МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Э. БАУМАНА
Факультет **Информатика и системы управления**
Кафедра **Информационная безопасность**

# Расчётно-пояснительная записка к дипломному проекту

«Создание средств обеспечения информационной безопасности при совместной работе пользователей в системе электронного документооборота на основе теории массового обслуживания»

Листов 80

Выполнил:
Карташов В.Е.

Руководитель:
Гудков О.В.

Москва
2014

# Содержание

# ПРИНЯТЫЕ СОКРАЩЕНИЯ

**АС** — автоматизированная система
**ПО** — программное обеспечение
**НСД** — несанкционированный доступ
**КХЭД** — конфиденциальное хранилище электронных документов
**СКЗИ** — средство криптографической защиты информации
**СЭД** — система электронного документооборота
**ХЭД** — хранилище электронных документов
**ЭД** — электронный документ
**ЭП** — электронная подпись
**CRL** — список отозванных сертификатов

# Введение

***Документооборот*** — движение документов в организации с момента их создания или получения до завершения исполнения или отправления [1]. Документооборот является неотъемлемой частью рабочего процесса любой компании любого масштаба. При выполнении производственных задач, организации процессов внутрии компании, коммуникации с контрагентами и органами государственной власти используются документы. Правильная организация документооборота способна повысить эффективнсть работы предприятия и оптимизировать временные и материальные затраты.

В течение последнего десятилетия наблюдается постепенный переход от бумажного документооборота к электронному. Это может проявляться как в полном или частичном отказе от бумажных версий документов, так и в дублировании бумажных копий электронными. Положительные моменты этого процесса — такие, как повышение скорости обработки документов и снижение материально-временных затрат на создание, хранение и передачу документов — компенсируются сложностями в обеспечении информационной безопасности электронных документов. Так, необходимо обеспечить защиту от несанкционированного доступа к хранилищу документов и каналу передачи данных, создать средства подтверждения авторства документа. Данный вопрос лежит как в технической, так и в правовой области.

Очевидна необходимость в создании системы электронного документооборота, сохраняющей описанные достоинства и минимизирующей недостатки, т.е. такой системы, которая будет обеспечивать как осуществление процесса электронного документооборота, так и безопасность обрабатываемых данных.

Основными задачами дипломного проектирования являются:

- проведение анализа угроз и средств противодействия им для систем электронного документооборота;
- осуществление выбора показателей эффективности реализации модулей системы электронного документооборота;
- выбор методов обработки данных в системе электронного документооборота;
- разработка программного обеспечения для защиты данных в системе электронного документооборота;

- проведение анализа нормативно-правовых актов в области информационной безопасности Российской Федерации;
- проведение организационно-экономического анализа проектной разработки, оценка структуры и показателей затрат дипломного проекта, исследования рынка.

# Глава 1

# ИССЛЕДОВАТЕЛЬСКАЯ ЧАСТЬ

## 1.1 Введение

Для организации процесса электронного документооборота создаются программные и программно-аппаратные комплексы. Для решения задач информационной безопасности они так или иначе используют средства криптографической защиты информации. Однако среди используемых СКЗИ встречаются в основном средства, основанные на технологии Microsoft CryptoAPI — криптопровайдеры, совместимые только с ограниченным наобором операционных систем Microsoft Windows. Более того, эти средства применяются только для решения двух наиболее очевидных задач: обеспечения работы с электронной подписью в соответствии с Федеральным законом №63 «Об электронной подписи» и защиты канала передачи данных между хранилищем электронных документов и операторами системы. Без внимания остаются другие вопросы безопасности — такие, как, например, обеспечение целостности хранимой истории изменений, внесённых в документ.

В то же время, открытый подход к разработке программного обеспечения (когда любой желающий может просмотреть исходные тексты и предложить свои изменения) доказал свою состоятельность: к примеру, операционные системы, разработанные таким образом, используются в Роскосмосе [2]. Плюсы данного подхода очевидны: за счёт открытости исходных текстов для так называемых «белых хакеров» и программистов по всему миру в итоговом ПО присутствует меньше ошибок по сравнению с аналогами. Разработанное таким способом ПО после внесения некоторых правок может быть сертифицировано и распространяться в соответствии с законодательством РФ. Системы электронного документооборота не подлежат обязательной сертификации, а значит, для их использования достаточно лишь задействовать сертифицированные СКЗИ.

Для системы электронного документооборота немаловажным является фактор скорости передачи и обработки данных, дающий СЭД преимущество перед классическим бумажным документооборотом.

Система электронного документооборота может быть разделена на модули, каждый из которых выполняет ту или иную операцию. Для каждого модуля исходя из особенностей его работы можно оценить набор угроз, и в соответствии с этими угрозами определить набор средств противодействия им.

При создании СЭД важно учитывать, что в системе обрабатываются данные, составляющие коммерческую, служебную, производственную, и другие виды тайн. Важно обеспечить защиту этих данных как в канале передачи данных, так и в локальном хранилище пользователя и сервера.

Таким образом, **целью дипломного проектирования является создание средств обеспечения информационной безопасности для системы электронного документооборота, удовлетворяющих современным требованиям по быстродействию и защите информации**.

## 1.2 Обзор существующих систем электронного документооборота

### 1.2.1 Назначение и основные свойства систем электронного документооборота

Документооборот включает в себя:

- создание
- обработку
- хранение
- передачу
- вывод документов.

Соответственно, в задачи системы документооборота входит обеспечение этих процессов, причём в разных системах упор делается на разные стадии. Это происходит за счёт интеграции со сторонними средствами – например, средствами сканирования и распознавания текста.

К основным свойствам СЭД относят:

- Открытость;

  СЭД строятся по модульному принципу, что позволяет подстраиваться под требования к системе, совершенствовать отдельные модули и интегрироваться со сторонними модулями.

- Высокая степень интеграции с прикладным программным обеспечением;

  Снижает затраты на обучение сотрудников: последние работают с привычным ПО, которое, в свою очередь, взаимодействует с СЭД.

- Организация хранения документов;

  К этому вопросу можно подойти разносторонне, но в основном выделяют три реальных модуля хранения данных, взаимодействующих между собой:

  - Хранилище документов;
  - Хранилище атрибутов документов;
  - Сервисы индексации и поиска.

На их основе можно строить виртуальные сущности вроде работы с привязанными к ней документами.

- Организация маршрутизации документов;

  В зависимости от решаемых задач, маршрутизация может быть свободной (меняться по мере работы с документом) или жёсткой (задаваться при создании задачи, без права исполнителя изменить маршрут).

- Разграничение доступа;

  Один из основных механизмов, обеспечивающих безопасность обрабатываемой информации – контроль доступа. Основные виды полномочий:

  - Полный контроль документа;
  - Разрешение на редактирование;
  - Разрешение на создание новых версий;
  - Право на чтение;
  - Право на доступ к учётной карточке, без разрешения на редактирование документа;
  - Право на доступ к карточке без доступа к документу;
  - Полный запрет на работу с документом.

  В зависимости от конкретной СЭД набор параметров может различаться.

- Поддержка версионности документов;

  Важное свойство для хранения достоверной истории и подтверждения авторства пользовательских изменений.

- Поддержка различных форматов данных;

  В зависимости от компании и решаемой задачи формат рабочего документа может варьироваться от ODT/DOCX до TeX и даже CAD. Выбор СЭД обуславливается в частности и поддержкой нужных форматов.

- Аннотирование документов.

  Полезное свойство для гибкости разграничения доступа: в некоторых ситуациях доступ к редактированию документа может быть излишним, но возможность добавления комментариев решает эту проблему.

### 1.2.2 Классификация систем электронного документооборота

По классу решаемых задач выделяют СЭД:

- Ориентированные на бизнес-процессы

  Развитое управление и процессами, и содержимым в контексте отрасли.

- Корпоративные

  Общекорпоративные системы.

- Системы управления содержимым

  Объектом является документ.

- Системы управления потоком работ

  Объектом является работа.

- Системы управления образами

  Большое внимание уделяется вводу документов из бумажных форм (в виде отсканированных изображений) и перевод их в электронный вид.

- Системы управления корпоративными электронными записями

  Работа с неизменяемыми данными (например, денежными транзакциями).

По способу распространения СЭД делятся на

- Коробочные

  Универсальные системы, которые потребитель может настроить для своих нужд самостоятельно.

- Проектные

  Системы «под заказ», разворачиваются и адаптируются индивидуально для предприятия.

### 1.2.3 Вопросы информационной безопасности

В любой системе электронного документооборота должны присутствовать базовые функции безопасности:

- Идентификация и аутентификация пользователей;

  Иначе применение СЭД бессмысленно

- Защита каналов передачи данных;

  Для противодействия атакам типа «человек посередине»

- Поддержка средств добавления и проверки электронной подписи;

  Для обеспечения юридической значимости обрабатываемым документам

- Строгое журналирование;

  Вместе с системой идентификации/аутентификации должно обеспечиваться жёсткое связывание автора и сделанных им изменений. При этом отмена изменений должна быть новой записью в журнале, а не отменой предыдущей.

- Резервирование сервисов (серверных средств), в т.ч. горячее.

  Для обеспечения свойства доступности

Помимо этого, если в системе обрабатываются данные, защита которых предусмотрена действующим законодательством, должны выполнятся и соответствующие требования.

### 1.2.4 Рынок СЭД в Российской Федерации

В Таблице 1.1 рассмотрены некоторые параметры крупнейших СЭД, представленных на российском рынке. Основное внимание уделено универсальности требований к среде исполнения и обеспечению информационной безопасности.

В целях быстрого захвата рынка большинство СЭД ориентируются на текущие ресурсы предприятий: в качестве целевой ОС используется Microsoft Windows, в качестве системы учёта задач и базы данных – Lotus и MS SQL / Oracle. Активное развитие мобильных операционных систем побуждает производителей выпускать клиенты для Android/iOS, а также веб-интерфейс для управления задачами. Функциональность таких версий обычно урезана: например, они не позволяют добавлять к документу цифровую подпись. Однако разработчики забывают учесть три важных фактора:

- В качестве стандарта для офисных приложений выбран формат ODT (ГОСТ Р ИСО / МЭК 26300 — 2010), который не поддерживается Microsoft Office;

- Для государственных и бюджетных учреждений использование ПО Microsoft является дополнительной крупной статьёй расхода, избежать которой помогает свободное программное обеспечение;

- ПО Microsoft не имеет сертификата Министерства Обороны, что накладывает дополнительные ограничения на использование указанных СЭД.

В части обеспечения безопасности обрабатываемой информации все СЭД располагают базовым набором функций:

- Шифруется канал передачи данных между клиентом и сервером;
- Используются средства добавления и проверки электронной подписи;
- Применяются механизмы разграничения доступа.

Однако, несмотря на работу с электронной подписью, не все СЭД располагают встроенным средством контроля целостности. В частности, это раскрывается в работе с версиями одного и того же документа: ЭП обычно используется при создании выходного документа, однако в процессе работы контроль целостности и подтверждение авторства отдаётся на откуп внутренним механизмам СЭД, которым можно доверять с ограничениями. В результате получаем систему, в которой возможен отказ от авторства, а в некоторых случаях и анонимное изменения документа или, наоборот, откат сделанных изменений без должного журналирования.

Что же касается последнего пункта, то и здесь часто применяются полумеры. Очевидно, что разграничение доступа в базовом виде «писать вверх, читать вниз» есть во всех системах. Почти везде есть средства делегирования полномочий. Но когда дело доходит до более сложных процессов и требуется более дифференцированное разграничение доступа, значительная часть СЭД перестаёт удовлетворять требованиям. Это касается таких возможностей, как:

- Право создавать задачи и документы, но не подписывать (завершать) их;
- Право комментировать результаты, но не вносить изменения в тело документа;
- Право просматривать атрибуты документа, но не его содержание;
- Право изменять часть параметров документа, но не все атрибуты вместе;
- Право работать с документом без доступа к части атрибутов документа;
- И т.д.

Всё это позволяет сделать вывод о целесообразности создания новой системы электронного документооборота, основанной на открытых технологиях и решающей перечисленные проблемы.

## 1.3 Исследование СЭД с точки зрения теории массового обслуживания

### 1.3.1 Общая схема электронного документооборота

Процесс документооборота можно представить в виде графа, изображённого на рис. 1.1. Вершинами в нём являются редакторы, а дугами — переходы задания на разработку документа

Таблица 1.1: Существующие решения

| СЭД | Платформа | Поддержка клиент-ских ОС | Поддержка серверных ОС | Лицензия | Разграничение доступа |
|---|---|---|---|---|---|
| Босс-референт | Lotus / MS SharePoint / JBOSS | Windows / Linux / Mac OS X | Windows / Linux | Проприетарная / СПО | По документам |
| 1С: Документо-оборот | 1С: Пред-приятие | Windows | Windows | Проприетарная | По документам |
| CompanyMedia / OfficeMedia | Lotus | Любые | Windows / Linux | Проприетарная | ? |
| Effect Office | Microsoft | Windows | Windows | Проприетарная | На уровне разделов и рубрик |
| LanDocs | Oracle / Microsoft | Windows | Windows | Проприетарная | Полное |
| Дело (ЭОС) | 1С / MS SharePoint / Oracle | Windows | Windows | Проприетарная | Полное |
| DIRECTUM | Microsoft | Windows | Windows | Проприетарная | Полное |
| OPTIMA - WorkFlow | MS / Oracle | Windows | Windows | Проприетарная | ? |
| DocVision | MS / Oracle | Windows | Windows | Проприетарная | Полное |

между редакторами в соответствии с принятой в организации структурой. Весам дуг соответствуют вероятности этих переходов. Обратные связи демонстрируют возвращение документа на переработку. Вершинами «Старт» и «Финиш» обозначены момент получения задания и завершение исполнения соответственно.

Ниже будет рассмотрена система электронного документооборота.

***Электронный документ*** — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах [3].

***Система электронного документооборота (СЭД)*** — автоматизированная система, реализующая процесс документооборота применительно к электронным документам.

Для организации системы электронного документооборота необходимо разработать ряд технических средств, среди которых хранилище электронных документов (ХЭД). В настоя-

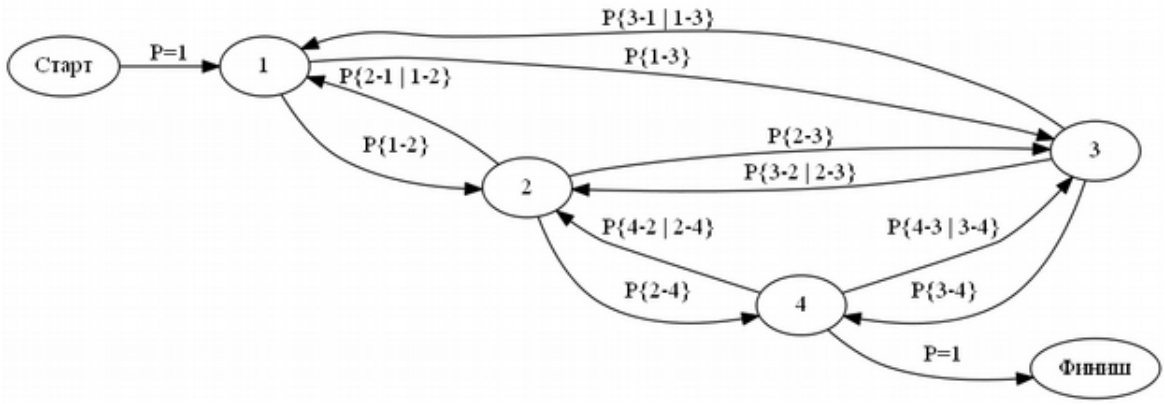


Рисунок 1.1: Характерный вид процесса документооборота

щее время электронный архив (одно из распространённых названий ХЭД) позиционируется как независимый компонент, способный быть как отдельным комплексом, заменяющим собой бумажный архив документов, так и основой для СЭД. Данный подход позволяет конструировать гибкую систему электронного документооборота из независимых модулей.

При проектировании ХЭД следует учитывать законодательно-нормативные требования, касающиеся информационной безопасности хранимых электронных документов. Это обстоятельство позволяет конкретизировать определение ХЭД как **конфиденциальное хранилище электронных документов (КХЭД)** – систему кратковременного и долговременного конфиденциального хранения электронных документов, предоставляющую возможности по защите от несанкционированного доступа (НСД), контролю доступа, обеспечению юридической значимости электронных документов [4].

Сложная структура, многоэтапное обслуживание, случайный характер моментов поступления запросов пользователей и длительности их обработки в КХЭД предопределяют использование моделей сетей массового обслуживания для анализа и проектирования.

### 1.3.2 Структура КХЭД

На рис. 1.2 изображена схема описанных модулей в нотациях UML.

- Модуль установки соединения

  Отвечает за организацию процесса подключения пользователя к конфиденциальному хранилищу электронных документов и передачу данных — проведение процедуры согласования параметров соединения, помещение заявок пользователей на ожидание в очередь основного процесса сервера приложений, выделение параллельных потоков для работы пользователя с системой.

- Модуль аутентификации

  Отвечает за проверку принадлежности субъекту доступа предъявленного им идентификатора.

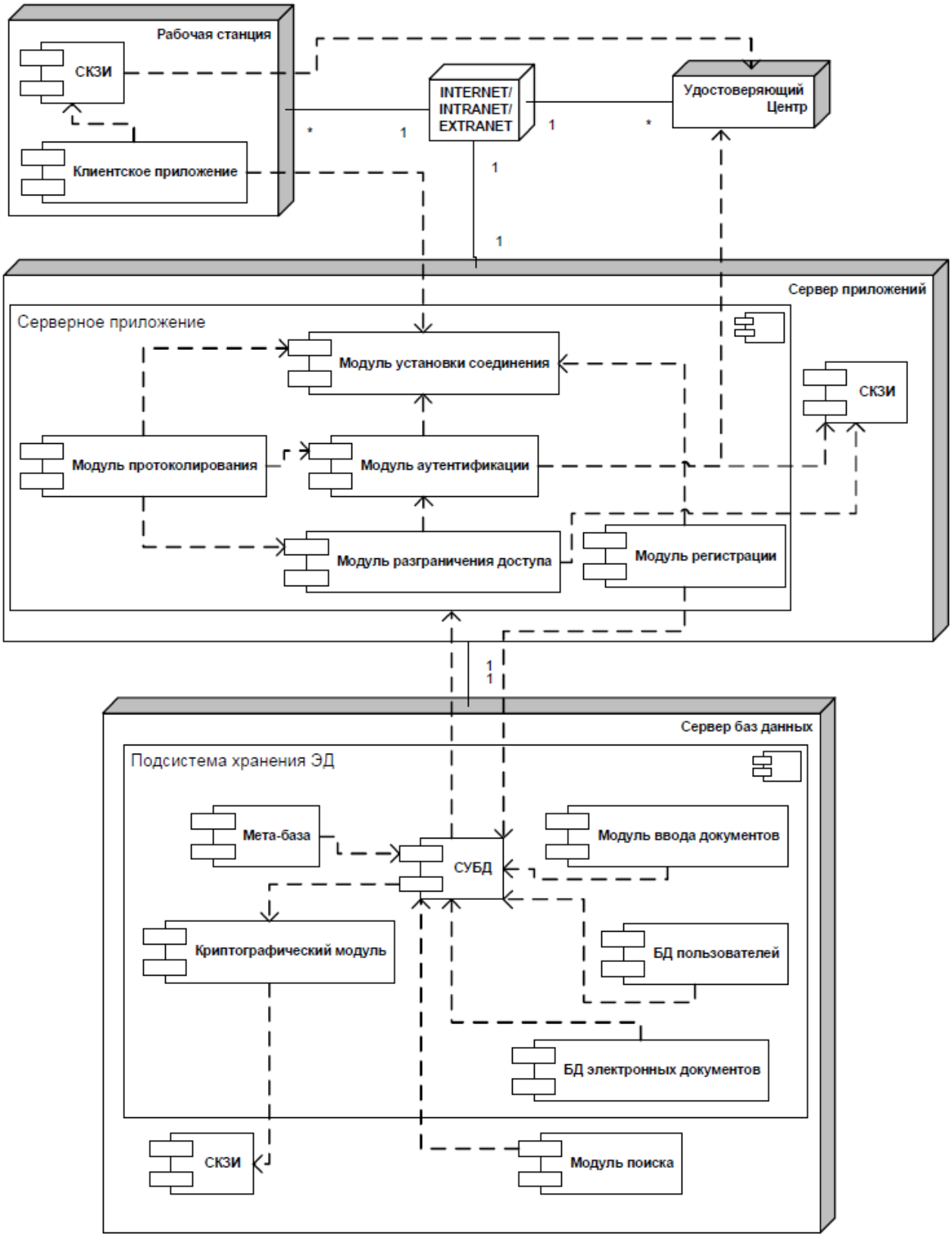


Рисунок 1.2: Структура КХЭД

- Модуль разграничения доступа

  Предназначен для проверки прав пользователей на доступ к функциям системы и электронным документам, а также для ограничения и контроля действий пользователей в соответствии с их правами.

