Краснодарское высшее военное училище имени генерала армии С.М.Штеменко

PKI-ФОРУМ РОССИЯ 2016
(14-16 сентября 2016 года, г. Санкт-Петербург)

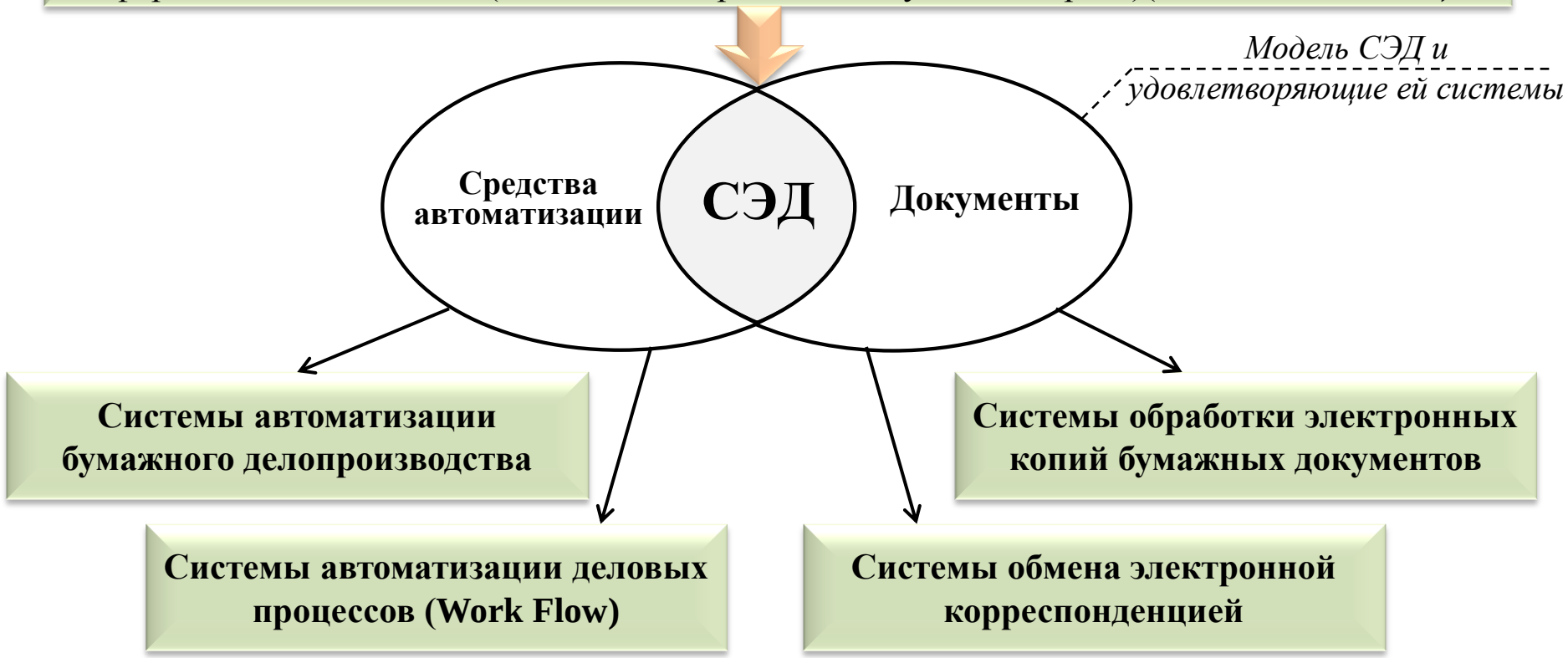
АНАЛИЗ И СИНТЕЗ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Авторы:
к.т.н., доцент Елисеев Николай Иванович
д.т.н., профессор Финько Олег Анатольевич

