой обмен информацией между компонентами Системы, сопрягаемыми Системами, находящимися в разных сетевых сегментах, должен осуществляться с использованием защищенных стандартов и протоколов, таких как:

– HTTPS/TLS;
– SFTP;
– FTPS;
– SSH-2;
– SCP;
– S/MIME с использованием сертификатов x.509 v3;
– VPN (IPSEC, L2TP, PPTP и т.д.).

4.3.2. DNS имена внешних/внутренних компонентов Системы (FQDN) должны быть зарегистрированы соответственно в прямой и обратной зонах внешних/внутренних служб DNS Предприятия.

4.3.3. Сетевое взаимодействие Системы и ее компонентов должно производиться с использованием FQDN, если это технически возможно.

4.3.4. Ни один из серверов Системы не должен подключаться одновременно к сетевым периметрам с различными уровнями безопасности (например, DMZ и корпоративная сеть).

4.3.5. Запрещается предоставлять доступ через сеть Интернет к сервисам Системы, предназначенным для внутреннего использования.

4.3.6. Запрещается предоставлять доступ через сеть Интернет к сервисам Системы, использующим для взаимодействия с пользователями следующие протоколы: SMB/SAMBA/CIFS, NFS, NETBIOS, протоколы доступа к СУБД (MYSQL, MSSQL, ORACLE и др.), протоколы удаленного управления (telnet, RSH, SNMP, RDP и др.).

4.3.7. Доступ к компонентам Системы, размещенным в DMZ, должен осуществляться с использованием минимально необходимого набора сетевых протоколов.

4.3.8. Серверные компоненты Системы должны размещаться в серверных сегментах сети Предприятия.

4.3.9. Внешние (публичные) интерфейсы Системы должны быть вынесены в DMZ. Размещение публичных интерфейсов и серверов Системы в DMZ возможно только после проведения ДИБ аудита ИБ и получения положительного заключения по результатам такого аудита.

4.3.10. Продуктивные и тестовые среды Системы должны быть разделены на физическом/виртуальном и логическом уровне. Например, тестовая среда Системы должна представлять собой отдельную копию Системы, не взаимодействующую с какими-либо продуктивными средами Систем.

4.4.Требования к окружению

4.4.1. Разрабатываемая или модернизируемая Система должна корректно функционировать с используемыми на Предприятии:

– средствами обеспечения безопасности рабочих станций и серверов, например, антивирусами, средствами обнаружения и предотвращения вторжений, средствами межсетевого экранирования, средствами контроля внешних устройств, средствами криптографической защиты информации и т.д.;

– ОС, СУБД, прикладными программами с действующими на момент разработки или модернизации Системы настройками.

4.4.2. Перечень средств защиты ОС, СУБД, прикладного программного обеспечения, используемого на Предприятии и с которыми должна быть совместима разрабатываемая или модернизируемая Система, должен уточняться и согласовываться с ДИБ в рамках предпроектного обследования.

4.4.3. Разрабатываемые компоненты Системы, включая программное и аппаратное обеспечение, не должны содержать недокументированных возможностей, направленных на скрытый контроль пользователей или администраторов системы (например, отправка информации в Интернет о действиях

в системе). Свободно распространяемые и проприетарные программные и аппаратные продукты, используемые в составе Системы, рекомендуется выбирать с учетом наличия заключения производителя или третьей стороны об отсутствии недокументированных возможностей.

4.4.4. На компонентах Системы должны быть запущены только те сервисы и приложения, которые необходимы для функционирования данной Системы или функционирования других Систем (при совместном использовании компонент).

4.4.5. Взаимодействие компонент Системы, а также взаимодействие с внешними Системами должно происходить под технологическими учетными записями с минимально необходимыми наборами привилегий.

4.4.6. Компоненты Системы должны быть построены исключительно на продуктах и операционных системах, удовлетворяющих всем требованиям безопасности настоящего Стандарта, а также стандартов информационной безопасности Предприятия, разработанных для конкретных ОС, СУБД, приложений. Стандарты информационной безопасности для конкретных ОС, СУБД, приложений утверждаются заместителем генерального директора по корпоративной безопасности Предприятия, размещаются на корпоративном портале совместно с настоящим Стандартом и могут быть предоставлены Департаментом информационной безопасности по электронной почте по запросу.

4.5. Требования к аудиту

4.5.1. Для Системы и ее компонент (включая уровни ОС, СУБД и Приложения) должен быть включен механизм протоколирования событий.

4.5.2. Механизм протоколирования событий должен быть способен сопоставить каждое подлежащее аудиту событие с источником события с возможным определением IP адреса источника.

4.5.3. В Системе как минимум должны протоколироваться следующие события:

- работа пользователей с данными Системы, в том числе создание, чтение, изменение или удаление данных;
- события аутентификации пользователя в Системе, выход (окончание сессии) из Системы, если технически применимо;
- действия привилегированных пользователей по настройке и изменению конфигурации Системы, в том числе изменение настроек Системы, настроек аудита, создание/удаление пользователей/ролей/групп пользователей, изменение привилегий пользователей/ролей/групп пользователей, установка/удаление компонент Системы;
- доступ к записям журнала протоколирования событий;
- очистка логов;
- запуск и остановка компонентов Системы.

4.5.4. По каждому событию должна протоколироваться следующая информация:

- результат операции (успешно/неуспешно);

– идентификатор источника операции (идентификатор пользователя, логин пользователя, имя процесса, IP-адрес, идентификатор рабочей станции и т.д.);

– идентификатор объекта, над которым была выполнена операция;

– название и тип выполненной операции (например, аутентификация, чтение, запись, удаление, установление соединения и др.);

– значение параметра до и после операции, если действие предполагает изменение данных или состояния компоненты Системы;

– дата и время выполнения операции, включая указание часового пояса.