- Модуль хранения электронных документов

  Отвечает за организацию конфиденциального хранения электронных документов и за предоставление доступа к ним пользователей.

- Модуль поиска и редактирования

  Предназначен для осуществления поиска ЭД по запросам пользователей, а также внесения изменений в них.

### 1.3.3 КХЭД как сеть массового обслуживания

***Система массового обслуживания (СМО)*** — система, производящая обслуживание поступающих в неё требований. ***Заявки*** (требования) поступают от нескольких источников через постоянные или произвольные промежутки времени. ***Приборы*** (каналы) служат для обработки этих заявок. Если в момент поступления заявки все приборы заняты, заявка поступает в ***очередь*** на обслуживание. Очередь может быть конечной или бесконечной. В случае переполнения конечной очереди заявка получает ***отказ*** с вероятностью, называемой ***вероятностью потери заявки***.

Для обозначения типа СМО Кендаллом и Башариным предложена система обозначений, имеющих вид $\Delta/\Theta/\Xi/\Omega$ [5–7]. Здесь $\Delta$ — обозначение закона распределения вероятностей для интервалов поступления заявок, $\Theta$ – обозначение закона распределения вероятностей для времени, $\Xi$ – число каналов обслуживания, $\Omega$ – число мест в очереди.

Обозначение законов распределения в позициях $\Delta$ и $\Theta$ выполняется обычно буквами из следующего списка:

- $M$ — экспоненциальное,
- $E^k$ — эрланговское порядка $k$,
- $R$ — равномерное,
- $D$ — детерминированное (постоянная величина),
- $G$ — произвольное (любого вида).

Если число мест в очереди не ограничено, то позиция $\Xi$ не указывается. Например, $M/M/1$ означает простейшую СМО (оба распределения экспоненциальные, канал обслуживания один, очередь не ограничена), а обозначение $R/D/2/100$ соответствует СМО с равномерным распределением интервалов поступления требований, фиксированным временем их

обслуживания, двумя каналами и 100 местами в очереди. В этой СМО заявки, приходящие в моменты, когда все места в очереди заняты, покидают систему (т.е. теряются).

***Сеть массового обслуживания (СеМО)*** — совокупность конечного числа обслуживающих узлов, в которой циркулируют заявки, переходящие в соответствии с маршрутной матрицей из одного узла в другой. Узел всегда является разомкнутой СМО, т.е. имеющей входящий и исходящий поток сообщений (заявок).

В соответствии с теорией массового обслуживания, можно классифицировать КХЭД как разомкнутую экспоненциальную сеть массового обслуживания [4]. Для таких СеМО равновесное совместное распределение количества заявок в центрах обслуживания представляется в виде произведения маргинальных распределений:

$$P(n_1, n_2, \ldots, n_k) = \prod_{i=1}^{R} P_i(n_i), \tag{1.1}$$

где $P_i(n_i)$ — стационарная вероятность того, что в $i$-м центре, рассматриваемом изолированно, находится $n_i$ сообщений, $R$ — количество центров массового обслуживания в сети.

Для определения потоков, циркулирующих в стационарном режиме в сети МО, вводятся коэффициенты передачи $e_i$, такие, что $\lambda(N)e_i$ представляет собой общую интенсивность потока сообщений в $i$-й центр сети ($i = \overline{1, R}$), $\lambda(N)$ — интенсивность входящего в СеМО потока сообщений:

$$\lambda_i(N) = \lambda(N)e_i, i = \overline{1, R}.$$

В открытых СеМО интенсивность $\lambda_i$ складывается из интенсивности поступления сообщений в $i$-й центр из источника и интенсивности поступления из других центров:

$$e_i = P_{oi} + \sum_{j=1}^{R} P_{ij}e_j, i = \overline{1, R}. \tag{1.2}$$

В случае замкнутых сетей исключается поток от внешнего источника. Для отыскания однозначного решения системы уравнений (1.2) достаточно произвольно задать значение $e_i$, например, положить $e_i = 1$. В этом случае величину $e_i$ можно интерпретировать как среднее число посещений центра $i$ между двумя последовательными посещениями первого центра.

На рис. 1.3 представлена формализованная схема КХЭД в виде СеМО.
$S0$ — центр, формализующий входной поток сообщений пользователей.

$S1$ — центр, формализующий работу модуля TCP (транспортный уровень) операционной системы сервера приложений КХЭД на этапе установления соединения. $K$ – число обслужи-

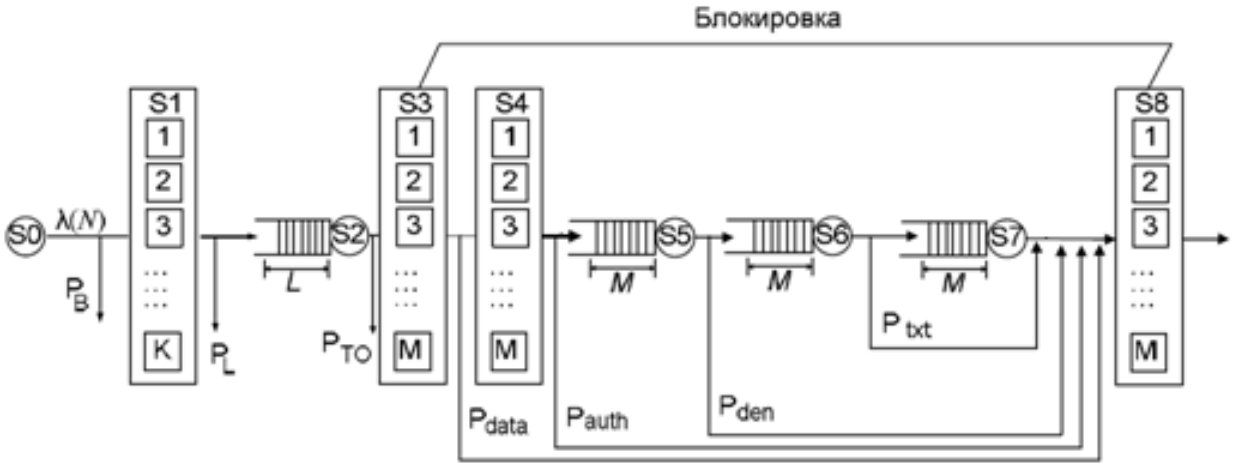


Рисунок 1.3: Открытая сеть массового обслуживания, формализующая работу КХЭД

вающих каналов, очередь отсутствует. Если в момент поступления сообщения в центр все $K$ каналов заняты, то сообщение теряется, вероятность этого события равна $P_B$.

$S2$ — основной поток приложения сервера, извлекающего сообщения из очереди на установление соединения. Максимальная длина очереди $L$ к центру задается в серверном приложении. Если при поступлении сообщения все $L$ мест очереди заняты, то сообщение теряется с вероятностью $P_L$.

$S3$ — параллельные потоки сервера, обеспечивающие одновременное обслуживание соединений на этапе получения запросов по сети. При переполнении центра сообщения теряются с вероятностью $P_{TO}$. Центры $S1$, $S2$, $S3$ реализуют модуль установки соединения.

Центры $S3$ и $S8$ имеют по $M$ каналов обслуживания (потоков сервера) и при начале обслуживания сообщения в $i$-ом канале центра $S3$ он считается занятым до завершения обслуживания в $i$-ом канале центра $S8$. Таким образом, происходит блокировка каналов центров $S3$ и $S8$ и поэтому потерь сообщений из-за переполнения очереди к центрам $S5$, $S6$, $S7$ и занятости всех обслуживающих устройств центра $S4$ не происходит, т.к. больше чем $M$ сообщений в центрах $S4$, $S5$, $S6$, $S7$ быть не может.

$S4$ — модуль аутентификации клиентов при обращении к КХЭД.

$S5$ — модуль проверки прав доступа клиентов при обращении к КХЭД.

В случае удачной аутентификации и проверки прав доступа клиента производится поиск электронного документа по запросу пользователя и выполнение операций по контролю целостности информации, проверке и простановки ЭЦП, шифрованию и дешифрованию. Для формализации процесса поиска и редактирования электронных документов выделены центры

$S6$ и $S7$ соответственно. После того, как запрос пользователя выполнен, происходит передача ответа пользователю в многолинейном центре обслуживания $S8$.

В соответствии с теоремой BCMP (Baskett, Chandy, Muntz, Palacios) мультипликативное свойство решения (1.1) для $P_(n_1, n_2, \ldots, n_R)$ сохраняется для СеМО, содержащих следующие виды узлов:

- $M/M/m$ с дисциплиной обслуживания FCFS (First Came First Served — первым поступил, первым обслужен);
- $M/G/1$ с дисциплиной дисциплиной PS (Process Sharing — разделение процессора);
- $M/G/\infty$ с обслуживанием без ожидания (IS — Immediately Serve);
- $M/G/1$ с дисциплиной LCFS (Last Came First Served — последним поступил, первым обслужен) с прерываниями [8].

В приведённой на рис. 1.3 схеме представлены следующие узлы:

- $S1, S3, S4, S8 - M/G/\infty$, IS;
- $S2, S6, S7 - M/M/1$, FCFS;
- $S5 - M/G/1$, PS. [4]

Одной из важнейших задач СЭД является обнаружение ошибок редактора. Такие ошибки делятся соответственно на *детектируемые* и *недетектируемые*. Описанная на рис. 1.3 СеМО обнаруживает следующие типы ошибок:

- Неверное предоставление аутентификационных данных — эта ошибка появляется с вероятностью $P_{data}$;
- Отсутствие прав доступа к запрашиваемому документу — с вероятностью $P_{auth}$;
- Ошибка поиска — с вероятностью $P_{den}$;
- Ошибки во вносимых изменениях (напр., обращение к некорректным полям документа) — с вероятностью $P_{txt}$.

Механизм обнаружения таких ошибок позволяет избежать выдачи заведомо неверного документа следующему редактору в схеме, представленной на рис. 1.1.

С учётом вышеописанного, каждый из редакторов в схеме на рис. 1.1 может быть представлен в виде автоматизированной системы, изображённой на рис. 1.4.

В роли АС здесь выступает КХЭД, описанное на рис. 1.3. В случае обнаружения ошибок силами АС пользователю выдаётся сообщение об ошибке, т.е. фактически новое задание на редактирование. С учётом этого факта граф, представленный на рис. 1.1, преобразуется к виду, представленному на рис. 1.5.

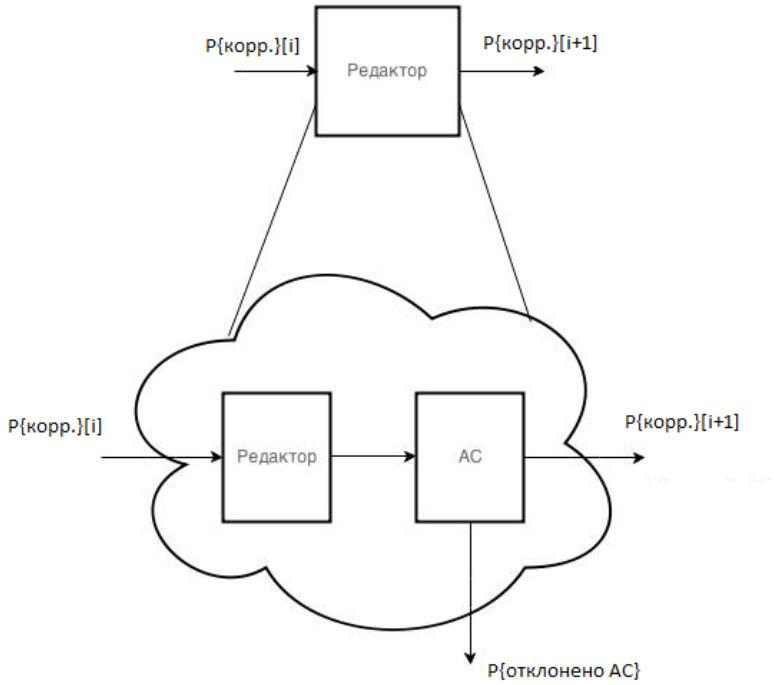


Рисунок 1.4: Схема узла СЭД с применением АС для обработки данных

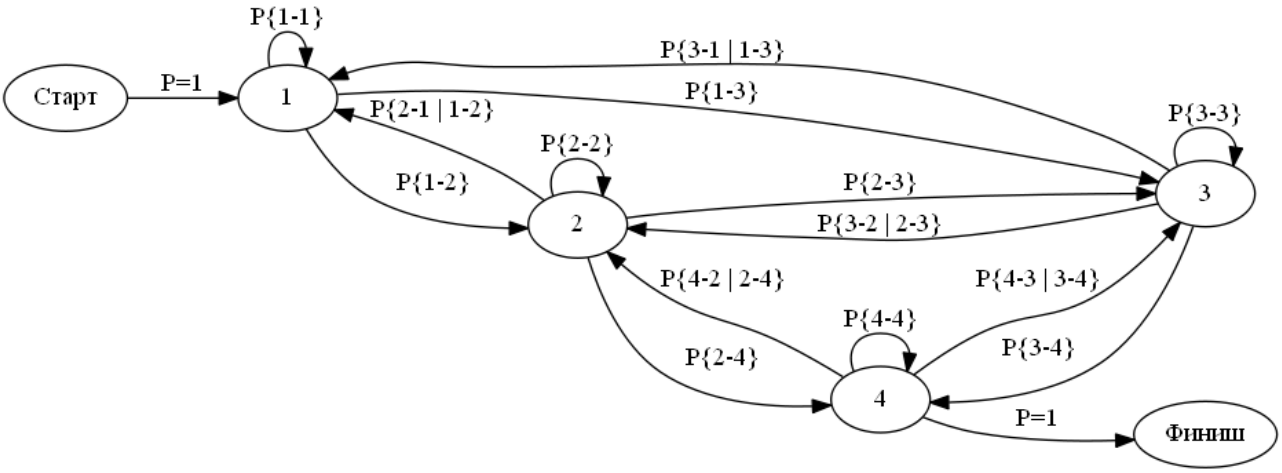


Рисунок 1.5: Документооборот с применением СЭД

## 1.4 Анализ угроз и средств противодействия им для систем электронного документооборота

Считается, что для защиты СЭД достаточно использования электронной подписи (ЭП), однако в большинстве случаев разработчики не поясняют, как правильно использовать ЭП, какая нужна инфраструктура и какие защищённые сервисы необходимо развернуть на её основе [9]. Обычно ими приводятся только конкретные примеры реализованных защищенных СЭД. Поэтому понятие защищённого электронного документооборота (ЗЭД) определить достаточно трудно, особенно в условиях активно развивающихся технологий. В общем случае к задаче создания такой системы необходимо подходить с точки зрения классической защиты информационной системы, обеспечивая решение таких задач, как:

- аутентификация пользователей и разделение доступа;
- подтверждение авторства электронного документа;
- контроль целостности электронного документа;
- конфиденциальность электронного документа;
- обеспечение юридической значимости электронного документа.

### 1.4.1 Классификация угроз информационной безопасности систем электронного документооборота

Угрозы СЭД можно сгруппировать по нарушаемым свойствам безопасности:

- угрозы конфиденциальности:
  - кража;
  - перехват информации;
  - изменение маршрутов следования информации.
- угрозы целостности — угрозы, при реализации которых информация теряет заранее определенные системой вид и качество. Объектами данной угрозы могут быть все компоненты СЭД:
  - документы;
  - резервные копии документов;
  - среда хранения электронных документов;
  - операционные системы и компоненты СЭД, установленные на клиентских рабочих станциях;
  - каналы связи.
- угрозы доступности, характеризующие возможность доступа к хранимой и обрабатываемой в СЭД информации в любой момент времени.

В табл. 1.2 представлены возможные воздействия на элементы СЭД, приводящие к нарушению их нормального функционирования и, как к одному из сдледствий, потере юридической значимости электронных документов [10].

Таблица 1.2: Угрозы безопасности информации в СЭД

| Элемент СЭД | Вид деструктивного воздействия | Результат воздействия |
|---|---|---|
| Система хранения и обработки документов | Воздействие на носитель информации | Нарушение целостности и доступности ЭД, истории и метаданных |
| | Внесение искажений в подписанный электронной подписью ЭД | Нарушение целостности ЭД |
| | Несанкционированное изменение метаданных документа (формат, реквизиты, и т.п.) | Нарушение целостности, возможное нарушение доступности ЭД |
| | Несанкционированное внесение изменений в историю ЭД | Нарушение целостности, возможное нарушение доступности ЭД |
| | Нелегитимное копирование ЭД | Нарушение конфиденциальности ЭД и истории |
| Система передачи информации | DoS каналов связи, отказ комплектующих | Нарушение целостности и доступности ЭД. Нарушение доступности CRL и сервера доверенного времени |
| | Внесение искажений в передаваемую информацию | Нарушение целостности ЭД |
| Система разграничения доступа | Компрометация аутентификационных данных легитимного пользователя | Нарушение конфиденциальности |

*продолжение следует*

| *(продолжение)* | | |
|---|---|---|
| Элемент СЭД | Вид деструктивного воздействия | Результат воздействия |
| | Ошибки администрирования (преднамеренные и непреднамеренные): разрешение на доступ нелегитимных пользователей, запрет доступа легитимным пользователям | Нарушение конфиденциальности. Нарушение доступности |
| Система проверки подлинности | Компрометация ключа ЭП либо ключа удостоверяющего центра | Нарушение целостности ЭД |
| | Нелигитимное делигирование уполномоченным лицом права подписи ЭД | |
| | Компрометация списка отозванных сертификатов | Нарушение достоверности ЭП |
| | Отказ носителя ключа ЭП | Нарушение доступности ключа ЭП, невозможность штатной работы СЭД |

Защиту от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота. При этом, с одной стороны, при внедрении СЭД увеличиваются риски реализации угроз, но, с другой стороны, при правильном подходе упорядочение документооборота позволяет выстроить более качественную систему защиты.

Таким образом, любая защищенная СЭД должна предусматривать реализацию как минимум следующих механизмов защиты:

- обеспечение целостности документов;
- обеспечение безопасного доступа к компонентам системы;
- обеспечение конфиденциальности документов;
- обеспечение подлинности документов;

- протоколирование действий пользователей.