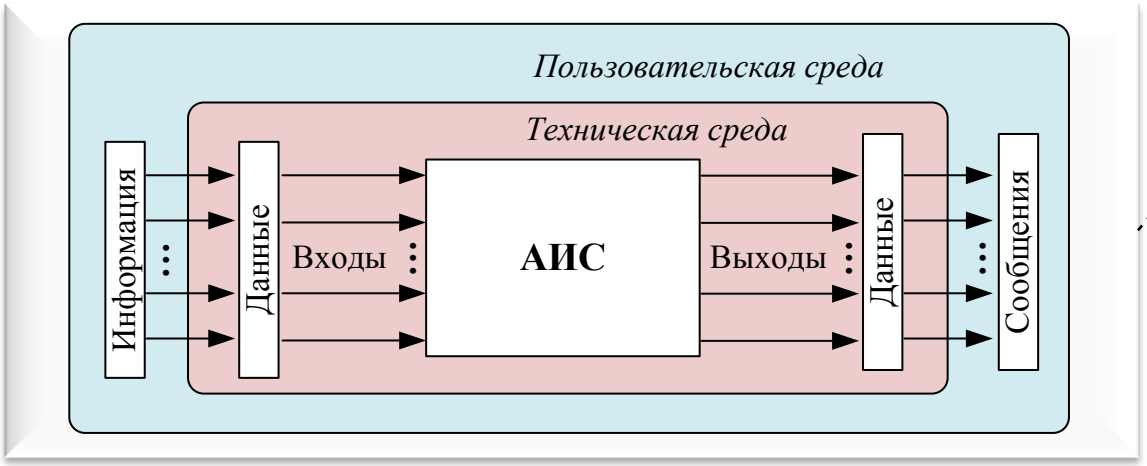
Текущее понимание определения «СЭД»

Система электронного документооборота – информационная система, предназначенная для управления всеми видами документов, включая проекты документов (Приказ Минкомсвязи России № 221).

Электронный документооборот – документооборот с использованием автоматизированной информационной системы (системы электронного документооборота)(ГОСТ Р 7.0.8-2013).

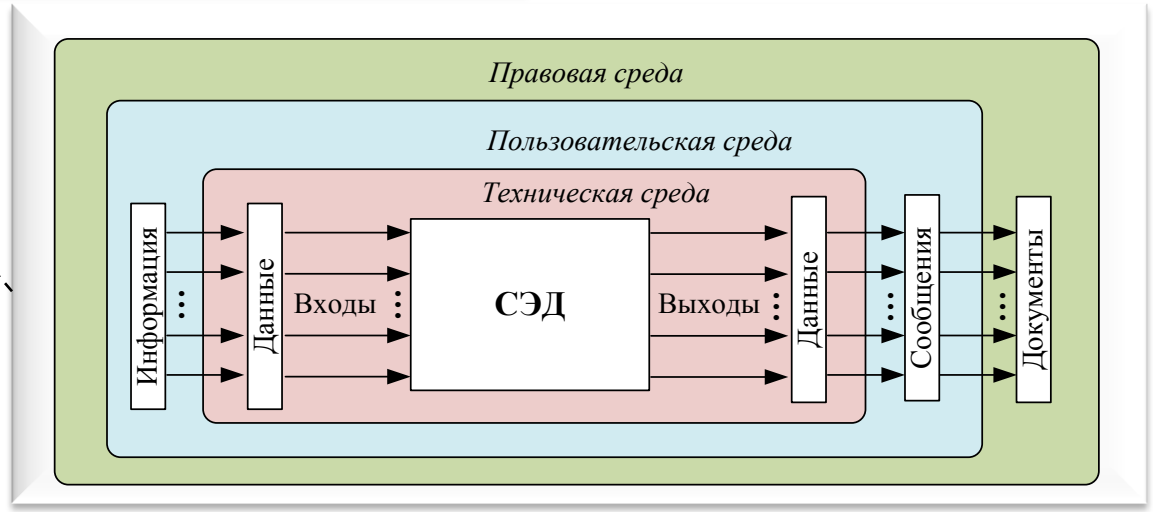


Результат функционирования АИС – электронное сообщение
Результат функционирования СЭД – электронное сообщение, обладающее сущностью документа, т.е. юридической значимостью



АИС на примере модели «черного» ящика

СЭД на примере модели «черного» ящика



Выводы. Каждая СЭД является АИС, но не каждая АИС, обладает сущностью СЭД. Поэтому следует разделять понятия «АИС с признаками СЭД» и «СЭД».

Целевая функция СЭД – обеспечение юридической значимости ЭлД на всех этапах их жизненного цикла

Функциональные требования к СЭД

Обеспечение информационной безопасности на всех этапах жизненного цикла электронных документов

Обеспечение юридической значимости электронных документов на всех этапах их жизненного цикла, в том числе при длительных сроках существования

Обеспечение унифицированности СЭД различных субъектов информационного взаимодействия

Обеспечение возможности обработки электронных документов различной степени секретности

Оперативность и надежность обработки больших объемов документированной информации