4.5.5. Время, указываемое в журналах аудита, должно быть синхронизировано с системным временем корпоративного NTP-сервера, являющегося частью инфраструктуры сети Предприятия (допустимая погрешность не более 5 секунд).

4.5.6. Срок хранения журналов аудита в оперативном доступе в Системе должен составлять не менее трех месяцев.

4.5.7. Журналы аудита должны иметь возможность автоматического разбиения и хранения по месяцам. По истечении установленного времени журналы должны автоматически архивироваться. Архивные журналы должны храниться не менее одного года, после чего могут быть удалены.

4.5.8. Система должна предоставлять средства фильтрации событий журнала аудита по протоколируемым параметрам.

4.5.9. Система должна предоставлять возможность сохранять журналы аудита во внешние системы. При этом могут быть использованы следующие способы доступа к журналам аудита: сетевой доступ к файлу с журналом, SQL доступ к таблице с журналом, SNMP, Syslog, Eventlog и т.д.

4.5.10. Журналы аудита Системы не должны содержать данных конфиденциального характера (например, пароли пользователей).

4.5.11. Журналы аудита Системы должны быть защищены от изменений.

4.6. Требования по отказоустойчивости

4.6.1. Система должна разрабатываться с учетом возможности балансирования нагрузки между отдельными компонентами и модулями. При этом выход из строя отдельных компонент или модулей Системы не должен сказываться на общей функциональности остальной части Системы.

4.6.2. В рамках разработки или модернизации Системы должны быть выстроены процессы резервного копирования и восстановления данных, обрабатываемых в Системе. Процесс резервного копирования не должен работать с резервируемыми данными в монопольном режиме.

4.7. Требования к эксплуатации

4.7.1. В Системе, находящейся в промышленной эксплуатации, компоненты должны обновляться до последних стабильных версий либо тех версий,

которые обеспечивают максимальную защищенность Системы (например, отсутствуют известные уязвимости).

4.7.2. В случае возникновения нестабильной работы Системы в результате установки обновлений безопасности организация, осуществляющая поддержку Системы, должна предложить и внедрить альтернативное решение возникшей проблемы в соответствии с действующим SLA.

4.7.3. Разработка и тестирование изменений Системы не должны выполняться на продуктивных экземплярах Системы. Установка средств разработки (компиляторы, отладчики, шестнадцатеричные редакторы и т.п.) и тестирования на продуктивные экземпляры Системы запрещена.

4.7.4. Компоненты Системы должны обеспечиваться действующей технической поддержкой на ОС, СУБД, приложения и оборудование.

4.7.5. Все компоненты Системы должны быть зарегистрированы в корпоративных системах мониторинга и управления конфигурациями.

4.7.6. В Системе, находящейся в промышленной эксплуатации, должен быть отключен детальный вывод отладочной информации об ошибках в Системе и ее компонентах, используемой в процессе разработки Системы.

4.7.7. Удаленный административный доступ к Системе и ее компонентам допускается в случае производственной необходимости только из корпоративной сети по защищенным протоколам (SSH-2, SFTP, FTPS, SCP, RDP не ниже версии 6.0 и т.п.).

4.7.8. Пароли от предустановленных учетных записей в продуктивной Системе и ее компонентах должны быть изменены сразу после их установки.

4.7.9. Административный доступ должен предоставляться только администраторам Системы на основании их должностных обязанностей и заявок на предоставление доступа. Доступ остальным пользователям к Системе должен регламентироваться соответствующими локальными нормативными документами и предоставляться на основе заявок. На продуктивной Системе учетные записи разработчиков и/или производителей должны быть удалены или заблокированы администраторами Системы.

4.8. Требования к web-приложениям

4.8.1. При разработке или модернизации Системы, содержащей web-интерфейсы или приложения, предъявляются дополнительные требования (приложение № 1).

4.9. Требования к документации и исходным кодам

4.9.1. В рамках работ по разработке или модернизации Системы должны быть разработаны или скорректированы следующие документы:

- описание Системы;
- руководство пользователя Системы (для внутренних пользователей);
- руководство администратора Системы;
- матрица предоставления доступа к Системе (по ролям);
- регламент технического обслуживания;

– схема резервного копирования данных;

– регламент восстановления Системы при сбоях.

4.9.2. Описание Системы должно содержать:

4.9.2.1. Общие сведения о Системе:

– краткое описание и назначение Системы;

– перечень категорий сведений, хранящихся, обрабатываемых или передающихся в Системе, с указанием степени их конфиденциальности и принадлежности к ПДн, и места хранения (перечень файлов, таблиц/схем СУБД и т.п.);

4.9.2.2. Описание архитектуры Системы, включающую:

– сведения о логической структуре и составе Системы (модули, компоненты);

– описание технологического процесса обработки данных;

– описание структуры программного обеспечения, комплектности и выполняемых функций, включая внешнюю спецификацию каждого включенного в нее модуля;

– описание протоколов обмена, схемы интеграций;

– описание механизма интеграции с другими Системами;

– перечень интерфейсов и перечень команд для каждого интерфейса[2]

4.9.2.3. Инвентаризационные сведения о Системе:

– схему сетевой архитектуры Системы (приложение № 2);

– таблицу IP адресов компонентов Системы (приложение № 3);

– таблицу информационных потоков/доступов Системы (приложение № 4);

– указание используемых типов и версий ОС;

– описание базы данных (логическая структуры)[1];

– описание типов и версий компонентов Системы;

– список компонентов и сервисов ОС, необходимых для работы Системы;