### 1.4.2 Анализ средств противодействия угрозам информационной безопасности систем электронного документооборота

Для борьбы с вышеописанными угрозами возможно применение следующих средств:

1. **Воздействие на носитель информации.**

   Для защиты от разрушающих воздействий на хранилища документов необходимо обеспечить их физическую, электромагнитную и вибрационную защиту.

2. **Несанкционированное изменение метаданных документа (формат, реквизиты, и т.п.).**

   Для предотвращения этой угрозы необходимо использование системы польного разграничения доступа с отдельной настройкой по каждому документы / пакету документов, метаданным к ним, и т.п. Контроль за делигированием полномочий, делегирование полномочий с ограничением по времени.

3. **Несанкционированное внесение изменений в историю ЭД.**

   Для защиты от правок записей в истории изменений документа необходимо обеспечить контроль целостности этих записей. В общем случае для этого необходим сервер доверенного времени, с помощью которого для каждой записи в истории будет создаваться метка времени, контролирующая одновременно её целостность и время создания.

   Однако, не всегда есть необходимость в установлении точного времени записи: часто достаточно только удостовериться во взаимном положении записей во времени. В таком случае целесообразно не устанавливать сложный в обслуживании сервер доверенного времени, а использовать метод хранения записей в виде цепочки хэш-сумм: в каждой такой записи помимо полезных данных будет содержаться хэш-сумма предыдущей записи. Это позволит упорядочить события во времени, а также усложнит задачу компрометации записей. Подробнее это метод описан в разделе 1.5.3.

4. **Нелигитимное копирование электронного документа.**

   Защитой от нелигитимного копирования электронных документов является любое средство защиты информации от НСД — например, средтсво шифрования данных на локальном хранилище, средство защиты каналов передачи данных, и т.п. Дополнительным уровнем защиты, применимым также для противодействия внутренним угрозам, является специальное ПО для чтения документов. Например, вместо предоставления документов по запросу можно предоставлять доступ к удалённому средству просмотра (например, через веб-браузер в защищённой сессии) без возможности локального копирования документов. Для полной защиты необходимо также ограничить круг терминалов удалённого доступа и запретить на них скриншоты (снимки экрана). В случае,

если помимо просмотра документа требуется и его редактирование, такое приложение должно предоставлять и данный сервис.

5. **Внесение искажений в передаваемую информацию.**

   Так как по каналу передаётся защищённый (зашифрованный) поток данных, в качестве искажений могут рассматриваться только помехи, наводимые на линию связи для нарушения целостности передаваемой информации. Для защиты от такой атаки следует экранировать кабели передачи данных, а также сетевое оборудование.

6. **Компрометация аутентификационных данных легитимного пользователя.**

   В общем случае, аутентификационные данные могут быть скомпрометированы путём взлома системы аутентификации, социальной инженерии либо полного перебора паролей. Для защиты от атак по первому вектору необходимо анализировать методы и реализации защиты до принятия решения об их использовании, по второму вектору — проводить обучающие семинары с персоналом на тему использования среств защиты данных и политик безопасности. Для усложнения перебора паролей рекомендуется заменить средства парольной защиты на системы, использующие асимметричную криптографию. В таком случае сертификат открытого ключа будет являться идентификатором пользователя, а доказательство владения закрытым ключом (proof of knowledge) — его аутентификатором. Сложность подбора пароля в таком случае возрастёт с $2^{48}$ (при средней длине пароля 8 знаков, без учёта словарного подбора) до $2^{512}$ (по ГОСТ Р 34.10-2012, словари отсутствуют по определению) и станет бессмысленной: для реализации данного вектора атаки злоумышленнику придётся получить доступ к хранилищу ключей, что обычно гораздо более сложная задача.

   В ещё более надёжной системе можно использовать асимметричные ключи, записанные на токены. Такие ключи неизвлекаемы, и для доступа к ним требуется физический доступ к их носителю — токен злоумышленнику придётся украсть, а обнаружить пропажу физического ключа проще, чем электронного.

7. **Нелигитимное делигирование уполномоченным лицом права подписи ЭД.**

   Данная атака является следствием нарушения административных регламентов обеспечения информационной безопасности. Бороться с ней неоходимо в двух направлениях: с одной стороны, проводить обучающие семинары по основам и политикам информационной безопасности среди сотрудников. С другой стороны, необходимо по возможности ограничить возможность делигирования полномочий как кругом лиц, которым можно передать права, так и по времени (например, сделать невозможным делигирование завершённой задачи, либо задачи, ожидающей обработки другим редактором).

Остальные описанные угрозы относятся либо к разряду криптографических проблем общего характера и требуют от разработчиков средств защиты лишь правильного выбора алго-

ритмов и реализаций (*внесение искажений в подписанный электронной подписью ЭД, компрометация ключа ЭП либо ключа удостоверяющего центра, компрометация списка отозванных сертификатов*), либо является следствием отказа оборудования (*отказ сетевых устройств, отказ носителя ключа ЭП*) или человеческого фактора (*ошибки администрирования*). Методы решения этих проблем носят общий характер и не уникальны для систем электронного документооборота

## 1.5 Исследование методов организации процесса обработки данных в СЭД

Система электронного документооборота, как и любая другая система, может быть представлена в виде совокупности модулей, выполняющих различные функции. Для каждого модуля можно определить варианты реализации, исходя из особенностей его работы. Наибольший интерес будут представлять следующие модули:

- модуль обеспечения совместной работы пользователей;
- модуль обнаружения ошибок при обработке документа;
- модуль хранения истории внесённых изменений;
- модуль авторизации.

Остальные модули (передачи данных, разграничения доступа, защиты хранилища от несанкционированного доступа) реализуются стандартными методами и не представляют такого интереса.

Для выбора реализации модулей СЭД в соответствии с показателями эффективностями, которые будут описаны позднее, необходимо провести экспериментальное исследование существующих реализаций подобных модулей. Так как системы электронного документооборота дороги и сложны в развёртывании, не все компании предоставляют демо-версии своих продуктов. Но и в случае наличия демо-версии довольно сложно её получить и оценить параметры (часто вместо демо-версии предоставляется презентация, а также отсутствует доступ к отдельным модулям системы). Существует и ещё один фактор, затрудняющий сложность проведения эксперимента: так как СЭД является системой массового обслуживания, для её объективного тестирования необходимо провести множество однотипных испытаний, включающих в себя работу нескольких испытуемых (пользователей СЭД) в течение длительного времени.

С учётом всех вышеизложенных ограничений, было принято решение првоести имитационное моделирвоание модулей СЭД в среде AnyLogic, приняв за описание моделей базовые принципы построения исследуемых модулей в различных реализациях.

### 1.5.1 Модуль обеспечения совместной работы пользователей

При совместной конкурентной работе пользователей в системе электронного документооборота существует проблема синхронизации вносимых изменений. Так, два редактора, работая над одним документом (но каждый со своим набором задач), во время внесения изменений блокируют работу друг друга, так как документ в рассматрвиаемом контексте — ограниченный ресурс. В один момент времени возможно только одно внесение изменений, это показано на рис. 1.6.

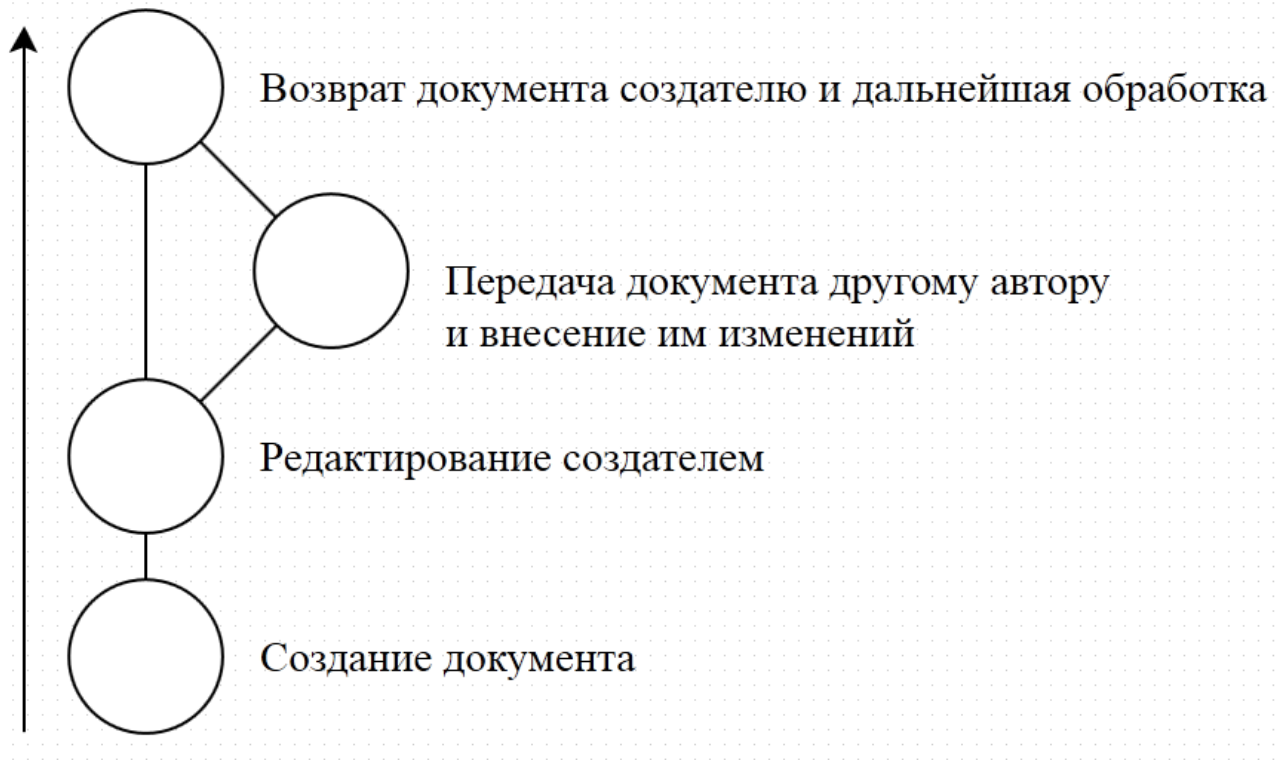


Рисунок 1.6: Схема конкурентной обработки документа с блокировкой

Схема такой модели в среде AnyLogic представлена на рис. 1.7.

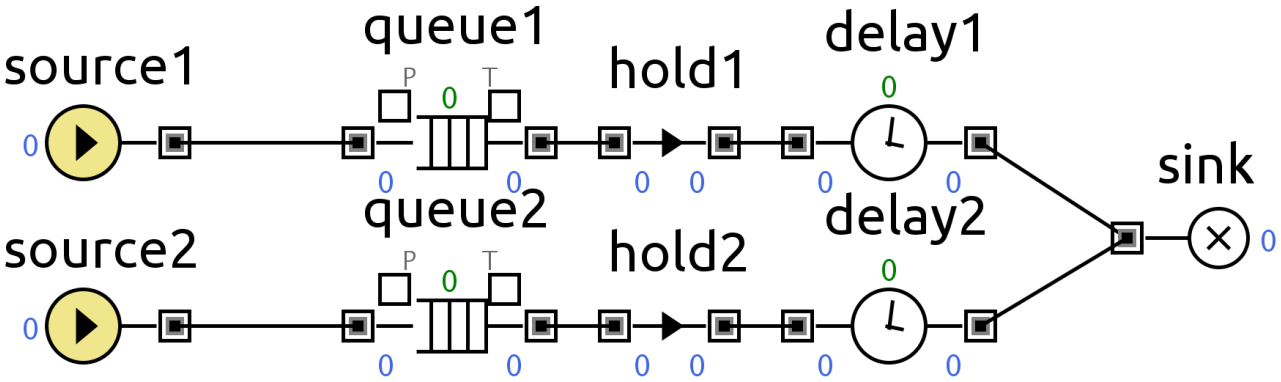


Рисунок 1.7: Модель обработки документа с блокировкой в среде AnyLogic

Здесь объекты $source$ моделируют источники заявок (по одной заявке в полчаса), $queue$ — персональные очереди заявок на обработку, $hold$ — элемент, блокирующий работу редактора

(когда работает первый редактор, второй блокируется, и наоборот), $delay$ — редакторы (время обработки заявки распределяется по нормальному закону со средним значением 25 минут, $\sigma = 5$), $sink$ — целевое хранилище, собирающее обработанные заявки.

Альтернативой является такая схема организации обработки документов, при которой разрешено одновременное внесение изменений в документ, что справедливо для разрабатываемой системы — см. рис. 1.8. Это становится возможным благодаря регистрации не состояний документа, а вносимых в него изменений в виде разницы текущего и предыдущего состояний. Пример такой разностной записи показан на рис. 1.9.

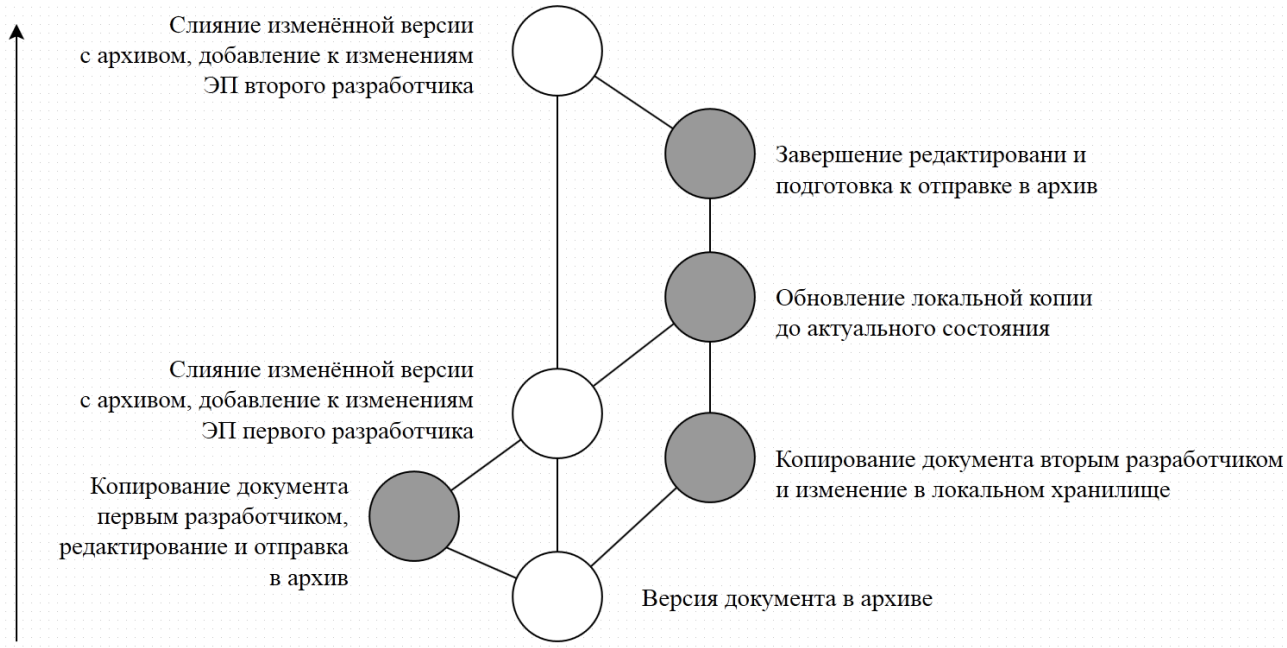


Рисунок 1.8: Схема конкурентной обработки документа без блокировки

Данная реализация позволяет не только сократить объём хранимых данных, но и реализовать вышеописанную схему, ведь при таком подходе одновременное внесение изменений несколькими редакторами рассматривается не как изменение одного документа, а как создание набора новых записей. Результирующий документ получается путём последовательного применения таких патчей к исходному документу.

Схема этой модели в среде AnyLogic представлена на рис. 1.10.

Элементы на этой схеме совпадают с элементами схемы рис. 1.7, однако здесь отсутствуют блоки $hold$, а время обработки заявки распределяется по нормальному закону со средним значением 30 минут, $\sigma = 6$ (из расчёта временного запаса на устранение ошибок слияния при одновременном переходе обработанных заявок в блок $sink$).

```
commit d1f67f6a2306a4472bc49620f3ccec566735488d
Author: Victor Kartashov <victor.kartashov@gmail.com>
Date:   Mon Apr 14 21:46:33 2014 +0400

    rights: штрихи к выводу

    Signed-off-by: Victor Kartashov <victor.kartashov@gmail.com>

diff --git a/diploma.pdf b/diploma.pdf
index 24324ea..246a674 100644
Binary files a/diploma.pdf and b/diploma.pdf differ
diff --git a/rights/rights_conclusion.tex b/rights/rights_conclusion.tex
index 4193e20..32d6a5a 100644
--- a/rights/rights_conclusion.tex
+++ b/rights/rights_conclusion.tex
@@ -1,8 +1,9 @@
 \section{Выводы} \label{rights_conclusion}

-Нормативно-правовые акты различного уровня устанавливают условия, при которых
+Нормативно-правовые акты различного уровня определяют условия, при которых бум
+так и выполнить требования по защите конфиденциальной, коммерческой и иной инф
```

Рисунок 1.9: Пример описания состояния документа в виде разностной записи

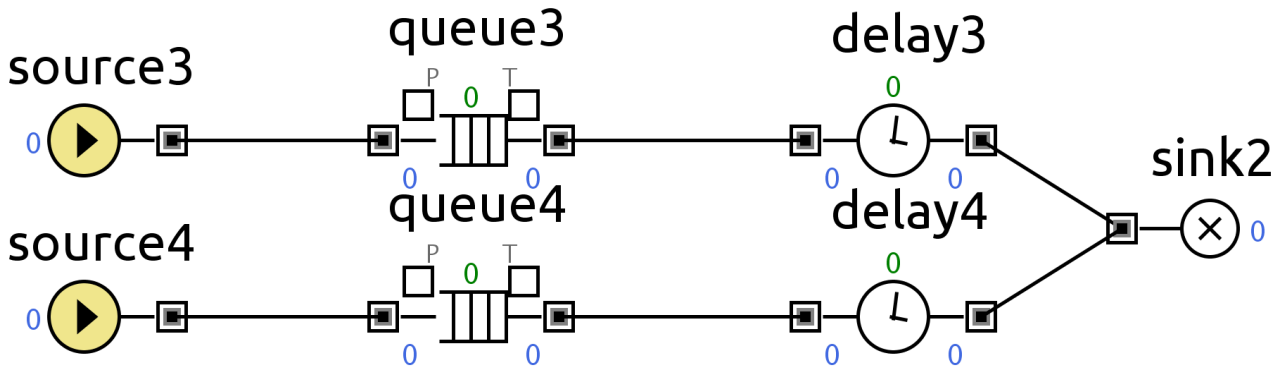


Рисунок 1.10: Модель обработки документа без блокировки в среде AnyLogic

В процессе эксперимента был промоделирован один рабочий день (с 9:00 до 18:00), в течение которого каждому из редакторов на обработку поступило 19 заявок. Число обработанных заявок в схеме с блокировкой показано на рис. 1.11, в схеме без блокировок — на рис. 1.12.

Как видно из представленных результатов, несмотря на бо́льшее среднее время обработки одной заявки, число успешно обработанных заявок в схеме без блокировки за один рабочий день в 1.5 раза больше, чем число успешно обработанных заявок в схеме с блокировкой за тот же период. Также по этим рисункам видно, что за счёт блокировок заявки редакторами в первой схеме обрабатывались неравномерно, в отличие от второй схемы. Дополнительным подтверждением этому служат временные диаграммы загруженности редакторов в течение рабочего дня, представленные на рис. 1.13 и 1.14.

Данные рисунки наглядно показывают время бездействия редакторов в схеме с блокировкой (два редактора работают с загрузкой, равной 100% загрузке одного редактора). Такого

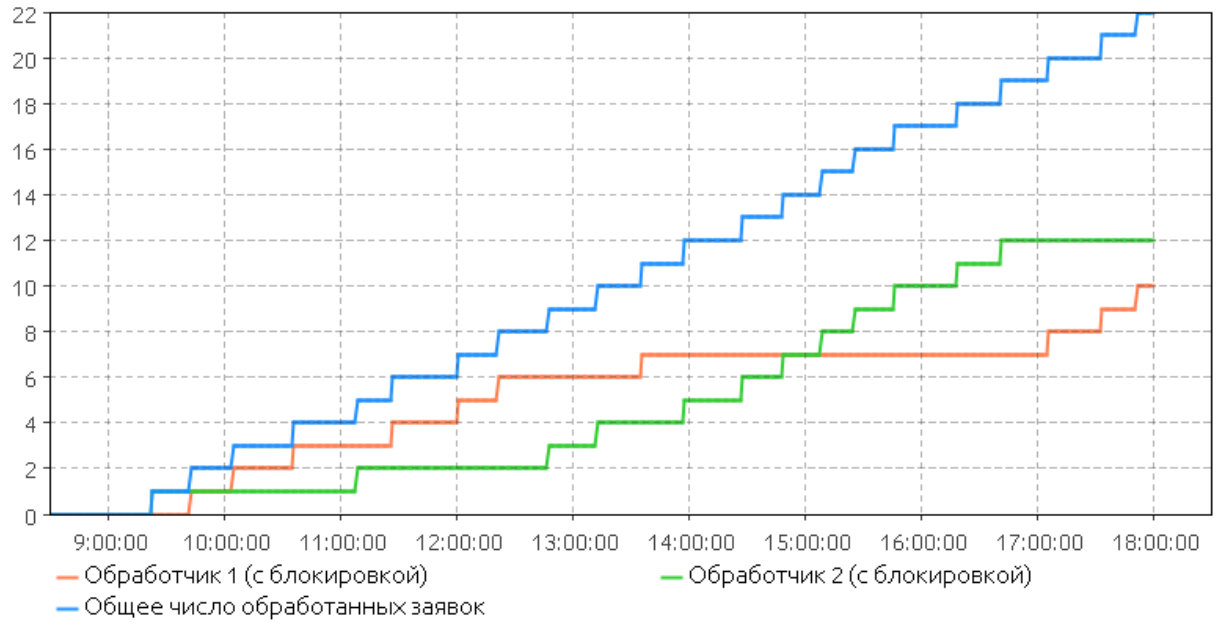


Рисунок 1.11: Число обработанных заявок в схеме с блокировкой

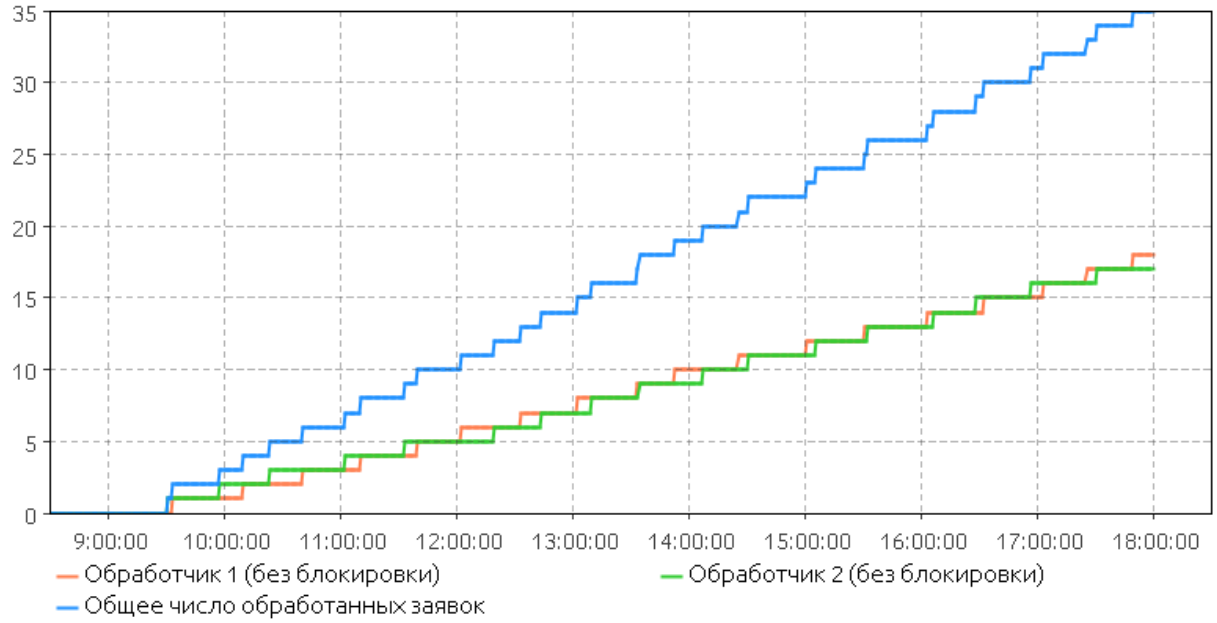


Рисунок 1.12: Число обработанных заявок в схеме без блокировки


Рисунок 1.13: Временная диаграмма загруженности редакторов в течение рабочего дня в схеме с блокировкой

продолжительного простоя можно избежать только обрабатывая параллельно несколько документов разными редакторами так, чтобы время блокировок сводилось к минимуму. Таким


Рисунок 1.14: Временная диаграмма загруженности редакторов в течение рабочего дня в схеме без блокировки

образом, появляется дополнительная задача временного планирования. При этом схема без блокировок помогает эффективно использовать рабочее время без дополнительного планирования.

Ещё один немаловажный показатель — загруженность очереди на обработку. Соответствующие графики приведены на рис. 1.15 и 1.16.

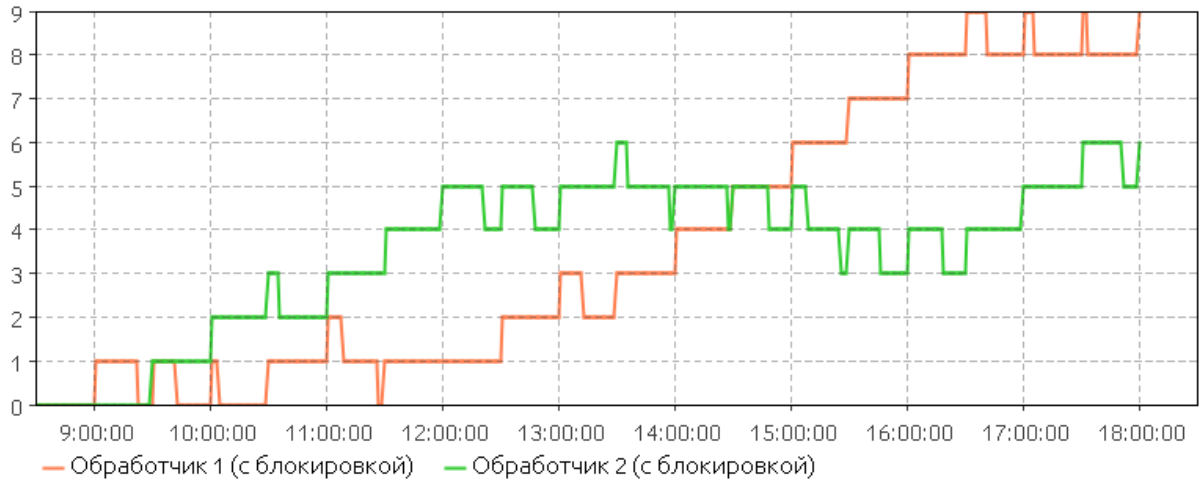


Рисунок 1.15: Загруженность очереди на обработку в схеме с блокировкой

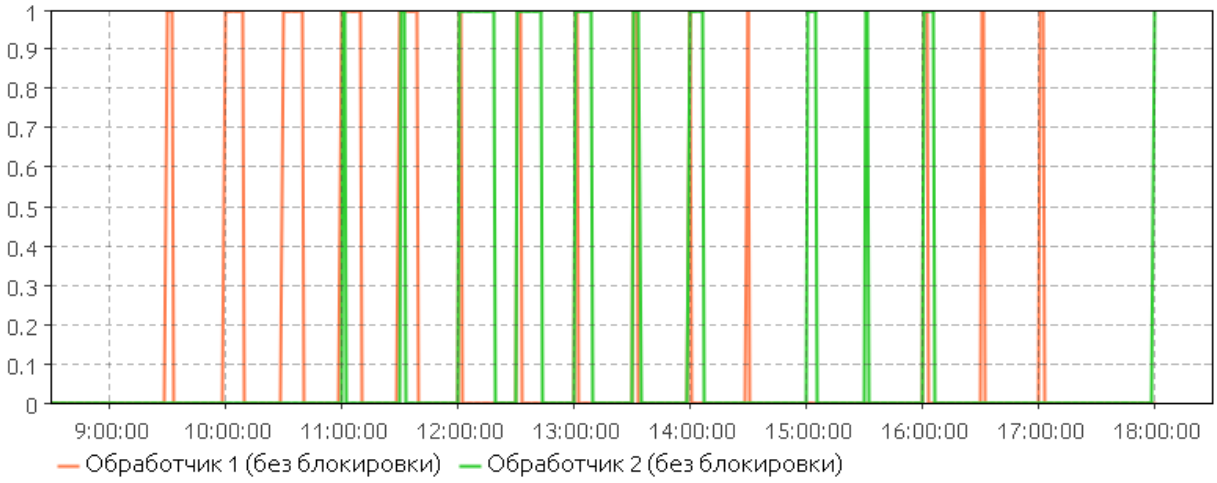


Рисунок 1.16: Загруженность очереди на обработку в схеме без блокировки

Как видно, при использовании схемы с блокировкой заполняемость очереди имеет тенденцию к росту, что в конечном итоге приведёт к ситуации, в которой заявки одного конкретного редактора будут полностью удовлетворены только по завершении всех работ остальными редакторами. В то же время, очереди в схеме без блокировок не имеют подобной тенденции и заявки, находящиеся в них, своевременно удовлетворяются.

Таким образом, при совместной работе пользователей над одним документом в системе электронного документооборота целесообразно использовать предложенную схему организации процесса без блокировок.

### 1.5.2 Модуль обнаружения ошибок при обработке документа

При обработке документов автоматиизирвоанным способом существует возможность обнаружения ошибок на стадии редактирования, т.е. до отправки документа далее по цепочке обработки. В таком случае ошибка либо устраняется автоматически, либо создаётся новая задача на устранение ошибки тому же редактору, который эту ошибку допустил.

Одной из разновидностей ошибки такого рода является некорректное обращение к полям документа. Стоит отметить, что речь здесь идёт не о метаданных, сопровождающих документ, а об информации, содержащейся непосредственно в документе. Например, для совместной работы, описанной в гл. 1.5.1, таким обращением будет считаться попытка редактирвоания полей документа, обработкой которых уже занимается другой редактор.

Для эксперимента были рассмотрены две схемы: одна — «классическая», без обнаружения ошибок такого рода (многие СЭД не предоставляют подобного сервиса, регулируя только поля метаданных, см. табл. 1.1), другая — согласно описанной выше схеме, реализованная в описываемой разработке.

На рис. 1.17 представлена схема без автоматизированного обнаружения ошибок. Возврат на доработку при такой организации возможен, но осуществляется в ручном режиме: редактор, получивший на вход задания документ с ошибкой, отправляет его на переработку предыдущему редактору (в реальной системе он будет передавать документ соседнему звену в обратном направлении, однако как показывает практика, в случае подчинения низших звеньев высшим документ будет возвращаться до первого редактора). Последний редактор в случае допуска ошибки получит неверный документ, на схеме приёмник таких результатов обозначен $sink$. Корректно обработанные заявки приходит в пункт $sink2$. Разветвления после обработчиков работают по вероятностному принципу с вероятностью обнаружения ошибки $P'_{txt}$.

В случае автомтизированного обнаружения ошибок (рис. 1.18) задание на переработку генерируется автоматически для того редактора, который допустил ошибку. Таким образом,

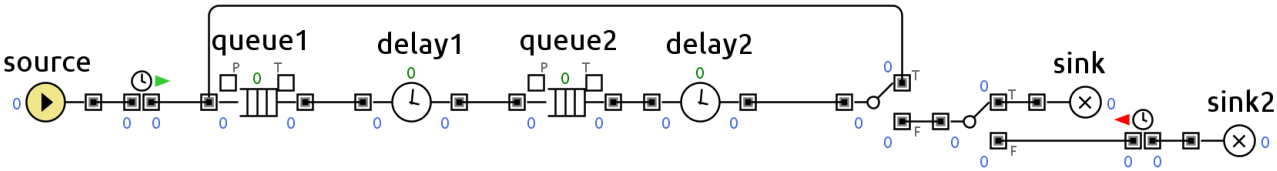


Рисунок 1.17: Схема коррекции ошибок ручным методом

даже последний редактор в цепочке имеет возможность исправить допущенную ошибку перед публикацией документа.

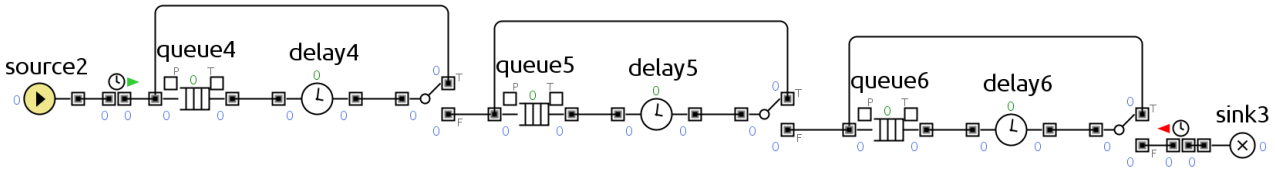


Рисунок 1.18: Схема коррекции ошибок автоматизированным методом

Одним из показателей эффективности метода организации процесса обработки документов является число корректно обработанных заявок. Как и в случае совместной работы пользователей, заявки генерируются по одной за полчаса реального времени, моделируется один рабочий день (с 9:00 до 18:00). Параметры обработчиков совпадают с описанными в гл. 1.5.1. Результат моделирования представлен на рис. 1.19.

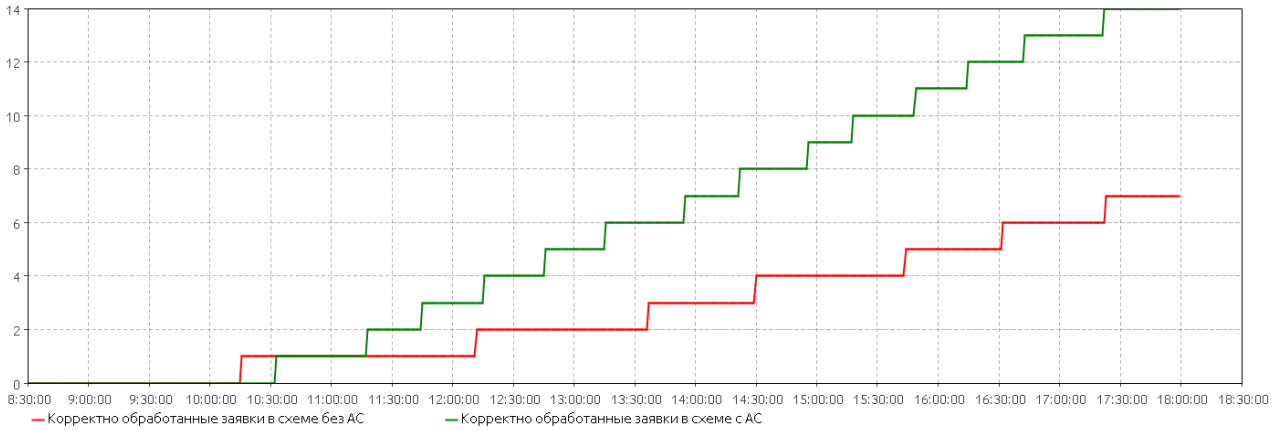


Рисунок 1.19: Число обработанных заявок в схемах с обратной связью

Как видно из рисунка, схема с автоматизирвоанным обнаружением ошибок позволяет обработать больше заявок за ограниченный промежуток времени. Также можно заметить, что частота, с которой заявкам присваивался статус «корректно обработанная», выше в схеме с АС. Это позволяет предположить, что среднее время обработки одной заявки при такой организации меньше, чем при ручном обнаружении ошибок. Данная гипотеза подтверждается графиком, приведённым на рис. 1.20.

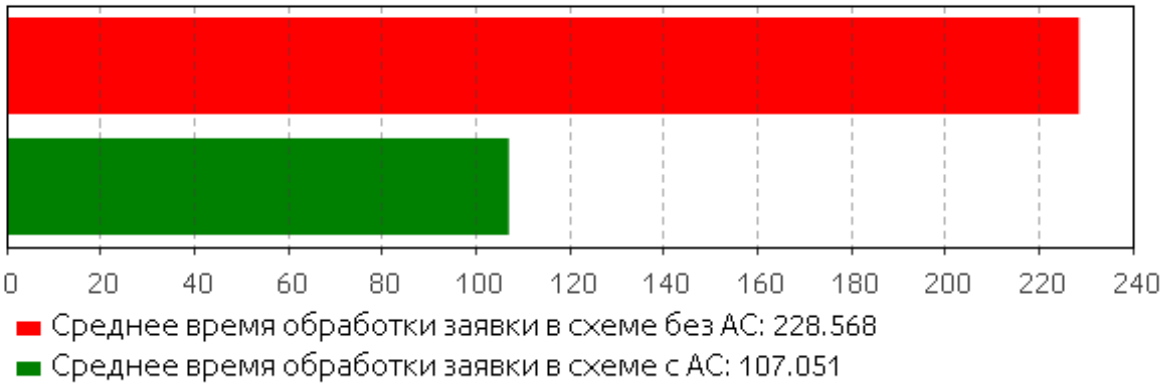


Рисунок 1.20: Среднее время обработки одной заявки в схемах с обратной связью

Уменьшение времени обработки заявки происходит за счёт того, что в случае необходимости исправления ошибки над документом работает один редактор из цепочки (тот, который допустил ошибку), а не все. Более того, среднее время обработки заявки в схеме без АС можно считать заниженным, т.к. в нём не учтено время поиска ошибки, а сама вероятность её обнаружения оценена довольно высоко — наравне с АС.

Таким образом, для снижения времени обработки заявок целесообразно использовать систему автоматического обнаружения ошибок.

### 1.5.3 Модуль хранения истории

Одной из важных функций системы электронного документооборота и КХЭД как её части является хранение истории внесённых изменений. Это необходимо не только для учёта затраченного времени, но и для разбора конфликтных ситуаций, а также возможности создавать несколько документов на базе одного. Необходимость хранения полной и достоверной истории изменения документа описана в ГОСТ Р ИСО 15489-1 — 2007 (см. главу 4.12). Однако, как показало исследование 1.2.4, компании-разработчики СЭД не афишируют способы организации хранения истории, полностью полагаясь на средства СУБД в вопросе обеспечения целостности данных.

В общем случае, при таком подходе каждая запись в истории хранится в виде автономного объекта, к которому необходимо добавлять метку времени для упорядочивания событий во временно*м* порядке, а также электронную подпись для установления авторства.