– параметры настроек программного и аппаратного обеспечения, входящих в состав Системы или используемых Системой в качестве поставщика сервиса и необходимых для корректного функционирования Системы;

– перечень папок и файлов, относящихся к приложению, с контрольными суммами для статических файлов;

– перечень ключей и основных параметров реестра, относящихся к приложению[1];

– перечень запускаемых после перезагрузки ОС процессов и сервисов приложения;

[2] Указанные сведения могут не включаться в описание для используемых в составе Систем готовых программных и аппаратных продуктов (свободно распространяемых и проприетарных)

– описание групп и ролей пользователей Системы (с принадлежностью к подразделениям Предприятия);

4.9.2.4. Сведения об обеспечении информационной безопасности:

– описание реализации выполнения требований настоящего Стандарта (пример приведен в приложении № 5);

– перечень и краткое описание используемых средств защиты информации;

– описание исполнения требований эксплуатационной документации на средства защиты информации;

– сведения о протоколируемых событиях ИБ.

4.9.3. Документация, указанная в пункте 4.9.1, должна быть доступна только авторизованным пользователям в рамках служебной необходимости. В документации должна отсутствовать аутентификационная информация (пароли и т.п.).

4.9.4. Исходные коды Системы не должны находиться в свободном доступе, если это не противоречит лицензии, по которой распространяется Система.

4.10. Требования к ИСПДн

4.10.1. Системы, обрабатывающие персональные данные, должны соответствовать требованиям законодательства Российской Федерации.

4.10.2. С целью минимизации затрат на соответствие регуляторным требованиям разрабатываемые или модернизируемые Системы должны соответствовать типовой модели угроз персональным данным, утвержденной на Предприятии.

4.10.3. В случае несоответствия разрабатываемой или модернизируемой Системы типовой модели угроз персональным данным рекомендуется применить компенсирующие меры, например, изменить объем обрабатываемых персональных данных, их категорию, применить обезличивание (как обратимое, так и необратимое), с целью приведения в соответствие архитектурных решений Системы типовой модели угроз.

4.10.4. Обезличивание информации может осуществляться в соответствии с приказом Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и Методическими рекомендациями по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных», утвержденных руководителем Роскомнадзора 13.12.2013.

4.10.5. При соответствии разрабатываемой или модернизируемой Системы типовой модели угроз защита персональных данных осуществляется развернутой на Предприятии системой защиты персональных данных, обеспечивающей для серверных компонент 3 уровень защищенности, а для пользовательских компонент - 4 уровень защищенности.

4.10.6. В случае неприменимости типовой модели угроз персональным данным к разрабатываемой и модернизируемой Системе даже с учетом корректировки ее архитектурных решений в рамках работ по разработке или модернизации Системы необходимо:

– разработать частную модель угроз персональным данным на основе типовой модели;

– разработать проект защиты персональных данных, обрабатываемых в Системе, соответствующий частной модели угроз, с учетом использования решений развернутой на Предприятии системы защиты персональных данных;

– внедрить проект защиты персональных данных разрабатываемой или модернизируемой Системы.

5. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ РАБОТ

5.1. В случае разработки или модернизации Системы, использующей средства криптографической защиты информации (СКЗИ), исполнитель должен обладать лицензией на выполнение работ, связанных с СКЗИ, и разработать предложения по выполнению требований приказа ФАПСИ от 13.06.2001 № 152.

5.2. В случае разработки или модернизации Системы, использующей сертифицированные средства защиты информации, исполнитель должен обладать лицензией ФСТЭК России на выполнение соответствующих работ.

5.3. В случае сопряжения Системы с другими информационными системами или использования любого состава и комбинаций технических и/или программных средств, обслуживаемых и/или закупаемых Предприятием для обеспечения функционирования разрабатываемой информационной системы и не входящих в ее состав, Исполнитель должен предоставить комплексное решение по обеспечению информационной безопасности, включая предложения по настройке, размещению и эксплуатации указанных выше средств начиная от каналообразующего оборудования и заканчивая прикладным программным обеспечением.

Приложение № 1
к Стандарту «Обеспечение информационной
безопасности при разработке или модернизации
информационных систем и приложений
ФГУП «Почта России»

Требования к WEB-приложениям

1. Требования к активному содержимому и скриптам

1.1. Требования к сценариям JavaScript

1.1.1. Структуры и данные, обеспечивающие безопасность web-приложения (токены аутентификации, сессионные cookie и т.д.) не должны обрабатываться сценариями JavaScript.

1.1.2. Рекомендуется использовать доверенные общепризнанные источники JavaScript сценариев или создавать собственные сценарии на основе таких. Использование собственных сценариев JavaScript по возможности должно быть сведено к минимуму.

1.2. Требования к сценариям AJAX (Asynchronous JavaScript and XML)

1.2.1. Использование технологии AJAX для обработки платежной информации запрещено.

1.3. Требования к ActiveX и сценариям Visual Basic

1.3.1. Использование скриптов, написанных на Visual Basic, запрещено.

1.3.2. Использовать компоненты ActiveX не рекомендуется.

1.4. Требования к Java-апплетам

1.4.1. Все используемые Java-апплеты должны иметь цифровую подпись доверенного удостоверяющего центра.

1.4.2. Java-апплет не является доверенным компонентом. В связи с этим в коде апплета не должны быть реализованы механизмы принятия критичных решений (например, относящимся к механизмам безопасности или бизнес процессам).

1.4.3. Рекомендуется использовать обфускацию байт-кода Java-апплетов.

2. Требования к проверке входных и выходных параметров

2.1. Общие требования

2.1.1. Все входные параметры должны проверяться на серверной стороне с целью проверки входных параметров и выявления распространенных сценариев атак на web-приложения (XSS, SQL-инъекции, CSRF и т.д.). Например, поле с ФИО не должно принимать в обработку данные, содержащие цифры или знаки препинания.

2.1.2. Проверка входных параметров должна осуществляться до их использования компонентами web-приложения (базы данных, скрипты и т.д.).

2.1.3. Web-приложение должно проверять полноту полученных от пользователя параметров (например, наличие всех параметров в форме ввода).

2.1.4. HTTP-заголовки и скрытые HTML поля (<input type=hidden>), если они используются в web-приложении, должны проходить проверку, как и обычные HTTP параметры.

2.1.5. Сообщения об ошибках не должны содержать сведений, по которым возможно восстановить метод проверки параметров.

2.1.6. Для настройки списка разрешенных ресурсов на клиентской части web-приложения и предотвращения атак типа XSS должны быть включены и настроены следующие опции:

– *X-Content-Security-Policy,*

– *X-WebKit-CSP.*

2.1.7. Для включения фильтра атак XSS в Web-приложении должна быть задействована опция:

– *X-XSS-Protection: 1; mode=block.*

2.1.8. Рекомендуется дополнительно осуществлять проверку входных параметров пользователя в клиентской части web-приложения.

2.2. Очистка возвращаемых данных

2.2.1. Проверка возвращаемых клиенту данных должна осуществляться до момента отправки web-страницы от сервера браузеру.

2.2.2. Форматирование вводимой пользователем HTML-разметки должно осуществляться средствами CMS или доверенных библиотек (например, функция htmlspecialchars в PHP). Запрещается использовать HTML теги из входных данных пользователя для формирования web-страниц (сообщения на форумах, гостевых книгах и т.д.).

2.2.3. В случае необходимости визуализировать управляющие символы, используемые в HTML, JavaScript, Flash и других компонентах, серверная часть web-приложения должна осуществлять замену всех управляющих символов на их «видимые» аналоги *(<script>* на *<script>* и т.д.).

3. Предотвращение раскрытия информации

3.1. Общие требования

3.1.1. Исходный код скриптов и активных компонент, исполняемых на клиентской стороне (сценарии JavaScript, AJAX, ActiveX, Java-апплеты и т.д.), не должен содержать сведений конфиденциального характера (специфических алгоритмов, паролей, критичных переменных и т.д.).

3.2. Минимизация вывода информации

3.2.1. Исходный код web-страниц не должен содержать служебную информацию. Например, комментарии, мета-теги, скрытые поля, куки не должны содержать сведения, которые могут быть использованы для подготовки атак (внутренние IP-адреса, телефоны, адреса электронной почты, описания работы алгоритмов и т.д.).

3.2.2. Сообщения ошибок не должны выдавать версии программного обеспечения, используемого системой, внутренних путей, а также ранее введенных пользователем данных.

3.2.3. Web-сервера, СУБД и используемые приложения должны быть сконфигурированы таким образом, чтобы затруднить атакующему определение реальных версий компонентов.

3.3. Требования к формированию URL

3.3.1. URL не должны содержать сведений конфиденциального характера (IP-адреса, пароли, номера кредитных карт, ФИО и т.д.).

3.3.2. Передача конфиденциальных данных должна осуществляться с помощью метода POST. Запрещается использование метода GET для передачи сведений конфиденциального характера. Возможность использования GET api-интерфейсов, передающих конфиденциальные данные, необходимо определять в соответствие с архитектурой системы, критичностью передаваемых данных, количества пользователей и др. параметров характерных для конкретного случая.

3.3.3. Запрещается использование «секретных» HTTP параметров (*debug=true, admin=1* и т.д.) для перевода web-приложения в режим отладки, администрирования или получения доступа к неподдерживаемому в обычном режиме функционалу.

3.3.4. Запрещается передавать конфиденциальные данные в рамках перенаправления (редиректа) на другие web-ресурсы.

3.4. Передача учетных данных

3.4.1. Передача учетных данных пользователя и другой аутентифицирующей информации должна осуществляться по защищённому протоколу TLS.

4. Требования к сессиям

4.1. Требования к идентификаторам сессий (Session ID)

4.1.1. Идентификатор сессии должен быть уникальным и не предугадываемым. Запрещается использование идентификаторов сессий, сформированных с помощью простого или известного алгоритма (инкрементирование, системное время и т.д.).

4.1.2. Идентификатор сессии должен быть устойчив к подбору. Длина идентификатора сессии должна быть не менее 128 бит.

4.1.3. Идентификатор сессии не должен зависеть от других идентификаторов (сформированных ранее), имени пользователя, пароля, состояния приложения.

4.1.4. Клиентская часть web-приложения не должна иметь возможность менять идентификатор сессии.

4.1.5. В случае, когда web-приложение использует SSL/TLS для передачи данных, идентификатор сессии должен всегда передаваться внутри защищённого соединения.

4.1.6. Новый идентификатор сессии должен формироваться приложением каждый раз после прохождения успешной аутентификации пользователя. В случае, когда пользователь в процессе аутентификации передает заранее сформированный идентификатор сессии, он должен быть проигнорирован.

Данное требование существует в целях исключения влияние пользователя на процесс генерации идентификатора сессии.

4.2.Управление сессиями

4.2.1. Время жизни сессий должно быть ограничено. По истечении данного времени, сессия должна быть удалена или должен быть сгенерирован новый запрос на обновление аутентификации. Значение необходимо определять в соответствие с критичностью передаваемых данных, количества пользователей и др. параметров характерных для конкретного случая.

4.2.2. Неактивные сессии должны завершаться автоматически. Время завершения сессии настраивается в зависимости от функционала веб-приложения, количества пользователей, критичности обрабатываемых ресурсов. Рекомендуемое значение для административных консолей – 5 мин, для пользовательского веб-интерфейса 30 мин.