В качестве альтернативы предлагается другой способ хранения истории изменений — в виде цепочки хэш-сумм. В такой структуре каждая запись содержит в себе контрольную сумму (хэш-сумму) предыдущей записи. Таким образом, события связываются в порядке появления, что избавляет от необходимости дополнительно устанавливать отношения между ними. Дополнительным преимуществом такой схемы является сложность её подделки: если в случае

атомарных записей злоумышленник атакует одну целевую запись, то в случае цепочки помимо атаки на целевую запись необходимо также подделать все записи, появившиеся после неё, чтобы целостность цепи не была нарушена. Сложность такой атаки возрастает с увеличением длины цепи.

В случае дополнения каждой записи электронной подписью становится возможным просматривать документ с построчным указанием авторства, как показано на рис. 1.21.

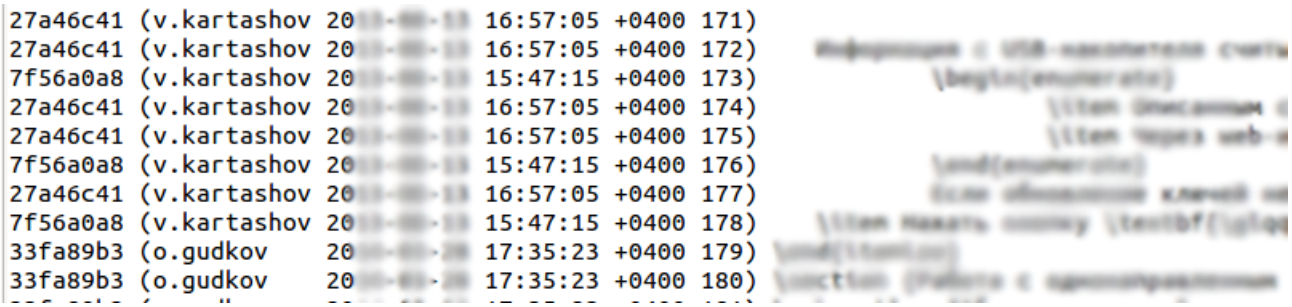


Рисунок 1.21: Просмотр документа с построчным указанием авторства

Таким образом, для проверки целостности истории в первом случае необходимо проверить метку времени каждой записи, а во втором — лишь убедиться в совпадении соответствующих хэш-сумм. Если последняя операция может считаться атомарной в соответствии с ГОСТ Р 34.11, то проверка метки времени состоит как минимум из трёх операций: сверки хэш-суммы, проверки электронной подписи сервера доверенного времени и проверки электронной подписи удостоверяющего центра, выдавшего сертификат серверу доверенного времени.

Однако, замеры реализации данных функций средствами openssl не показали большой разницы в результатах: $0.03$ сек. для подсчёта контрольной суммы и $0.05$ сек. для проверки метки времени того же объекта. Это можно объяснить тем, что все операции, необходимые для проверки метки времени, являются независимыми и могут выполняться параллельно.

Для проверки целостности истории, содержащей 800 записей, в соответствии с описанными замерами была построена схема для имитационного моделирования. Результаты временных замеров представлены на рис. 1.22.

Как показал эксперимент, даже при таком большом объёме данных и несмотря на то, что система с использованием цепочки хэш-сумм сработала быстрее в $1,7$ раз, разница в реальном времени составила всего 16 секунд, что для конечного пользователя может быть не существенно. Однако описанный метод имеет другие достоинства: возрастающая с увеличением длины цепочки сложность подделки записей, отсутствие необходимости в содержании сервера доверенного времени. Это позволяет говорить о целесообразности применения такого метода для хранения полной и достоверной истории сделанных изменений.

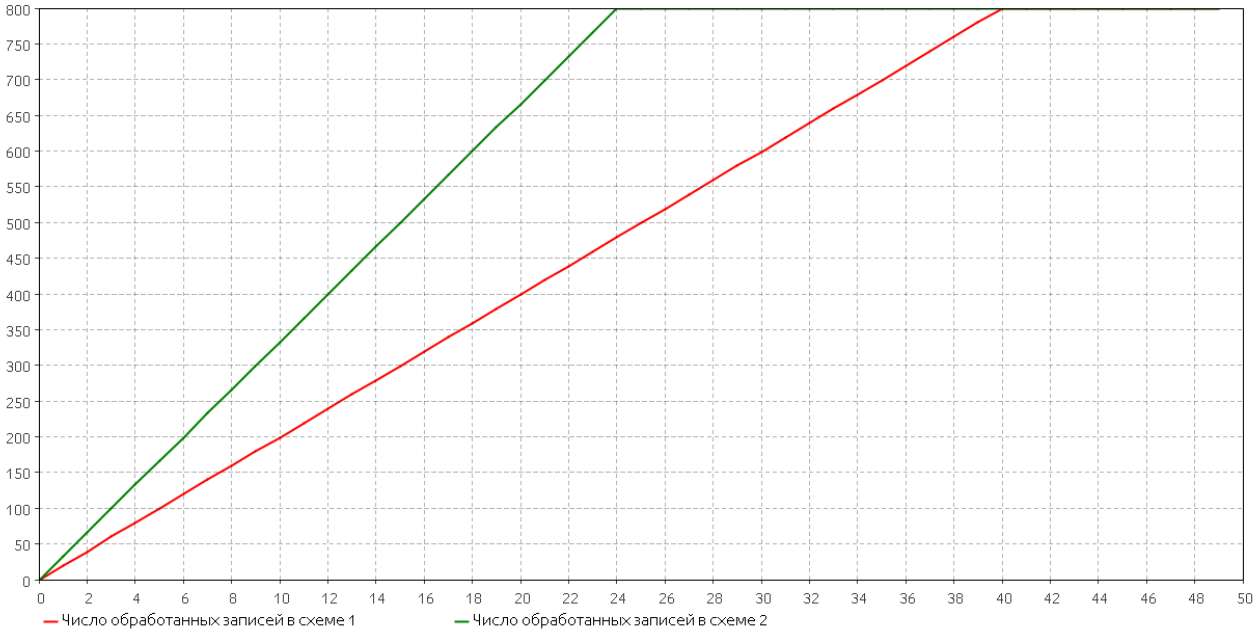


Рисунок 1.22: Время проверки целостности истории из 800 записей

# Глава 2

# КОНСТРУКТОРСКАЯ ЧАСТЬ

## 2.1 Математическая постановка задачи

Пусть вероятность получения корректного документа (документа, не содержащего ошибок) после обработки i-м редактором в схеме рис. 1.1 равна $p_i$. Тогда вероятность получения корректного документа после обработки последовательно $N$ редакторами равна

$$P = \prod_{i=1}^{N} p_i.$$

При обработке документов в соответствии со схемой рис. 1.3 АС исправляет часть ошибок редактора. Детектируемые ошибки появляются при редактировании с вероятностью

$$P_{AC} = P_{data} + (1 - P_{data})P_{auth} + (1 - P_{data})(1 - P_{auth})P_{den} + (1 - P_{auth})(1 - P_{data})(1 - P_{den})P_{txt}. \tag{2.1}$$

Вероятность отклонения автоматизированной системой (вероятность возврата на доработку) равна

$$P'_{AC} = P'_{data} + (1 - P'_{data})P'_{auth} + (1 - P'_{data})(1 - P'_{auth})P'_{den} + (1 - P'_{auth})(1 - P'_{data})(1 - P'_{den})P'_{txt}, \tag{2.2}$$

где вероятности $P'_i$ обозначают одновременное наступление двух событий: появление ошибки $k$ и её обнаружение соотв. модулем АС.

Вероятность появления *недетектируемых* ошибок — $P_A$.

Вероятность возникновения ошибки на $i$-том узле в процессе документооборота составляет $P_{A_i} + P_{AC_i}$. В случае использования АС для обнаружения ошибок она уменьшается до $P_{A_i} + (P_{AC_i} - P'_{AC_i})$.

Пусть процесс документооборота характеризуется графом $G(V, E)$, изображённым на рис. 1.5.

Пусть $M = \{m_1, m_2, ...\}$ — множество всех возможных маршрутов при обработке документа. Тогда любой маршрут $m \in M$ характеризуется упорядоченным набором весов рёбер, лежащих на нём: $m = (p_{ij}); i, j \in V$. Тогда показатель эффективности СЭД соответствует вероятности получения корректного документа после обработки:

$$\sum_{m \in M} (\prod_{p_{ij} \in m} p_{ij}(1 - P_{\text{ош.}})),$$

где $P_{\text{ош.}_j} = P_{A_j} + P_{AC_j}$ — вероятность ошибки для классического документооборота. Для СЭД вероятность ошибки составляет $P_{\text{ош.}_j} = P_{A_j} + (P_{AC_j} - P'_{AC_j})$.

Задачей дипломного проектирования является повышение показателя эффективности:

$$\begin{cases} E_k = \frac{\sum_{m \in M}(\prod_{p_{ij} \in m} p_{ij}(1 - P'_{\text{ош.}}))}{\sum_{m \in M}(\prod_{p_{ij} \in m} p_{ij}(1 - P_{\text{ош.}}))} = \frac{\sum_{m \in M}(\prod_{p_{ij} \in m} p_{ij}(1 - (P_{A_j} + (P_{AC_j} - P'_{AC_j}))))}{\sum_{m \in M}(\prod_{p_{ij} \in m} p_{ij}(1 - (P_{A_j} + P_{AC_j})))} > E_{\text{пред.}} \\ E_{\text{пред.}} > 1 \end{cases}$$

## 2.2 Обоснование структуры системы в защищённом исполнении

В рамках разработки защищенной системы электронного документооборота необходимо обеспечить решение следующих задач:

- предоставление пользователю интерфейса использования функций разрабатываемого ПО;
- управление учётными записями пользоваетлей;
- идентификация и аутентификация пользователей;
- передача документов и метаданных;
- обработка вносимых в документ и метаданные изменений;
- хранение внесённых изменений;
- отображение истории внесённых изменений и текущего состояния документа.

В качестве основных требований к конструкции ПО можно указать следующие:

- конструкция ПО не должна отрицательно влиять на производительность;

- пользователь ПО должен быть обеспечен удобным интерфейсом для работы;
- конструкция разрабатываемого ПО должна способствовать обеспечению достаточного уровня производительности;
- конструкция разрабатываемого ПО должна соответствовать выбранной в исследовательской части.

Рассмотренные задачи и требования обуславливают следующую структуру системы (рис. 2.1)

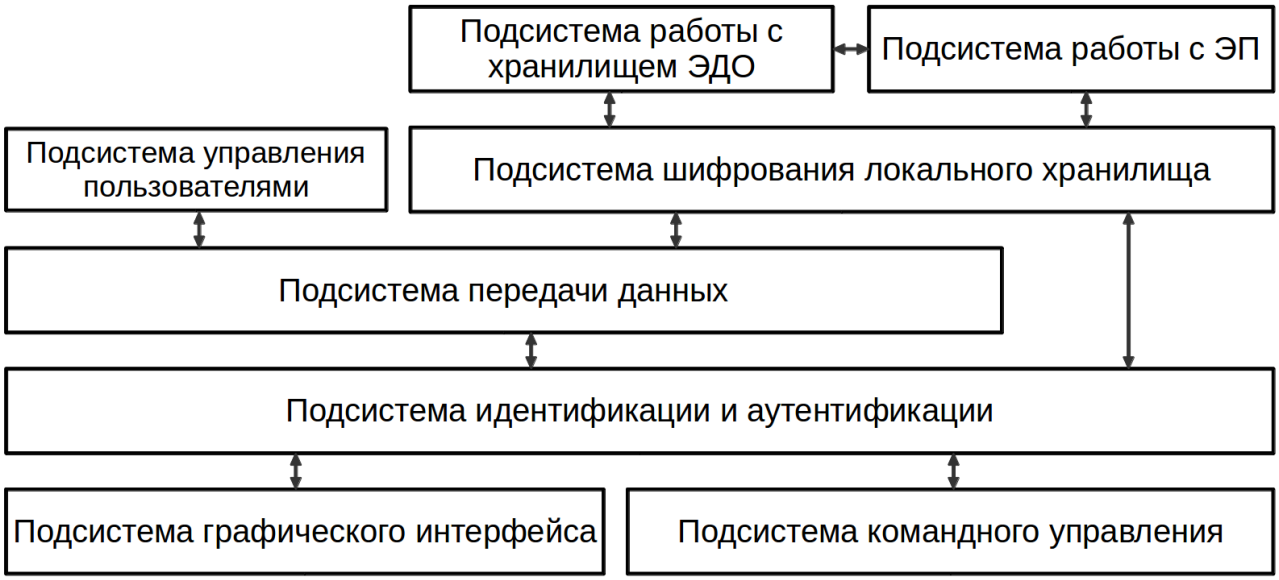


Рисунок 2.1: Общая структура разрабатываемого ПО

**Подсистема графического интерфейса** должна обеспечивать:

- возможность просмотра истории документов;
- возможность просмотра сотояния любого документа в любой момент времени;
- возможность проверки статуса электронной подписи записей истории.

**Подсистема командного управления** должна обеспечивать предоставления интерфейса для выполнения всех функций системы.

**Подсистема идентификации и аутентификации** выполняет проверку идентификаторов пользователей и осуществляет их аутентификацию в системе.

**Подсистема передачи данных** отвечает за передачу данных между клиентами и серверами по защищённому каналу в случае необходимости. Защита канала осуществляется по протоколам ssh и https.

**Подсистема управления пользователями** реализует механизм разграничения доступа.

**Подсистема шифрования локального хранилища** обеспечивает шифрование ХЭД как на стороне клиента, так и на стороне сервера. Может быть ореализована на основе TrueCrypt или другой подобной системы.

**Подсистема работы с электронной подписью** реализует операции создания и проверки электронной подписи. Использует механизмы GPG и OpenSSL.

**Подсистема работы с хранилищем электронных документов** реализует все функции работы с документами и их историей, кроме тех, которые требуют проведения криптографических операций.

Общий алгоритм действий программы представлен на рис. 2.2.

Как следует из представленной структуры, разрабатываемое ПО имеет сложную многокомпонентную структуру, что обуславливает целесообразность реализации программных средств не как автономно работающего приложения, а как программного пакета, содержащего исполняемые модули, библиотеки данных и другие информационные ресурсы.

К достоинствам такого подхода можно отнести масштабируемость, простоту разработки, а также возможность более гибкого распределения задач между программистами при организации управления программным проектом.

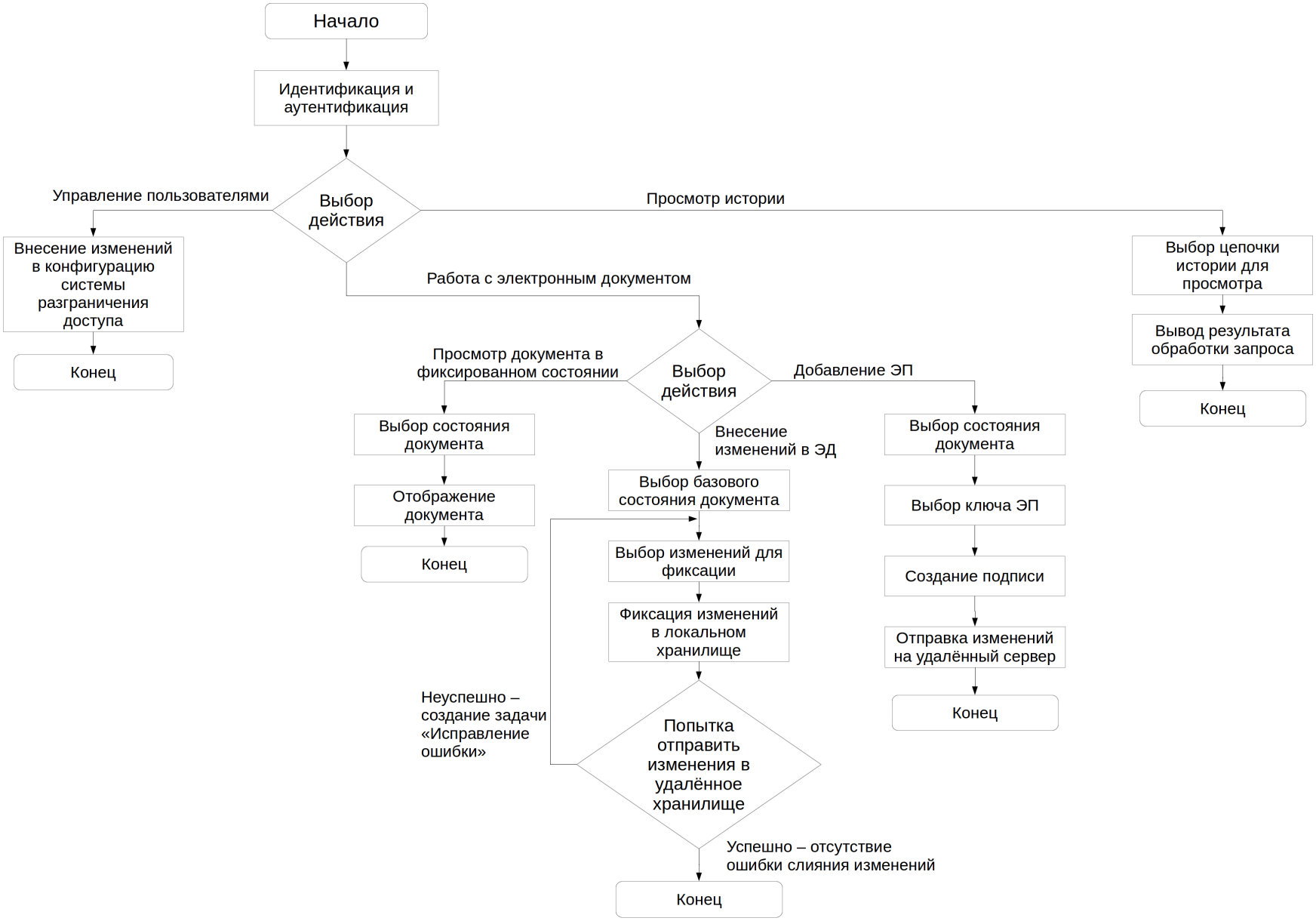


Рисунок 2.2: Общий алгоритм действий программы

# Глава 3

# ТЕХНОЛОГИЧЕСКАЯ ЧАСТЬ

## 3.1 Введение

Разрабатываемое программное обеспечение должно обеспечить защищённость информации при обработке в системе электронного документооборота. Язык программирования, с помощью которого будет написано данное программное обеспечение, должен удовлетворять требованиям по быстродействию, переносимости для поддержки максимально возможного числа пользовательских программных платформ, а также обеспечить защищенность системы в соответствии с результатами исследований данного дипломного проекта.

## 3.2 Выбор языка реализации

При выборе языка реализации, разработчик сталкивается с необходимостью учета следующих аспектов:

- возможность разработки приложений, поддерживаемых большинством современных веб-браузеров;
- возможность разработки приложений, поддерживаемых большинством современных клиентских платформ;
- особенности системы разработки программного обеспечения (простота использования, открытость, наличие доступной справочной документации);
- опыт конкретного разработчика в области проектирования и написания кода для этого языка программирования.

С учётом перечисленных требований, в качестве возможных языков программирования рассматривались: Perl, Bash, Python, PHP. Все они являются гибкими и современными и позволяют решить поставленную задачу. С учётом имеющихся наработок в области программирования пользовательских сценариев для работы в системах контроля версий было отдано предпочтение языкам Perl и Bash.

Для конфигурации поведенческих сценариев будет использоваться язык Bash, а для модификации средства просмотра истории gitweb — Perl. Так как данные языки являются открытыми и свободно распространяемыми, а также не требуют специальных средств отладки, в качестве среды исполнения будут выступать стандартные интерпретаторы Perl и Bash, а также PowerShell для Windows.