4.2.3. Web-приложение на клиентской стороне не должно искусственно поддерживать сессию в активном состоянии, предотвращая ее автоматическое завершение по таймауту неактивности.

4.2.4. Необходимо использовать встроенные в стандартные библиотеки и механизмы управления сессиями в случае наличия таковых. Реализация собственных механизмов управления сессиями не рекомендуется.

4.2.5. Для предотвращения кражи или модификации данных о сессиях пользователей web-приложения, эти данные должны храниться в месте не доступном для других приложений и систем (в том случае, если они не защищены другим способом, например, путем шифрования). К недопустимым местам хранения, в частности, относятся общие папки с временными файлами на web-сервере.

4.2.6. Разрешается использование 2-х ступенчатых механизмов, когда веб-приложение с помощью постоянных cookies помнит некоторые настройки пользователя и применяет их при следующем посещении. Однако для доступа к персональным данным или совершения транзакций по-прежнему требуется прохождения стандартной процедуры аутентификации и проверки прав.

4.2.7. Возможность использование механизмов «запомнить меня» для включения механизма автоматической аутентификации необходимо определять в соответствие с критичностью передаваемых данных, количества пользователей и др. параметров характерных для конкретного случая.

4.2.8. В случае, если веб-приложение использует клиентские сертификаты для аутентификации пользователей (или другие механизмы, при которых кража идентификатора сессии не ведет к получению доступа в контексте пользователя приложения), могут быть установлены специальные требования к механизму управления сессиями.

4.3. Завершение сессий

4.3.1. Web-приложение должно содержать механизм завершения сессии (кнопка выход), доступный пользователю из любой страницы приложения.

4.3.2. По завершении сессии относящиеся к ней конфиденциальные данные должны быть полностью удалены на серверной стороне.

4.3.3. Сессия, содержащая конфиденциальные данные, должна автоматически завершаться при закрытии браузера.

4.3.4. Рекомендуется удалять сессионные данные на ПК клиента.

5. Требования к использованию протокола HTTP

5.1. Общие требования

5.1.1. Web-приложение должно поддерживать минимально необходимый набор HTTP-методов. Неиспользуемые HTTP-методы должны быть отключены на web-сервере, а попытки их использования должны игнорироваться.

5.1.2. Необходимо использовать на web-сервере опцию протокола:

– *HTTP X-Content-Type-Options: nosniff.*

5.2. Требования к использованию cookies

5.2.1. Атрибут *HTTPOnly* должен быть установлен значением true.

5.2.2. В случае использования протокола HTTPS должен быть установлен флаг *secure*.

5.2.3. Атрибут *domain* должен быть установлен значением только того ресурса, для которого требуется поддержка данного cookie. Например, если приложение располагается на домене market.pochta.ru, то связанный с ним cookie должен иметь значение параметра «*domain=market.pochta.ru*», а не «*domain=.pochta.ru*».

5.2.4. Атрибут *path* должен быть настроен таким образом, чтобы браузер клиента отправлял cookies только тому web-приложению, которому они предназначаются.

6. Требования к HTML

6.1. Требования к комментариям и скрытым полям HTML

6.1.1. HTML-комментарии не должны содержать внутреннюю информацию web-приложения (IP-адреса, логины, пароли, адреса электронной почты, телефоны) а также раскрывать особенности реализации системы.

6.1.2. В скрытых полях HTML-страниц в незашифрованном виде запрещается передавать конфиденциальные сведения (номера кредитных карт, номера телефонов и т.д.), аутентификационные данные (имя пользователя, пароль, токен аутентификации), а также управляющие команды, которые могут нарушить работу web-приложения (теги, SQL-операторы, shell-команды).

6.2. Требования к всплывающим окнам (pop-up)

6.2.1. Использование всплывающих окон (Pop-up) для реализации логики web-приложений должно быть ограничено. В случае крайней необходимости всплывающие окна должны использоваться только для отображения информационных сообщений.

6.2.2. Запрещается использование всплывающих окон для получения данных от пользователя.

6.3. Требования к фреймам

6.3.1. Для вводимых в эксплуатацию веб-приложений должна быть включена опция *X-Frame-Options: deny*, запрещающая внедрение web-приложения в iframe предотвращая Clickjacking атаки. Для уже внедренных в случае передачи контента в Iframe необходимо использовать *X-Frame-Options: SAMEORIGIN*, разрешающих передавать в iframe контент своих веб-страниц.

7. Криптография

7.1. SSL/TLS и сессии

7.1.1. В случае, если web-приложение использует HTTPS для защиты взаимодействия с клиентом, доступ к ресурсам по HTTP должен быть запрещен. При этом рекомендуется использовать опцию *Strict-Transport-Security* на web-сервере для предотвращения возможности использования HTTP на уровне web-сервера. В качестве криптографического протокола необходимо использовать TLS v. 1.2.

7.1.2. В случае перенаправления пользователя с защищенных ресурсов web-приложения (доступных только по HTTPS) на незащищенные (доступные по HTTP) сессия клиента должна быть либо завершена, либо должны быть удалены конфиденциальные данные, используемые в рамках сессии. Подобные обстоятельства возникают в случае если часть ресурсов веб-приложения доступна по HTTP, а часть защищена HTTPS, чего в обычной практике лучше избегать. Рекомендуемая мера не позволяет атакующему получить доступ по HTTP к web-страницам, защищенным HTTPS.

7.1.3. Конфиденциальная информация (например, пароли, детализации разговоров, финансовые отчеты, персональные данные и др.) должна передаваться только по защищенному протоколу HTTPS.

7.1.4. Использование гиперссылок, перенаправляющих с защищенных web-страниц приложения (доступных только по HTTPS) на незащищенные, не должно приводить к появлению конфиденциальных сведений в поле HTTP-referer.

8. Требования к архитектуре

8.1. Требования к контролю состояний процессов

8.1.1. Web-приложение должно контролировать состояние, на котором находится клиент. Нелегитимные переходы между состояниями процессов должны быть заблокированы (переход к оплате без выбора товара или заполнения данных о клиенте и т.д.).

8.1.2. Рекомендуется реализовывать механизм контроля состояний процессов на серверной стороне web-приложения.

8.1.3. Индикатор состояния должен быть уникальным и не являться предугадываемым.

8.1.4. Запрещается использовать содержимое HTTP-referer для контроля состояния процессов.

8.2. Скрытые и замаскированные ресурсы

8.2.1. Все страницы и активные скрипты web-сервера, к которым пользователь может получить доступ должны быть частью web-приложения. Пользователю не должны быть доступны web-страницы, директории, файлы, непосредственно не принадлежащие приложению, а также:

- файлы резервных копий (например, *.old, *.bak);
- файлы баз-данных (например, *.db, *.sqlite, *.accdb);
- лог-файлы;
- временные директории;
- исходные коды и директории SVN;
- используемые библиотеки.

8.2.2. Запрещается ограничивать доступ к файлам путем переименования файлов или путем не указания гиперссылок на них.

8.2.3. Запрещается оставлять неиспользуемые директории и файлы на продуктивном сервере (например, файл login.php.old или директория jsp.old).

8.3. Требования к регистрации пользователей

8.3.1. Форма регистрации клиентов в web-приложении должна быть защищена от автоматических средств регистрации (CAPTCHA или альтернативные решения для защиты).

8.4. Требования к аутентификации

8.4.1. Учётные данные не должны храниться в местах, доступных для клиента (cookies, URL, исходный код и т.д.).

8.4.2. Процесс аутентификации не должен основываться на данных и переменных, которые можно легко модифицировать (HTTP заголовки, user-agent, HTTP-referer и т.д.).

8.4.3. При начальной регистрации пользователя или восстановлении утерянного пароля необходимо предусмотреть возможность проверки его сложности.

8.4.4. Для доступа к разделам, связанным с пользовательской информацией и выполнением действий от лица пользователя необходима обязательная аутентификация.

8.4.5. Процедура аутентификации должна иметь защиту от подбора паролей (CAPTCHA, POW задержка на повторный ввод или временный запрет на доступ). Количество неудачных попыток ввода пароля и время блокировки повторного ввода пароля должны быть настраиваемыми параметрами с стороны администратора Системы.

8.5. Требования к авторизации

8.5.1. Web-сервер, на котором работают web-приложения и сервер СУБД (по возможности), должен быть запущен под специально созданной технологической учетной записью ОС с минимально необходимым набором привилегий. Запуск web-сервера под системными учетными записями (например, root или LOCALSYSTEM) может вести к серьезным уязвимостям.

8.5.2. Для предотвращения полной компрометации сервера в случае взлома web-приложения пользователю СУБД, под которым работает веб-приложение, необходимо предоставлять ограниченные права на работу с файловой системой сервера (на функции создания, чтения, удаления, изменения файлов), а также исполнение команд ОС с помощью вызова хранимых процедур или путем использования библиотек.

8.6. Взаимодействие между компонентами

8.6.1. При обращении к базам данных web-приложения должны использовать хранимые процедуры, вместо SQL запросов содержащих параметры.

8.6.2. Хранение паролей в БД веб-приложения должно осуществляться с использованием криптографических алгоритмов, определяемых в соответствии с пунктом 4.1.1 Стандарта «Обеспечение информационной безопасности при разработке или модернизации информационных систем и приложений ФГУП «Почта России».

8.6.3. Доступ к веб-интерфейсам администрирования web-приложений из сети интернет должен быть запрещен.

8.6.4. Административные и пользовательские интерфейсы должны быть разделены. Пользовательский интерфейс не должен предоставлять возможностей администрирования Системы.

8.6.5. Web-интерфейсы систем мониторинга (Nagios, Zabbix, Cacti, Munin и др.) не должны быть доступны из сети Интернет.

8.7. Контроль состояния клиента

8.7.1. Должен использоваться механизм контроля состояния клиента, путем присвоения клиенту начального идентификатора состояния (при начале работы с приложением) и его последовательного изменения в процессе работы. При этом клиенту передается зашифрованный параметр (токен), содержащий сведения о текущем состоянии клиента, который в свою очередь передается серверу при каждом обращении.

8.7.2. Если механизм управления состоянием используется на стороне клиента, параметр контроля состояния клиента (идентификатор состояния или токен) должен быть зашифрован.

8.8. Сокрытие внутренней структуры

8.8.1. В целях сокрытия внутренней информации web-приложения от злоумышленников (структуры приложения, правил именования файлов) запрещается использовать прямое, легко угадываемое именование содержимого (например, Report-2013.xls, Report-2014.xls и т.д.).

8.8.2. Необходимо контролировать отсутствие информации о внутренней структуре Системы или сети Предприятия в ответах и страницах web-приложений Системы.

Приложение № 2
к Стандарту «Обеспечение информационной
безопасности при разработке или модернизации
информационных систем и приложений
ФГУП «Почта России»

Требования к схеме сетевой архитектуры Системы

Схема должна содержать следующие элементы:

– Компоненты ИС предоставляющие сервис или нуждающиеся в доступе (сервера или кластера серверов Системы, сервера СУБД, сервера внешних Систем, с которыми взаимодействует внедряемое решение, рабочие станции администраторов, рабочие станции пользователей, сетевое оборудование и другие устройства);
– IP адреса, FQDN компонентов ИС;
– Информационные потоки между компонентами ИС;
– Модели оборудования компонентов ИС.