## 3.3 Выбор формата представления данных

Структура данных, используемых в работе программного обеспечения:

- Исходные данные
  - Структура с измненениями документа
  - Идентификатор пользователя
- Запись в истории изменений
  - Идентификатор пользователя
  - Фиксируемые изменения в документе
  - Описание фиксируемых изменений
  - Указатель на предыдущую запись в истории изменений (хэш-сумма)
  - ЭП пользователя, подтверждающая подлинность изменений, их описания и положения в истории
- Отчёт об истории внесённых изменений
  - Цепочка изменений в порядке добавления, результаты проверки ЭП каждого изменения

## 3.4 Выбор системы контроля версий

Для хранения истории вносимых изменений, а также синхронизации данных между хранилищами будет использоваться система контроля версий — программное обеспечение, разработанное для удобства совместной разработки ПО: синхронизации данных и слияния веток разработки. Такие системы решают задачи, схожие с задачами электронного документооборота, и на их основе можно строить СЭД [11].

Системы контроля версий делятся на:

- Централизованные — имеется общий сервер для хранения документов, клиенты работают в режиме он-лайн;

- Децентрализованные — все участники информационного обмена равноправны. Обычно на уровне политики принимается некоторый центральный сервер, который считается эталоном. Пользователи могут работать в режиме оффлайн, время от времени синхронизируя данные и сливая ветки разработки друг с другом.

В применении к системе электронного документооборота разумным выглядит применение децентрализованной системы ввиду масштабируемости и гибкости развёртывания, а также простоте создания резервных копий. Среди всех децентрализованных систем контроля версий была выбрана система Git как самая распространённая и хорошо документированная.

## 3.5 Вывод

В данной части был произведен выбор языка программирования с учетом требований к разрабатываемому ПО. Для системы контроля версий, спроектированной в рамках конструкторской части, была выбрана система Git с учётом гибкости настройки и широкого функционала.

# Глава 4

# ОРГАНИЗАЦИОННО-ПРАВОВАЯ ЧАСТЬ

## 4.1 Введение

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищённость национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы её обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Российской Федерации. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Российской Федерации.

Законодательные меры по защите информации предусматривают создание в стране законодательной базы, предусматривающей разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля над исполнением требований в указанных документах.

Правовое обеспечение информационной безопасности Российской Федерации представляет собой систему правового регулирования общественных отношений в области противодействия угрозам национальных интересов Российской Федерации в информационной сфере. Оно включает в себя согласованную систему нормативных актов, регулирующих рассматриваемые отношения, а также согласованную деятельность органов государственной власти по их развитию и совершенствованию.

## 4.2 Конституция Российской Федерации

Конституция Российской Федерации, принятая на всенародном голосовании 12 декабря 1993 года, имеет высшую юридическую силу и прямое действие и применяется на всей территории Российской Федерации. Она является основным источником права в Российской Федерации, в том числе в области обеспечения информационной безопасности Российской Федерации.

Согласно статье 23 Конституции Российской Федерации, каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Данная статья подтверждает необходимость защиты информации, передаваемой по открытым каналам связи.

Статья 29 гласит, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом. Для обеспечения этого права необходимо позаботиться о доступности информации.

## 4.3 Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации, принятая 23 июня 2000 года Советом безопасности РФ, представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина информационной безопасности служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Доктрина информационной безопасности Российской Федерации развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

В соответствии с доктриной информационной безопасности Российской Федерации, основными объектами обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;
- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;
- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа.

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;
- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;
- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;
- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;
- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;
- обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;
- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;
- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

## 4.4 Федеральный закон «Об информации, информационных технологиях и о защите информации»

Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации», принятый Государственной Думой 8 июля 2006 года, одобренный Советом Федерации 14 июля 2006 года, вступивший в силу 27 июля 2006 года после публикации в Российской газете (№4131), регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Положения Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

Согласно ФЗ №149, правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания

и эксплуатации государственных информационных систем не установлена федеральными законами.

Федеральный закон гласит, что информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Статья 16 Федерального закона «Об информации, информационных технологиях и о защите информации» посвящена защите информации. Согласно ей защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа,
- реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

## 4.5 Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

Приказ ФСБ РФ от 09 февраля 2005 года №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», вступивший в силу через 10 дней после публикации в Российской газете (№55 от 19 марта 2005 года), создан с целью определения порядка разработки, производства, шифровальных (криптографических) ограниченным доступом, не реализации средств содержащей государственную тайну.

Положением необходимо руководствоваться при разработке, производстве, реализации и эксплуатации средств криптографической защиты информации конфиденциального характера в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее - государственные органы);
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее - организации, выполняющие государственные заказы);
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;
- при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Положение регулирует порядок разработки, производства, реализации и эксплуатации системы криптографической защиты информации.

## 4.6 Гражданский кодекс Российской Федерации. Часть четвёртая

Гражданский кодекс Российской Федерации, вступивший в силу 18 декабря 2006 года, в части четвертой регулирует вопросы охраны результатов интеллектуальной деятельности и средств индивидуализации. Согласно ГК РФ, статья 1225, к результатам интеллектуальной деятельности, которым предоставляется правовая охрана, в числе прочих относятся: произведения науки и программы для электронных вычислительных машин (ЭВМ).

Статья 1228 гласит, что автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Не признаются авторами результата интеллектуальной деятельности граждане, не внесшие личного творческого вклада в создание такого результата, в том числе оказавшие его автору только техническое, консультационное, организационное или материальное содействие или помощь либо только способствовавшие оформлению прав на такой результат или его использованию, а также граждане, осуществлявшие контроль за выполнением соответствующих работ.

Согласно статье 1259, объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения. К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения. Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей. В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 ГК РФ. Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования.

Таким образом, для объектов авторского права важно иметь средства подтверждения авторства и времени создания.

## 4.7 Уголовный кодекс Российской Федерации

Уголовный кодекс Российской Федерации, вступивший в силу 13 июня 1996 года, ставит своей целью охрану прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человече-

ства, а также предупреждение преступлений. В частности в нем рассматриваются вопросы обеспечения информационной безопасности. Статья 272 Уголовного Кодекса РФ предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование модификацию либо копирование информации, нарушение работы вычислительной системы.

Данная статья защищает право владельца на неприкосновенность информации в системе. Владельцем информационной системы может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы или как лицо, приобретшее право использования компьютера.

Преступное деяние, ответственность за которое предусмотрено ст. 272, состоит в неправомерном доступе к охраняемой законом компьютерной информации, который может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные защиты, незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

По уголовному законодательству субъектами компьютерных преступлений могу быть лица, достигшие 16-летнего возраста, однако часть вторая статьи 272 предусматривает наличие дополнительного признака к субъекта, совершившего данное деяние — служебное положение, а равно доступ к ЭВМ, системе ЭВМ или сети ЭВМ, способствовавших его совершению.

Статья 272 УК не регулирует ситуацию, когда неправомерный доступ осуществляется в результате неосторожных действий.

## 4.8 Федеральный закон «О коммерческой тайне»

Федеральный закон №98-ФЗ «О коммерческой тайне» принят Государственной Думой 09 июля 2004 года, одобрен Советом Федерации 15 июля 2004 года и вступил в силу 16 августа 2004 года после публикации в Российской газете (№3543). Цель данного закона — ограничить нелегальный отток служебной информации коммерческого характера от одной компании к другой.

Коммерческая тайна определяется как конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или

получить иную коммерческую выгоду. Закон предусматривает, что обладатель коммерческой тайны имеет право устанавливать, изменять и отменять в письменной форме режим коммерческой тайны.

Закон также устанавливает, что срок неразглашения работником информации, составляющей коммерческую тайну определяется соглашением между сотрудником и компанией, если такое соглашение не подписывалось, срок составляет три года с момента прекращения действия трудового договора. Помимо этого в документе вводится понятие ответственности за разглашение коммерческой тайны и за непредставление органам государственной власти и местного самоуправления информации, составляющей коммерческую тайну, по специальному требованию.

Закон вводит то, что пострадавшая от разглашения коммерческой тайны компания сможет в Арбитражном суде потребовать возмещения всего доказанного ущерба у компании, которая воспользовался утечкой, или у представителей власти, виновных в утечке секретов.

В тексте документа оговаривается, что коммерческую тайну не могут составлять сведения о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, качестве пищевых продуктов и других факторах, связанных с обеспечением безопасности населения. Кроме того, не может засекречиваться информация, имеющаяся в учредительных документах юридического лица, о численности и составе работников организаций, о системе оплаты труда и задолженности работодателей по выплате зарплаты. Помимо этого в законе установлен круг лиц, которым предприятия обязаны предоставлять информацию, относящуюся к разряду коммерческой тайны. Это касается запросов со стороны судов и органов прокуратуры. Круг лиц, обязанных осуществлять меры по охране конфиденциальности информации, дополнен индивидуальными предпринимателями.

## 4.9 Федеральный закон «О персональных данных»

Федеральный закон №152-ФЗ «О персональных данных» принят Государственной Думой 08 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года и вступил в силу 26 января 2007 года после публикации в Российской газете (№4131). Данный закон направлен на реализацию конституционных положений, закрепляющих право каждого на неприкосновенность частной жизни и свободу информации, а также международных обязательств Российской Федерации по ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных.

В законе устанавливаются общие унифицированные требования к обработке персональных данных во всех сферах, где используются эти данные, определяются права субъектов персональных данных и обязанности операторов, осуществляющих обработку данных, принципы

трансграничной передачи персональных данных, а также меры государственного контроля за деятельностью государственных и муниципальных органов, юридических и физических лиц, связанной с обработкой персональных данных.

Федеральным законом допускаются различные способы учета персональных данных в государственных и муниципальных информационных системах, в том числе различные способы обозначения принадлежности персональных данных конкретному лицу.

В государственных и муниципальных информационных системах предусматривается возможность создания государственного регистра населения, правовой статус и порядок работы с которым устанавливаются федеральным законом.

Обеспечение контроля и надзора за соответствием обработки персональных данных возлагается на уполномоченный орган по защите прав субъектов персональных данных, которым является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Россвязькомнадзор осуществляет контроль и надзор за соответствием обработки ПДн требованиям законодательства. ФСТЭК России устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий. ФСБ России устанавливает методы и способы защиты информации в информационных системах в пределах своих полномочий (регулирует сферу использования криптографических средств защиты информации).

## 4.10 Федеральный закон «Об электронной подписи»

Федеральный закон №63-ФЗ «Об электронной подписи», принятый Государственной Думой 25 марта 2011 года, одобренный Советом Федерации 30 марта 2011 года, вступивший в силу 8 апреля 2011 года после публикации в Российской газете (№5451), регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

В ФЗ №63 используются следующие понятия:

- электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;
- сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

- квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

- владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

- ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

- ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

- удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

- аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

- средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

- средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

- участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

- корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

- информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Статья 6 определяет условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:

- Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

- Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

- Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

- Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

В статье 9 определяются условия, при выполнении которых электронный документ считается подписанным простой электронной подписью:

- простая электронная подпись содержится в самом электронном документе;

- ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Таким образом, ФЗ №63 определяет условия, при которых бумажный документооборот может быть заменён электронным.

## 4.11 Постановление Правительства Российской Федерации «О мерах по совершенствованию электронного документооборота в органах государственной власти»

Постановление Правительства Российской Федерации «О мерах по совершенствованию электронного документооборота в органах государственной власти» от 06 сентября 2012 года №890 устанавливает, что переход на обмен электронными документами при взаимодействии федеральных органов исполнительной власти между собой и с Правительством Российской Федерации осуществляется по мере готовности к такому обмену информационно-технологической инфраструктуры, входящей в состав информационных систем электронного документооборота указанных органов, имея в виду, что этот переход необходимо завершить до 31 декабря 2017 года, а перед началом обмена электронными документами каждый из участников информационного взаимодействия должен подтвердить готовность своей информационной системы электронного документооборота к подобному обмену.

## 4.12 ГОСТ Р ИСО 15489-1 — 2007

ГОСТ Р ИСО 15489-1 — 2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования» регулирует процессы управления документами государственных или коммерческих организаций, предназначаемыми для внутреннего или внешнего пользования.

В статье 4 описываются преимущества управления документами. Так, документы содержат информацию, являющуюся ценным ресурсом и важным элементом деловой деятельности. Системный подход к управлению документами позволяет организациям и обществу защищать и сохранять документы в качестве доказательства действий. Система управления документами позволяет создать информационный ресурс о деловой деятельности, который может поддерживать последующую деятельность и отдельные решения, а также обеспечивать подотчетность всем заинтересованным сторонам. Данная статья аргументирует необходимость хранения полной и достоверной истории изменения документа.

Статья 7.2 «Характеристики документа» описывает признаки надёжного документа:

- Документ является аутентичным, если он:
    1. является тем, чем должны быть;
    2. был создан или отправлен лицом, уполномоченным на это;
    3. был создан или отправлен в то время, которое обозначено в документе.
- Достоверным является документ, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности. Документы должны создаваться во время или сразу же после операции или случая, к которым они

относятся, лицами, достоверно знающими факты, или средствами, обычно используемыми в деловой деятельности при проведении данной операции.

- Целостность документа определяется его полнотой и неизменностью.
- Пригодным для использования является документ, который можно локализовать, найти, воспроизвести и интерпретировать.

## 4.13 Выводы

Нормативно-правовые акты различного уровня определяют условия, при которых бумажный документооборот может быть заменён электронным. Одно из важнейших условий — обеспечение информационной безопасности обрабатываемых документов. Необходимо как обеспечить юридическую значимость документов, так и выполнить требования по защите конфиденциальной, коммерческой и иной информации, а также персональных данных согласно соответствующим нормативно-правовым актам.

Кроме того, ГОСТ Р ИСО 15489-1 устанавливает, что в процессе документооборота должна полно и достоверно храниться история изменения документа. Этот вопрос — один из тех, которые не решаются современными системами электронного документооборота, что является обоснованием для новой разработки.

# Глава 5

# ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКАЯ ЧАСТЬ

## 5.1 Введение

Процесс разработки сложного ПО предполагает необходимость координации значительного количества весьма разноплановых работ, в которых принимают участие специалисты различного профиля и квалификации. Необходимость обеспечения эффективности разработки требует формирования единого плана, предусматривающего окончание всего комплекса работ и отдельных его составляющих в заданные сроки и при лимитированных издержках.

Анализ предстоящей разработки целесообразно проводить, представляя работу в виде экономико-функциональных блоков, что позволяет спланировать деятельность оптимальным образом и обоснованно спрогнозировать конкретные сроки выполнения отдельных этапов работы. Построение диаграммы Гантта позволяет наглядно представить последовательные и параллельные участки, продолжительность и очерёдность работ.

## 5.2 Расчёт трудоёмкости проекта

Общие затраты труда на разработку и ПО определим следующим образом:

$$Q_p = \sum_i T_i, \tag{5.1}$$

где $T_i$ — затраты труда на выполнение $i$-го этапа проекта.

Используя метод экспертных оценок, вычислим ожидаемую продолжительность работ $T$ каждого этапа по формуле:

$$T = \frac{3 \cdot T_{MIN} + 2 \cdot T_{MAX}}{5}, \tag{5.2}$$

где $T_{MAX}$ и $T_{MIN}$ – максимальная и минимальная продолжительность работы. Они назначаются в соответствии с экспертными оценками, а ожидаемая продолжительность работы рассчитывается как математическое ожидание для $\beta$- распределения.

Полный перечень работ с разделением их по этапам приведён в таблице 5.1.

Таблица 5.1: Распределение работ по этапам

| № | Этап | № работы | Содержание работы | $T_{MIN}$, чел / часы | $T_{MAX}$, чел / часы | $T$, чел / часы | $T$, чел / дни |
|---|---|---|---|---|---|---|---|
| 1 | Разработка технических требований | 1 | Получение задания, анализ полученных требований к разрабатываемому ПО | 8 | 8 | 8 | 1 |
| | | 2 | Разработка и утверждение ТЗ | 24 | 24 | 24 | 3 |
| | | 3 | Анализ предметной области и существующих решений | 24 | 44 | 32 | 4 |
| | | 4 | Анализ потоков данных в процессе электронного документооборота | 72 | 92 | 80 | 10 |
| 2 | Разработка алгоритмов | 5 | Разработка общей структуры ПО и пользовательского интерфейса | 24 | 44 | 32 | 4 |
| | | 6 | Разработка алгоритмов, структуры входных и выходных данных | 64 | 84 | 72 | 9 |
| 3 | Разработка программных модулей | 7 | Реализация пользовательского интерфейса | 32 | 52 | 40 | 5 |
| | | 8 | Программная реализация модулей защищенной обработки, передачи и хранения информации | 72 | 92 | 80 | 10 |
| 4 | Тестирование и отладка разрабатываемого ПО | 9 | Тестирование ПО | 64 | 84 | 72 | 9 |
| | | 10 | Внесение изменений в ПО | 32 | 52 | 40 | 5 |
| 5 | Разработка документации | 11 | Разработка программной и эксплуатационной документации | 64 | 84 | 72 | 9 |
| Итого $Q_P$: | | | | 616 | | | 77 |

$$Q_P = Q_{\text{ОЖ}} = 77(\text{чел/дней}) = 616(\text{чел/час}).$$

### 5.2.1 Определение численности исполнителей

Для оценки возможности выполнения проекта имеющимся в распоряжении разработчика штатным составом исполнителей нужно рассчитать их среднее количество, которое при реализации проекта разработки и внедрения ПО определяется соотношением:

$$N = \frac{Q_P}{F}, \tag{5.3}$$

где $Q_P$ — затраты труда на выполнение проекта (разработка и внедрение ПО), а $F$ — фонд рабочего времени, который определяется по формуле:

$$F_M = T \cdot \frac{t_P \cdot (D_K - D_B - D_{\text{П}})}{12}, \tag{5.4}$$

где $T$ — время выполнения проекта в месяцах, $t_P$ — продолжительность рабочего дня, $D_K$ — общее число дней в году, $D_B$ — число выходных дней в году, $D_{\text{П}}$ — число праздничных дней в году.

Таким образом, фонд времени в текущем месяце 2014 года составляет

$$F_M = \frac{8 \cdot (365 - 104 - 14)}{12} = 165 \text{ часов/мес.} \tag{5.5}$$

Время выполнения проекта $T = 3,5$ (месяца).

Величина фонда рабочего времени составляет:

$$F = T \cdot F_M = 577,5 \text{ ч.} \tag{5.6}$$

Затраты труда на выполнения проекта были рассчитаны в предыдущем разделе, их величина равна $616$ чел/час. В соответствии с этими данными и выражением (5.3), среднее количество исполнителей равно:

$$N = \frac{616}{577,5} = 1,07. \tag{5.7}$$

Округляя до большего, получим число исполнителей проекта $N = 2$.

### 5.2.2 Построение сетевого графика

Для определения временных затрат и трудоемкости разработки ПО используем метод сетевого планирования. Метод сетевого планирования позволяет установить единой схемой связь

между всеми работами в виде наглядного и удобного для восприятия изображения (сетевого графика), представляющего собой информационно-динамическую модель, позволяющую определить продолжительность и трудоёмкость, как отдельных этапов, так и всего комплекса работ в целом.

Составление сетевой модели включает в себя оценку степени детализации комплекса работ и определения логической связи между отдельными работами. С этой целью составляется перечень всех основных событий и работ. В перечне указываются кодовые номера событий, наименования событий в последовательности от исходного к завершающему, кодовые номера работ, перечень всех работ, причём подряд указываются все работы, которые начинаются после наступления данного события.

Основные события и работы проекта представлены в таблице 5.2.