Приложение № 3
к Стандарту «Обеспечение информационной
безопасности при разработке или модернизации
информационных систем и приложений
ФГУП «Почта России»

Образец таблицы IP адресов компонентов Системы

Таблица IP адресов компонентов Системы (IP план Системы) должна включать следующую информацию:

- IP адрес (IP address) и Тип IP (virtual IP или real IP);
- FQDN;
- VLAN;
- Назначение интерфейса/хоста (Комментарий).

IP address	FQDN	VLAN	Комментарий
10.20.444.4	server1.inside.russianpost.ru	ServOS	Адрес сетевой карты первого сервера приложений ИС, используемый для организации IPMP
10.20.444.66	--/--	--/--	Адрес демона IPMP ОС Solaris. Не используется для организации сетевого взаимодействия
10.20.444.12	server2.inside.russianpost.ru	ServOS	Адрес сетевой карты второго сервера приложений ИС, используемый для организации IPMP
10.20.444.68	--/--	--/--	См. 10.20.444.66
10.20.444.70	server3.inside.russianpost.ru	ServOS	Сетевой адрес базы данных Oracle, принимающий подключения от серверов приложений
10.20.246.246	web.russianpost.ru	DMZ	Сетевой адрес внешнего сервера ИС, принимающего подключения от внешних пользователей к web-службам

Приложение № 4
к Стандарту «Обеспечение информационной
безопасности при разработке или модернизации
информационных систем и приложений
ФГУП «Почта России»

Требования к таблице информационных потоков/доступов Системы

Таблица информационных потоков/доступов Системы должна включать следующую информацию:

- IP адрес (IP address) и Тип IP (virtual IP или real IP);
- FQDN;
- Входящий или исходящий поток;
- Протокол (TCP, UDP, ICMP и т.п.);
- Номер порта;
- Назначение потока (Комментарий).

Source FQDN	Source IP	NATed Source IP	NATed Destination IP	Destination IP	Destination FQDN	Transport or Network protocol	Application protocol	Source Port	Destination Port	Description
server5.inside.rus-sianpost.ru	10.20.445.8			10.242.8.12	sql5.russianpost.ru	TCP	PL/SQL	Any	1443	Передача данных на сервер агрегации данных
web.russianpost.ru	10.20.246.246			10.242.8.12	web4.russianpost.ru	TCP	HTTP	Any	80	Доступ пользователей к личным кабинетам на web-портале
web2.russianpost.ru	10.20.246.247	172.18.11.114 172.18.11.115 172.18.11.116	172.18.8.12	10.242.8.12	webadm.rus-sianpost.ru	TCP	HTTPS	Any	443	Администрирование web-портала

Приложение № 5
к Стандарту «Обеспечение информационной
безопасности при разработке или модернизации
информационных систем и приложений
ФГУП «Почта России»

Пример описания реализации требований Стандарта

Пункт Стандарта	Требования (вопросы)	Реализация (ответ)
Общие требования		
6.1.2.	Перечислите полные названия/версии всех компонентов ИС и ПО третьих производителей, используемого в составе ИС.	Oracle Database 11.2.0.1 (Сервер БД) , Solaris 10 Release 9 (ОС сервера БД), openldap 2.4.21 (каталог пользователей), Windows 2003 SP2 + IIS6 (сервер приложений)
Требования к аутентификации и авторизации		
6.2.1.	Позволяет ли ИС предоставить уникальную учетную запись каждому пользователю, по которой его можно однозначно идентифицировать?	Да.
6.2.2.	Перечислите механизмы/средства аутентификации поддерживаемые ИС и ее компонентами (собственные, Kerberos, NTLM, LDAP и т.д.)?	LDAPs
6.2.3.	К каким объектам ИС позволяет разграничить доступ (пользователи, отчеты, документы и т.д.)? Какие права можно задать на объекты ИС (полный доступ, чтение, редактирование, запуск и т.д.)?	Отчеты, данные (полный доступ, чтение)
6.2.4.	Какая модель доступа используется в ИС (мандатная, ролевая, групповая)?	групповая
6.2.5.	Имеются ли в ИС процессы/сервисы, которые не используют аутентификацию? Имеются ли в ИС процессы/сервисы, которые не используют авторизацию?	Да. Вызов Web служб по протоколу SOAP не использует авторизации
6.2.7.	Предоставляет ли ИС возможность пользователю сменить свой пароль самостоятельно?	Да
6.2.7.	Предоставляет ли ИС возможность обязательной смены первичного пароля пользователя заданного администратором при первом входе в систему?	Нет
6.2.7.	Позволяет ли ИС установить требования к сложности пароля (количество символов, наличие строчных и заглавных букв, цифр, служебных символов и т.д.)? Какие? Требования устанавливаются на пользователя или на группу?	Да

6.2.7.	Позволяет ли ИС осуществлять принудительную смену пароля через заданный промежуток времени?	Нет
6.2.7.	Имеет ли ИС возможность автоматической блокировки пользователя, если пароль установленной даты не был изменен?	Нет
6.2.7.	Имеет ли ИС возможность заблаговременно оповещать пользователей о необходимости смены пароля?	Да
6.2.7.	Обеспечивает ли ИС хранение истории паролей пользователей для предотвращения повторного их использования? За какой период?	Нет
6.2.7.	Обеспечивает ли ИС блокирование пользователя после заданного количества неудачных попыток аутентификации?	Да
6.2.7.	Позволяет ли ИС задавать длительность простоя пользовательской сессии, после которого сессия принудительно завершается?	Да
6.2.7.	Позволяет ли ИС ограничить множественный вход под одной учетной записью?	Нет
6.2.8.	Какие криптографические алгоритмы используются при хранении/передаче паролей пользователей?	TLS (web форма)
6.2.9.	Выдает ли ИС информацию о типе и версии системы или ее компонент до успешного завершения процедур аутентификации и авторизации?	Нет
6.2.10.	В случае обнаружения ошибки при проверке логина и пароля пользователя, уточняет ли ИС, какие именно данные введены неправильно? Отображается ли пароль при вводе?	Нет
6.2.11.	Имеются ли в ИС и ее компонентах жестко запрограммированные учетные записи?	Нет
6.2.12.	Проходят ли компоненты ИС процедуру взаимной аутентификации в случае сетевого взаимодействия?	Нет
6.2.13.	Проверка/валидация учетных данных пользователя проводиться на стороне серверных компонентов ИС?	Да
Требования к аудиту		
6.3.1.	Поддерживает ли ИС синхронизацию с NTP-сервером (собственными средствами, средствами ОС и т.д.)?	Да. Средствами ОС
6.3.2.	Имеется ли в ИС система аудита действий пользователей?	Да
6.3.3.	Позволяет ли ИС хранить журналы аудита за 90 дней в собственном хранилище? Предоставляет ли ИС возможность сохранять журналы аудита во внешних системах (syslog, SQL, SNMP и др.)?	Да. Внешнее хранилище - нет

6.3.4.	Протоколирование каких событий осуществляется в ИС (вход/выход, запуск/останов и т.д.)? Если журналов аудита несколько (от нескольких подсистем) - перечислите все.	Вход, выход, запрос отчета, запрос данных. Плюс все стандартные логи аудита Oracle и IIS6
6.3.5.	Какую информацию протоколируют журналы аудита (дата, IP, объект и т.д.)? Если журналов аудита несколько (от нескольких подсистем) - перечислите все.	Для ИС. Пользователь, дата, объект, действие, результат
6.3.6.	Позволяет ли ИС обрабатывать (просматривать, фильтровать и т.д.) журналы аудита внутренними средствами?	Нет
6.3.8.	Записывает ли ИС в журналы аудита данные конфиденциального характера (например, ФИО абонента, MSISDN, пароль пользователя и т.д.)?	Нет
6.3.9.	Можно ли редактировать журналы аудита (внутренними или третьими средствами)?	Да
7.1.5.	Позволяет ли ИС отключить аудит действий пользователей?	Нет
Требования к сетевому взаимодействию		
6.4.1.	Необходим ли ИС для штатного функционирования доступ к сетям общего пользования (Интернет)? Если да, то какие протоколы и для каких целей используются?	Нет
6.4.3.	Предполагается ли расположение ИС в демилитаризованной зоне сети (DMZ)?	Нет
6.4.4.	Какие протоколы и средства используются при взаимодействии между компонентами ИС (клиенты, БД, подсистемы и т.д.)?	LDAPs, SQL/Net, HTTPs, HTTP, SOAP
6.4.4.	Какие протоколы и средства используются для обмена данными между ИС и внешними системами Компании (LDAP, Sun Java CAPS, Web-services и т.д.)?	Внешние системы не используются. Система автономна и не интегрирована с другими ИС
6.4.6.	Имеются ли компоненты ИС, подключенные одновременно в разные сетевые периметры с разными уровнями безопасности (например в DMZ и корпоративную сеть)?	Нет
Требования к конфиденциальности, целостности и доступности данных		
6.5.1.	Поддерживает ли ИС транзакционность операций над критичными данными?	Да
6.5.2.	Какие компоненты ИС поддерживают установку в кластерном режиме?	IIS6
6.5.3.	Содержит/обрабатывает ли ИС данные, относящиеся к коммерческой тайне Компании или конфиденциальной информации (см. перечень данных в ПТ-002 Приложения 5 и 6)? (Например, Персональные данные, Планы и отчеты подразделений Компании, Условия договоров, Финансовая информация)	Да. Персональные данные абонентов. Финансовые отчеты
6.5.3.	Предоставляет ли ИС встроенные средства шифрования собственных данных? Если да, то	Нет

	какие алгоритмы используются при шифровании?	
6.5.4.	Проходит ли данные (параметры, аргументы, переменные, файлы и т.д.) полученные системой обязательную процедуру валидации? По каким параметрам проходит валидация данных (тип, длинна и т.д.)? В какой момент осуществляется валидация?	Да (длинна, запрещенные символы). Валидация осуществляется до момента отправки запроса на IIS
6.5.6.	Позволяют ли ИС отключить детальный вывод информации об ошибках (версии подсистем, таблицы БД, сетевые адреса компонент ИС и т.д.), выдаваемых пользователю?	Да
6.5.7.	Предоставляет ли ИС встроенные средства создания резервных копий данных и настроек ИС? Если нет, то какие третьи средства рекомендуются к использованию?	Встроенных средств нет. Резервирование осуществляется внешними средствами
6.5.8.	Поддерживается ли штатная работа ИС в момент создания резервной копии?	Да
6.5.9.	Позволяет ли ИС автоматически шифровать резервируемые данные? Если да, то какие алгоритмы при этом используются?	Нет
Требования к обновлениям и изменениям		
7.3.1.	Укажите среднюю частоту выпуска обновлений безопасности ИС.	3 мес.
7.3.1.	Какое время занимает тестирование обновлений безопасности третьих производителей (ОС, БД и т.д.) на совместимость с ИС?	1 мес.
7.3.1.	Входит ли установка обновлений третьих производителей (ОС, БД и т.д.) в рамки технической поддержки ИС?	Да. В составе обновлений системы