Таблица 5.2: Основные события и работы проекта

| $N_i$ | Наименование события | Код работы | Работа | $t$, чел / час | $t$, чел / день |
|---|---|---|---|---|---|
| 0 | Разработка ПО начата | 0-1 | Получение задания, анализ полученных требований к разрабатываемому ПО | 8 | 1 |
| 1 | Анализ полученных требований к разрабатываемому ПО проведен | 1-2 | Разработка и утверждение ТЗ | 24 | 3 |
| 2 | ТЗ разработано и утверждено | 2-3 | Анализ предметной области и существующих решений | 32 | 4 |
| 3 | Анализ предметной области и существующих решений проведён | 3-4 | Анализ потоков данных в процессе электронного документооборота | 80 | 10 |
| 4 | Анализ потоков данных в процессе электронного документооборота проведён | 4-5 | Разработка общей структуры ПО и пользовательского интерфейса | 32 | 4 |

*продолжение следует*

*(продолжение)*

| $N_i$ | Наименование события | Код работы | Работа | $t$, чел / час | $t$, чел / день |
|---|---|---|---|---|---|
| 5 | Разработка общей структуры ПО и пользовательского интерфейса завершена | 5-6 | Разработка алгоритмов, структуры входных и выходных данных | 72 | 9 |
| 6 | Разработка алгоритмов, структуры входных и выходных данных завершена | 6-7 | Реализация пользовательского интерфейса | 40 | 5 |
| | | 6-8 | Программная реализация модулей защищенной обработки, передачи и хранения информации | 80 | 10 |
| 7 | Реализация пользовательского интерфейса завершена | 7-8 | Фиктивная работа | 0 | 0 |
| 8 | Программная реализация модулей защищенной обработки, передачи и хранения информации завершена | 8-9 | Тестирование ПО | 64 | 8 |
| | | 8-10 | Разработка документации | 80 | 10 |
| 9 | Тестирование ПО завершено | 9-11 | Внесение изменений в ПО | 40 | 5 |
| 10 | Документация разработана | 1-12 | Фиктивная работа | 0 | 0 |
| 11 | Внесение изменений в ПО закончено | 11-12 | Фиктивная работа | 0 | 0 |
| 12 | Разработка ПО закончена | — | — | — | — |

Рассчитанные оставшиеся параметры элементов сети (сроки наступления событий, резервы времени событий, полный и свободный резервы времени работ) приведены в таблице 5.3.

Таблица 5.3: Временные затраты на каждый этап работы

| $N_i$ | Код работы $i-j$ | $t_{i-j}$, чел / день | $T_i^P$, чел / день | $T_i^{\text{П}}$, чел / день | $R_i$, чел / день | $R_{i-j}^{\text{П}}$, чел / день | $R_{i-j}^C$, чел / день |
|---|---|---|---|---|---|---|---|
| 0 | 0-1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1-2 | 3 | 1 | 1 | 0 | 0 | 0 |
| 2 | 2-3 | 4 | 4 | 4 | 0 | 0 | 0 |
| 3 | 3-4 | 10 | 8 | 8 | 0 | 0 | 0 |
| 4 | 4-5 | 4 | 18 | 18 | 0 | 0 | 0 |
| 5 | 5-6 | 9 | 22 | 22 | 0 | 0 | 0 |
| 6 | 6-7 | 5 | 31 | 31 | 0 | 5 | 0 |
| | 6-8 | 10 | | | | 0 | 0 |
| 7 | 7-8 | 0 | 36 | 41 | 5 | 0 | 0 |
| 8 | 8-9 | 8 | 41 | 41 | 0 | 0 | 0 |
| | 8-10 | 10 | | | | 3 | 0 |
| 9 | 9-11 | 5 | 49 | 49 | 0 | 0 | 0 |
| 10 | 10-12 | 0 | 51 | 54 | 3 | 0 | 0 |
| 11 | 11-12 | 0 | 54 | 54 | 0 | 0 | 0 |
| 12 | - | - | 54 | 54 | 0 | 0 | 0 |

Здесь **ранний срок совершения события** $T_j^P$ определяет минимальное время, необходимое для выполнения всех работ, предшествующих данному событию и равен продолжительности наибольшего из путей, ведущих от исходного события к рассматриваемому:

$$T_j^P = max\{T_i^P + t_{i-j}\}. \tag{5.8}$$

**Поздний срок совершения события** $T_i^{\text{П}}$ – это максимально допустимое время наступления данного события, при котором сохраняется возможность соблюдения ранних сроков наступления последующих событий. Поздние сроки равны разности между поздним сроком совершения $j$-го события и продолжительностью работы $i-j$:

$$T_i^{\text{П}} = min\{T_j^{\text{П}} - t_{i-j}\}. \tag{5.9}$$

**Критический путь** – это максимальный путь от исходного события до завершения проекта. Его определение позволяет обратить внимание на перечень событий, совокупность которых имеет нулевой резерв времени.

Все события в сети, не принадлежащие критическому пути, имеют **резерв времени** $R_i$, показывающий, на какой предельный срок можно задержать наступление этого события, не

увеличивая сроки окончания работ:

$$R_i = T_i^{\text{П}} - T_i^P. \tag{5.10}$$

**Полный резерв времени работы** $R_{i-j}^{\text{П}}$ и **свободный резерв времени** $R_{i-j}^C$ работы можно определить, используя следующие соотношения:

$$R_{i-j}^{\text{П}} = T_j^{\text{П}} - T_i^P - t_{i-j}. \tag{5.11}$$

$$R_{i-j}^C = T_j^P - T_i^P - t_{i-j}. \tag{5.12}$$

Полный резерв работы показывает максимальное время, на которое можно увеличить длительность работы или отсрочить ее начало, чтобы не нарушился срок завершения проекта в целом. Свободный резерв работы показывает максимальное время, на которое можно увеличить продолжительность работы или отсрочить ее начало, не меняя ранних сроков начала последующих работ.

Сетевой график приведён на рис. 5.1.

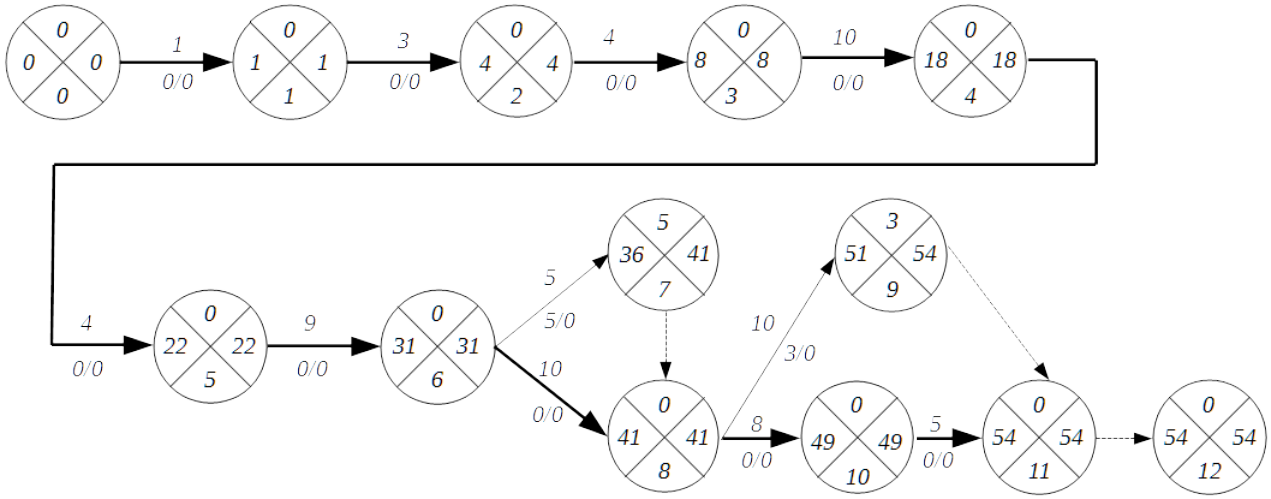


Рисунок 5.1: Сетевой график выполнения работ

### 5.2.3 Диаграмма Гантта

Для иллюстрации последовательности проводимых работ приведем диаграмму Гантта данного проекта, на которой по оси $X$ изображены календарные дни от начала до конца проекта, а по оси $Y$ – выполняемые этапы работ. Диаграмма Гантта приведена на рисунке 5.2. Занятость исполнителей приведена в таблице 5.4.

### 5.2.4 Анализ структуры затрат проекта

Затраты на выполнение проекта могут быть представлены в виде сметы затрат, включающей в себя следующие статьи:

Таблица 5.4: Временные затраты на каждый этап работы

| Код работы | Дата начала | Дата окончания | Исполнитель |
|---|---|---|---|
| 0-1 | 07.02.2014 | 07.02.2014 | Ведущий программист |
| 1-2 | 09.02.2014 | 12.02.2014 | Ведущий программист |
| 2-3 | 13.02.2014 | 18.02.2014 | Ведущий программист |
| 3-4 | 19.02.2014 | 04.03.2014 | Ведущий программист |
| 4-5 | 05.03.2014 | 11.03.2014 | Ведущий программист |
| 5-6 | 12.03.2014 | 24.03.2014 | Ведущий программист |
| 6-7 | 25.03.2014 | 31.03.2014 | Программист |
| 6-8 | 25.03.2014 | 07.04.2014 | Ведущий программист |
| 8-9 | 08.04.2014 | 17.04.2014 | Программист |
| 8-10 | 08.04.2014 | 21.04.2014 | Ведущий программист |
| 9-11 | 22.04.2014 | 28.04.2014 | Ведущий программист |

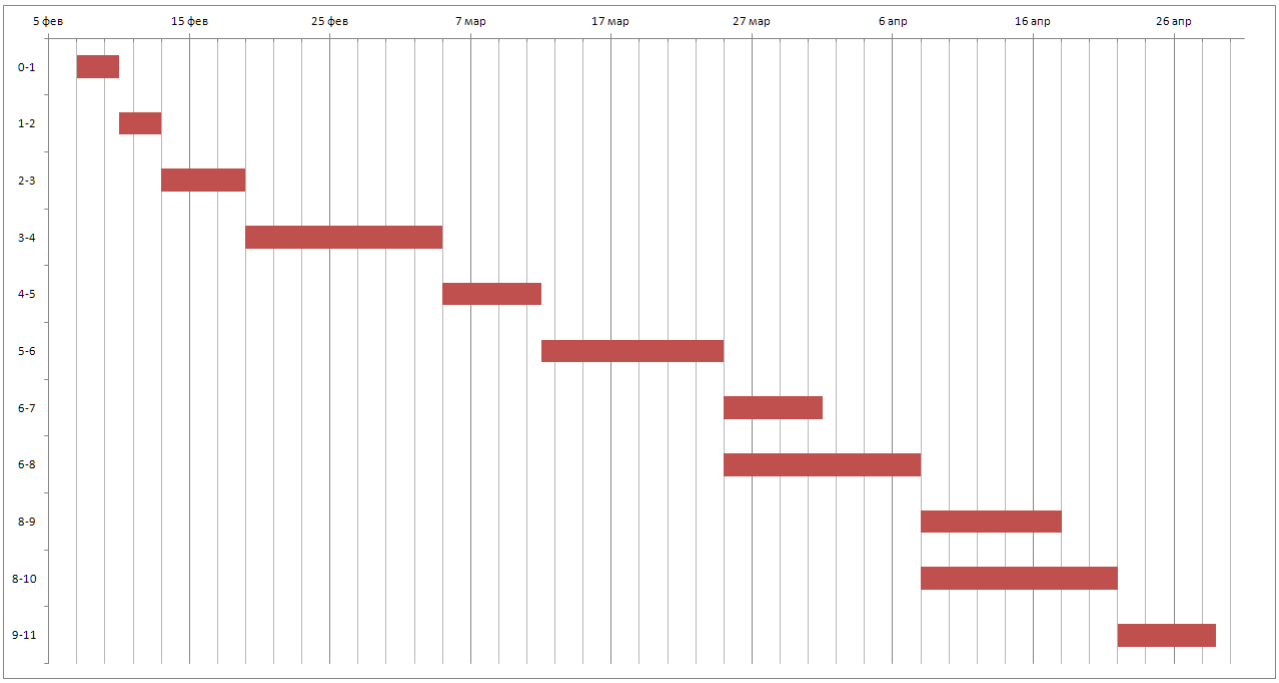


Рисунок 5.2: Диаграмма Гантта проводимых работ

- заработная плата исполнителям;
- отчисления на социальные нужды;
- материальные затраты;
- амортизационные затраты;
- прочие затраты.

### 5.2.5 Затраты на выплату заработной платы

Затраты на выплату исполнителям заработной платы линейно связаны с трудоемкостью и определяется следующим соотношением:

$$C_{\text{ЗАРП}} = C_{\text{З.ОСН}} + C_{\text{З.ДОП}} + C_{\text{З.ОТЧ}}, \tag{5.13}$$

где $C_{\text{З.ОСН}}$ — основная заработная плата, $C_{\text{З.ДОП}}$ — дополнительная заработная плата, $C_{\text{З.ОТЧ}}$ — отчисление с заработной платы.

Расчёт основной заработной платы (оплаты труда непосредственных исполнителей):

$$C_{\text{З.ОСН}} = T_{\text{ЗАН}} \times O_{\text{ДН}}, \tag{5.14}$$

где $T_{\text{ЗАН}}$ — число дней, отработанных исполнителем проекта, а $O_{\text{ДН}}$ — днейвной оклад исполнителя, который при 8-часовом рабочем дней рассчитывается по формуле:

$$O_{\text{ДН}} = \frac{O_{\text{МЕС}} \cdot 8}{F_M}, \tag{5.15}$$

где $O_{\text{МЕС}}$ — месячный оклад, а $F_M$ — месячный фонд рабочего времени (5.4).

С учетом налога на доходы физических лиц размер оклада увеличивается:

$$O_{\text{МЕС}} = O \cdot (1 + \frac{H_{\text{ДФЛ}}}{100}), \tag{5.16}$$

где $O$ — «чистый» оклад, $H_{\text{ДФЛ}}$ — налог на доходы физических лиц ($13\%$).

Сведем результаты расчета в таблицу с перечнем исполнителей и их месячных и дневных окладов, а также времени участия в проекте и рассчитанной основной заработной платой каждого исполнителя (таблица 5.5).

Таблица 5.5: Заработная плата исполнителей

| № | Должность | «Чистый» оклад, руб. | Дневной оклад, руб. | Трудозатраты, чел-дни | Затраты на зарплату, руб. |
|---|---|---|---|---|---|
| 1 | Ведущий программист | 60 000 | 3267,47 | 54 | 176443,37 |
| 2 | Программист | 50 000 | 2722,89 | 15 | 40843,37 |

Из таблицы получим общие затраты проекта на заработную плату исполнителей: $C_{\text{З.ОСН}} = 217286,24$ руб.

Расходы на дополнительную заработную плату учитывают все выплаты непосредственным исполнителям за время, не проработанное производстве, но предусмотренное законодательством. Величина выплат составляет $20\%$ от размера основной заработной платы:

$$C_{\text{З.ДОП}} = 0.2 \cdot C_{\text{З.ОСН}} = 0.2 \cdot 217286,24 = 43457,25(\text{руб.}) \quad (5.17)$$

### 5.2.6 Отчисления на социальные нужды

Согласно нормативным документам суммарные отчисления в пенсионный фонд, фонд социального страхования и фонды обязательного медицинского страхования составляют 30% от размеров заработной платы.

$$C_{\text{З.ОТЧ}} = 0.3 \cdot (C_{\text{З.ОСН}} + C_{\text{З.ДОП}}) = 0.3 \cdot (217286,24 + 43457,25) = 78223,05 \text{ руб.} \quad (5.18)$$

Общие расходы на заработную плату составляют:

$$C_{\text{ЗАРП}} = C_{\text{З.ОСН}} + C_{\text{З.ДОП}} + C_{\text{З.ОТЧ}} = 217286,24 + 43457,25 + 78223,05 = 338966,54 \text{ руб.} \quad (5.19)$$

### 5.2.7 Материальные затраты

Затраты, учитываемые данной статьёй, включают в себя канцелярские товары, расходные материалы для принтера, представлены в таблице 5.6.

Таблица 5.6: Материальные затраты

| № | Наименование | Ед. изм. | Кол-во. | Цена за ед., руб. | Сумма, руб. |
|---|---|---|---|---|---|
| 1 | Носители CD-R (TDK CD-R 700Mb 52x Cake/100) | Упаковка (100шт.) | 1 | 1091 | 1091 |
| 2 | Бумага формата A4 Ballet Classic | Упаковка (500 л.) | 2 | 171 | 342 |
| 3 | Ноутбуки (Lenovo IdeaPad G580 1005M / 2Gb / 500Gb / Intel HD / DVD-RW / 15.6"/ WiFi / DOS) | Шт. | 2 | 10550 | 21100 |
| Итого $C_{\text{ОБ}}$: | | | | | 22533 |

### 5.2.8 Прочие затраты

К прочим затратам в проектах по разработке программного обеспечения обычно относят стоимость обслуживания сетей коммуникации (доступ к сети Интернет) и стоимость необходимого для разработки ПО (сред разработки, операционных систем).

В данном проекте в качестве операционной системы для разработчиков будем использовать свободную ОС Ubuntu 12.04.4 LTS, а в качестве среды разработки — свободный текстовый редактор Vi, свободный компилятор g++ и свободный интерпретатор Perl. Таким образом, затраты данной категории сведены к нулю.

### 5.2.9 Затраты на организацию рабочих мест

Расчет затрат, связанных с организацией рабочих мест для исполнителей проекта, проводится на основе требований СНИПа (санитарные нормы и правила) и стоимости аренды помещения требуемого уровня сервиса.

В соответствии с санитарными нормами расстояние между рабочими столами с видеомониторами должно быть не менее 2 м., а между боковыми поверхностями видеомониторов - не менее 1,2 м. Площадь на одно рабочее место с терминалом или ПК должна составлять не менее 6 кв.м., а объем - не менее 20 куб.м.. Расположение рабочих мест в подвальных помещениях не допускается. Помещения должны быть оборудованы системами отопления, кондиционирования воздуха или эффективной приточно-вытяжной вентиляцией. Таким образом, для размещения двух сотрудников и принтера необходимо помещение (комната) площадью 6+6+3=15 кв. м.

Затраты на аренду помещения можно вычислить исходя из следующего соотношения:

$$C_{\text{ОРГ}} = \frac{C_{\text{КВМ}}}{12} \cdot S \cdot T_{AP}, \tag{5.20}$$

где $C_{\text{КВМ}}$ — стоимость аренды одного квадратного метра площади за год, $S$ — арендуемая площадь рабочего помещения, $T_{AP}$ — срок аренды (мес).

В настоящее время возможна аренда не офисного помещения, а раздельных рабочих мест, оборудованных всеми необходимыми коммуникациями, мебелью и оргтехникой. Стоимость обслуживания каналов телекоммуникации, а также расходных материалов для оргтехники включена в стоимость аренды рабочих мест. Для бизнец-центра «Matrixoffice» (м. Шаболовская) стоимость аренды одного рабочего места составляет 9 000 рублей. С учётом относительно небольших сроков разработки проекта и небольшого штата сотрудников, целесообразно арендовать не отдельное офисное помещение, а рабочие места. Таким образом, стоимость аренды составляет

$$C_{\text{ОРГ}} = 18000 \cdot 3 = 54000(\text{руб.}) \tag{5.21}$$

### 5.2.10 Накладные расходы

Накладные расходы состоят из расходов на производство, управление, техническое обслуживание и прочее. С учётом минимизации затрат, накладные расходы составляют 60% от

основной заработной платы:

$$C_{\text{НАКЛ}} = 0,6 \cdot C_{\text{ОСН}} = 0,6 \cdot 217286,24 = 130371,75 \text{ руб.} \quad (5.22)$$

### 5.2.11 Суммарные затраты на реализацию программного проекта

Круговая диаграмма, отображающая структуру затрат проекта, приведена на рисунке 5.3. Расчёт суммарных затрат на реализацию программного проекта приведён в таблице 5.7.

Таблица 5.7: Суммарные затраты на проект

| № | Статья расходов | Затраты, руб. |
|---|---|---|
| 1 | Заработная плата исполнителям $C_{\text{ЗАРП}}$ | 338 966,54 |
| 2 | Закупка и аренда оборудования $C_{\text{ОБ}}$ | 22 533 |
| 3 | Организация рабочих мест $C_{\text{ОРГ}}$ | 54 000 |
| 4 | Накладные расходы $C_{\text{НАКЛ}}$ | 130 371,75 |
| Суммарные затраты | | 545 871,29 |

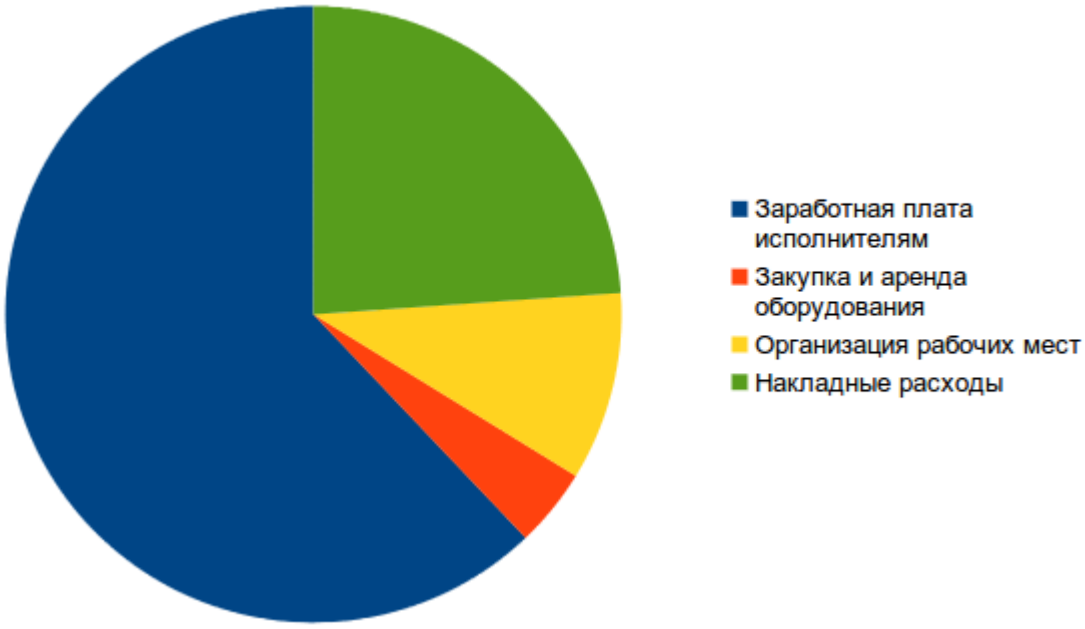


Рисунок 5.3: Структура затрат проекта

## 5.3 Исследование рынка

В разрабатываемом ПО в первую очередь заинтересованы организации, желающие внедрить систему электронного документооборота, одним из направлений деятельности которых является инженерия программного обеспечения. Только среди компаний, занимающихся вопросами информационной безопасности, обладателей лицензии ФСТЭК на деятельность по

разработке и производству средств защиты конфиденциальной информации более тысячи, не считая лицензиатов ФСБ, Минобороны. Общее число предприятий, осуществляющих разработку программного обеспечения в разных областях, составляет не менее 3 000.

На рынке существуют аналоги разрабатываемого ПО. Компания «Логика бизнеса 2.0» разрабатывает систему электронного документооборота «Логика ECM. СЭД», являющуюся частью комплексного решения «Логика ECM» и основанную на платформах IBM Collaboration Solution (Lotus Notes/Domino) и СПО. Однако в качестве клиентского ПО под Linux предлагается Web-доступ, что несовместимо со средствами криптографической защиты информации, применяемыми для работы с электронной подписью. Кроме того, данная система является одной из самых дорогих — от 350 000 руб. для группы из 20 пользователей.

Другие системы, представленные на российском рынке (LanDocs, DIRECTUM, OPTIMA, и т.д.) обладают схожими недостатками — отсутствие полноценных клиентов под свободные платформы (поддерживается только Windows), отсутствие сертификатов ФСТЭК, отсутствие внятно декларированной системы доверенного хранения истории изменений документов.

Более подробный анализ существующих решений представлен в исследовательской части.

Учитывая количество заинтересованных организаций, оценим число потенциальных покупателей на годовом интервале времени $N_P^O = 60$.

### 5.3.1 Планирование цены и прогнозирование прибыли

«Рыночную» стоимость ПО можно рассчитать, используя соотношение (5.23):

$$K_{\text{ПР}} = (\Delta K + K_{\text{ВН}}) + \cdot(1 + D_{\text{ПРИБ}}), \tag{5.23}$$

где $\Delta K$ — часть стоимости разработки, приходящаяся на одну копию программы, $K_{\text{ВН}}$ — стоимость внедрения программы, $D_{\text{ПРИБ}}$ — процент прибыли, заложенный в стоимость.

Частичная стоимость разработки, приходящаяся на каждый комплект ПО, определяется исходя из данных о планируемом объеме установок:

$$\Delta K = \frac{K}{N_P} \cdot (1 + H_{\text{СТ}}), \tag{5.24}$$

где $K$ — стоимость проекта, $N_P$ — планируемое число копий ПО, $H_{\text{СТ}}$ — ставка банковского процента по долгосрочным кредитам (более одного года).

Приняв ставку процента по долгосрочным кредитам 21% (ЗАО КБ «Ситибанк») и используя полученные ранее значения, вычислим:

$$\Delta K = \frac{545871,29}{60} \cdot (1 + 0,21) = 9097,85 \cdot 1,21 = 11008,40 \text{ (руб.)} \tag{5.25}$$

Установим $K_{\text{ПР}} = 40000$ рублей. Данная стоимость ниже среднерыночной, что позволит привлечь б*о*льшее число покупателей.

Тем самым, сумма от продаж за год составит $60 \cdot 40000 = 2400000$ рублей, что обесечивает срок окупаемости проекта менее 1 года.

Определим процент прибыли от одной реализации ПО по формуле:

$$D_{\text{ПРИБ}} = (\frac{K_{\text{ПР}}}{\Delta K + K_{\text{ВН}}} - 1) \cdot 100, \tag{5.26}$$

где $K_{\text{ВН}} = 0$ — затраты на внедрение.

Для данного проекта:

$$D_{\text{ПРИБ}} = (\frac{40000}{11008,40} - 1) \cdot 100 = 363,36. \tag{5.27}$$

Сумма расчётной прибыли от продажи каждой установки ПО с учётом налога на добавочную стоимость $H_{\text{НДС}} = 18\%$:

$$C_{\text{ПРИБ}} = (\Delta K + K_{\text{ВН}}) \cdot D_{\text{ПРИБ}} \cdot (1 - H_{\text{НДС}}) = 11008,40 \cdot 3,6336 \cdot 0,82 = 32800,10 \text{ (руб.)} \tag{5.28}$$

Для оплаты расходов на разработку ПО возьмем кредит в банке ЗАО КБ «Ситибанк» в размере 650000 рублей на срок 24 месяца. Ежемесячный платеж по данному кредиту составляет 33401 руб. Сумма погашения кредита (с учётом комиссии за обслуживание кредита) составляет 801624 рублей.

За первые три месяца разработки продажи равны нулю, т.к. продукт еще не разработан. При этом осуществляются выплаты заработной платы и производятся другие ранее рассчитанные расходы на разработку в размере 545871,29 рублей.

Будем считать, что через три месяца после начала разработки за каждый последующий год продается 60 экземпляров программы (5 в месяц).

Фрагмент таблицы общего баланса приведен в таблице 5.8. Из таблицы видно, что в августе 2014 года возможно досрочное погашение кредита. Структура дохода показана на рисунке 5.4.

Таким образом, на графике видно, что срок окупаемости составляет 7 месяцев.

### 5.3.2 Сервисное обслуживание

Сервисное обслуживание нашего программного обеспечения будет выполнять один сотрудник. Для того, чтобы не обучать новый персонал особенностям нашего программного обеспечения для выполнения данной работы привлечем программиста, который участвовал в разработке программного обеспечения. Так как мы продаём по 5 экземпляров нашего продукта в месяц, то время, которое затратит программист, составит 5 рабочих дней в месяц, 60 дней за год. Затраты на сервисное обслуживание приведены в таблице 5.9

Таблица 5.8: Фрагмент таблицы общего баланса

| Период расчёта | Баланс начальный, руб. | Сумма продаж, руб. | Расход (включая сумму погашения кредита), руб. | Чистая прибыль, руб. | Баланс конечный, руб. | Остаток по кредиту, руб. |
|---|---|---|---|---|---|---|
| 02-04.2014 | 650000,00 | 0,00 | 646074,29 | -646074,29 | 3925,71 | 701421,00 |
| 05.2014 | 3925,71 | 200000,00 | 33401,00 | 166599,00 | 170524,71 | 668020,00 |
| 06.2014 | 170524,71 | 200000,00 | 33401,00 | 166599,00 | 337123,71 | 634619,00 |
| 07.2014 | 337123,71 | 200000,00 | 33401,00 | 166599,00 | 503722,71 | 601218,00 |
| 08.2014 | 503722,71 | 200000,00 | 33401,00 | 166599,00 | 670231,71 | 567817,00 |

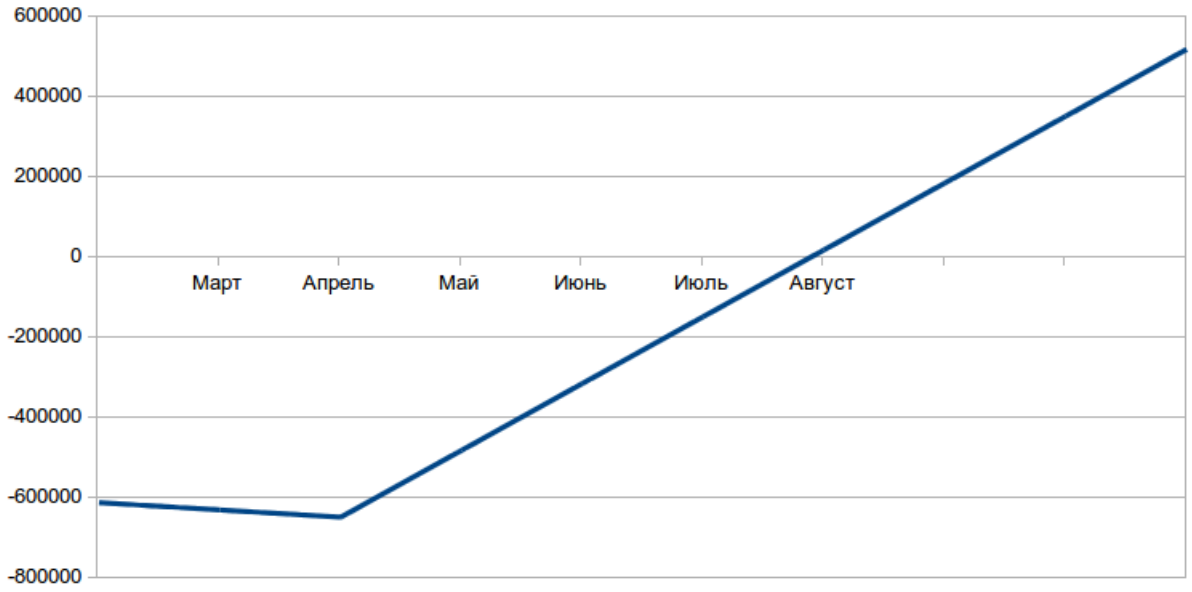


Рисунок 5.4: Структура дохода

Таблица 5.9: Заработная плата исполнителей

| № | Должность | «Чистый» оклад, руб. | Дневной оклад, руб. | Трудозатраты, чел–дни | Затраты на зарплату, руб. |
|---|---|---|---|---|---|
| 1 | Программист | 50 000 | 2722,89 | 60 | 163373,40 |

Расходы на дополнительную заработную плату учитывают все выплаты непосредственным исполнителям за время, не проработанное на производстве, но предусмотренное законодательством. Величина этих выплат составляет 20% от размера основной заработной платы:

$$C_{\text{з.доп}} = 0.2 \cdot C_{\text{з.осн}} = 0.2 \cdot 163373,40 = 32674,68(\text{руб.}) \tag{5.29}$$

### 5.3.3 Отчисления на социальные нужды

Согласно нормативным документам суммарные отчисления в пенсионный фонд, фонд социального страхования и фонды обязательного медицинского страхования составляют 30% от размеров заработной платы.

$$C_{\text{З.ОТЧ}} = 0.3 \cdot (C_{\text{З.ОСН}} + C_{\text{З.ДОП}}) = 0.3 \cdot (163373,40 + 32674,68) = 58814,42 \text{ руб.} \quad (5.30)$$

Общие расходы на сервисное обслуживание составляют:

$$C_{\text{ЗАРП}} = C_{\text{З.ОСН}} + C_{\text{З.ДОП}} + C_{\text{З.ОТЧ}} = 163373,40 + 32674,68 + 58814,42 = 254862,50 \text{ руб.} \quad (5.31)$$

## 5.4 Выводы

Результаты проведённых организационно-экономических расчетов позволили оценить структуру работ, необходимое количество исполнителей, структуру затрат проекта, срок окупаемости проекта.

1. Общие затраты труда для выполнения программного проекта составили 77 чел/дней или 616 чел/часов. Затраты на разработку ПО составляют 545871,29 рублей.

2. Исходя из временных требований к реализации проекта, была определена численность исполнителей: 2 человека. По результатам построения сетевого графика и диаграммы Гантта можно сделать вывод о том, что введение дополнительных разработчиков не принесет положительного эффекта, поскольку основные этапы работы должны выполняться последовательно.

3. Из структуры затрат проекта видно, что основной статьёй расходов является заработная плата исполнителей.

4. Стоимость продукта оценивается в 40000 рублей при объеме спроса 60 экземпляров в год. Планирование цены позволило спрогнозировать срок окупаемости проекта, который составляет 7 месяцев.

На основании вышеизложенного можно сделать вывод о целесообразности проведения работ и внедрения в производство данной разработки. Структура дохода, дохода с сервисным обслуживанием показана на рисунке 5.5.

**Себестоимость:** 545871,29 руб.
**Выручка от продаж за год:** 2400000 руб.
**Затраты на сервисное обслуживание:** 254862,50 руб.
**Прибыль от продажи каждого экземпляра ПО:** 32800,10 руб.
**Вывод:** проект обладает высокими техническими характеристиками и экономически целесообразен.

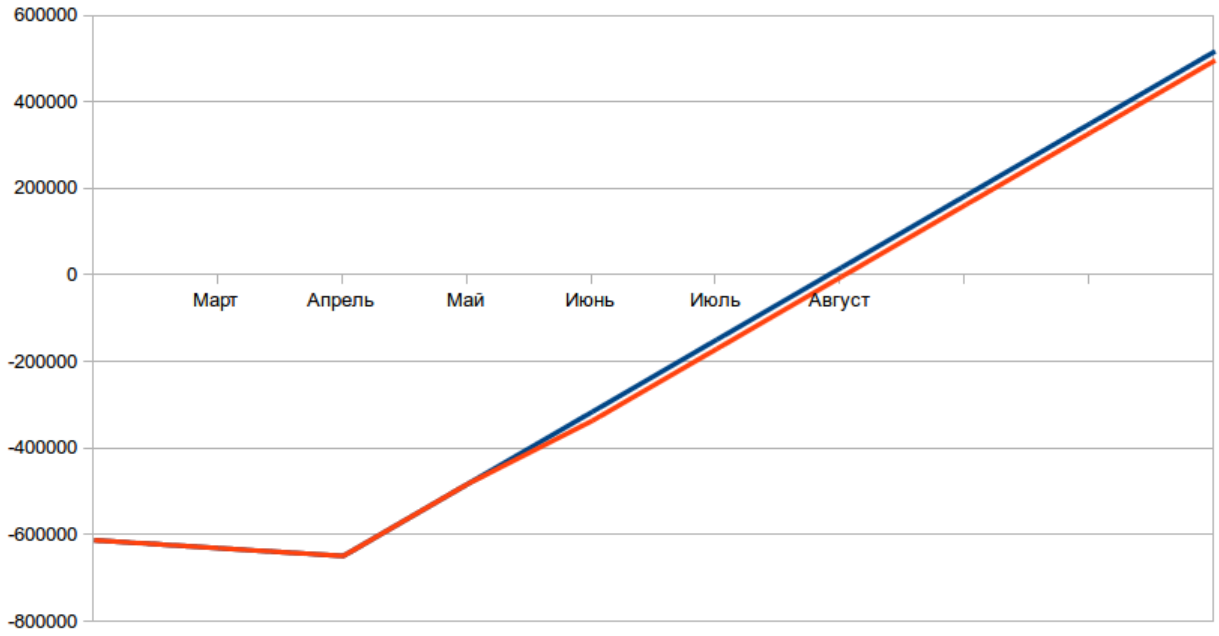


Рисунок 5.5: Структура дохода, дохода с сервисным обслуживанием

# Заключение

В ходе выполнения дипломного проекта были решены следующие задачи:

- проведён анализ угроз и средств противодействия им для систем электронного документооборота;
- осуществлён выбор показателей эффективности реализации системы электронного документооборота;
- осуществлён выбор реализации модулей системы электронного документооборота;
- разработаны программные средства защиты информации в системе электронного документооборота;
- проведён анализ нормативно-правовых актов в области информационной безопасности Российской Федерации;
- проведены организационно-экономический анализ проектной разработки, оценка структуры и показателей затрат дипломного проекта, исследование рынка.

Программное обеспечение внедрено внедрено и успешно функционирует в департаменте специальных разработок ЗАО «НПО “Эшелон“».

# Литература


1. ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения».
2. Концепция информатизации Роскосмоса. 2010. март. (дата обращения: 06.05.2014). URL: http://www.federalspace.ru/2158/.
3. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации».
4. Д.В. Быков. Диссертация кандидата технических наук на тему «Исследование процессов передачи и обработки информации в конфиденциальном хранилище электронных документов» // Волгоград. 2009.
5. Г. Башарин В. Анализ очередей в вычислительных сетях. М.: Наука, 1989. С. 334.
6. Г. Башарин В. Модели Информационно–вычислительных систем. М.: Наука, 1993. С. 69.
7. П. Башарин Г. Модели информационно–вычислительных систем: Сборник научных трудов. М.: Наука, 1994. С. 78.
8. В.М. Вишневский. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. С. 512.
9. Т.И. Булдакова Б.В. Глазунов Н.С. Ляпина. Оценка эффективности защиты систем электронного документооборота // Доклады ТУСУРа, № 1 (25), часть 2. 2012.
10. Елисеев Н.И. Модель угроз безопасности информации при её обработке в системе защищённого электронного документооборота // Известия ЮФУ. Технические науки. 2012.
11. В.Е. Карташов О.В. Гудков. Обзор инструментария систем контроля версий исходных текстов в контексте электронного документооборота // Сборник трудов конференции «Безопасные информационные технологии». 2013.