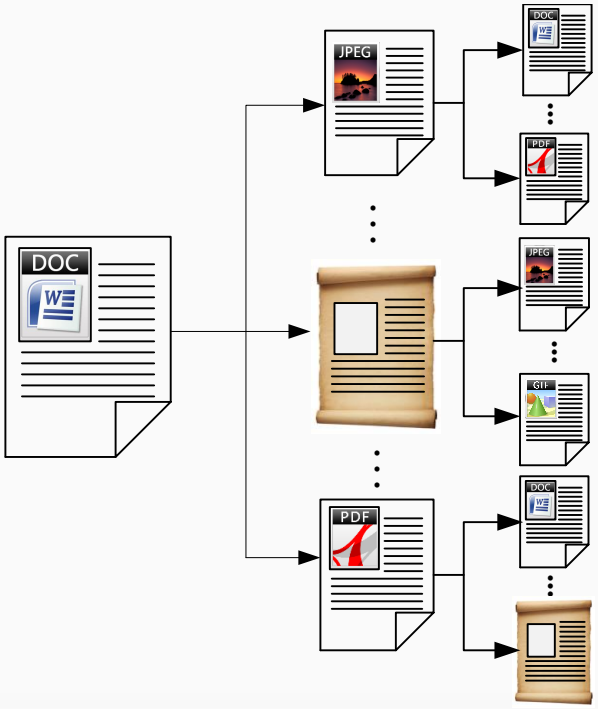
Обеспечение информационной безопасности на всех этапах жизненного цикла электронных документов

ПРОБЛЕМА

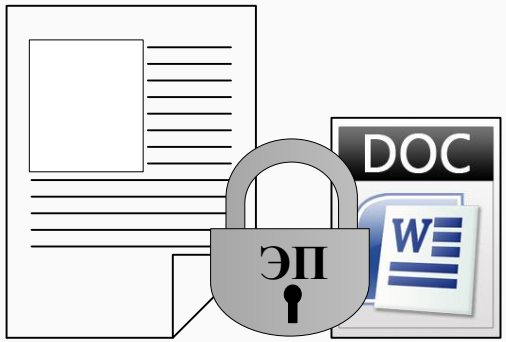
Проблема межформатных преобразований электронных документов

Пояснение к проблеме

Технические требования к СЭД



Юридические требования к СЭД



СУЩЕСТВУЮЩЕЕ РЕШЕНИЕ: новый формат представления одного и того же документа требует формирования новой электронной подписи.

СЛЕДСТВИЯ:

- **повышение доступности ЭП для потенциального криптоаналитика;**
- **возникновение дополнительных уязвимостей в подсистеме защиты на этапе переподписания электронного документа.**

Обеспечение информационной безопасности на всех этапах жизненного цикла электронных документов

ПРОБЛЕМА

Проблема взаимодействия электронного и бумажного документооборота (проблема «гибридного» документооборота)

Пояснение к проблеме

Документ на бумажном носителе –
необходимость документооборота МО РФ

Одновременно используются две юридически равносильные, но технически не равнозначные технологии защиты документов (собственноручная и ЭП).

Следствие: общий уровень защищенности системы не может превышать уровня, обеспечиваемого наиболее слабым механизмом защиты – собственноручной подписью.

Обеспечение информационной безопасности на всех этапах жизненного цикла электронных документов

ПРОБЛЕМА

Существующий механизм электронной подписи не позволяет обеспечить действенный контроль всех объектов и процессов, участвующих в обеспечении информационной безопасности при создании электронного документа

СЛЕДСТВИЕ

- **пользователь несет юридическую ответственность за некоторые объекты и процессы контроль которых ему не доступен.**

9

Обеспечение юридической значимости электронных документов на всех этапах их жизненного цикла, в том числе при длительных сроках существования

ПРОБЛЕМЫ

Утрата криптографической стойкости ЭП со временем

Необходимость преобразования форматов представления одних и тех же данных со временем

СЛЕДСТВИЕ

- **лавинообразный рост нагрузки на подсистему ЭП;**
- **возникновение уязвимостей в подсистеме защиты;**

Обеспечение унифицированности СЭД различных субъектов информационного взаимодействия

ПРОБЛЕМЫ

Один и тот же документ, представленный в различных форматах и не различимый в рамках 149-ФЗ *(… сведения (сообщения, данные) не зависимо от формы их представления*) в СЭД это различные документы

Обеспечение возможности обработки электронных документов различной степени секретности

ПРОБЛЕМА

Оперативность и надежность обработки больших объемов документированной информации

ПРОБЛЕМЫ

Избыточная техническая и организационная нагрузка на СЭД, не позволяет достигнуть потенциально возможных показателей оперативности и надежности системы

Решение 1.
Обеспечение контроля «целостности СЭД»*

Под **целостностью СЭД понимается состояние системы, при котором обеспечивается **техническая** и **юридическая пригодность** всех сервисов, участвующих в обеспечении информационной безопасности при создании электронного документа*

Структура перспективной СЭД МО РФ

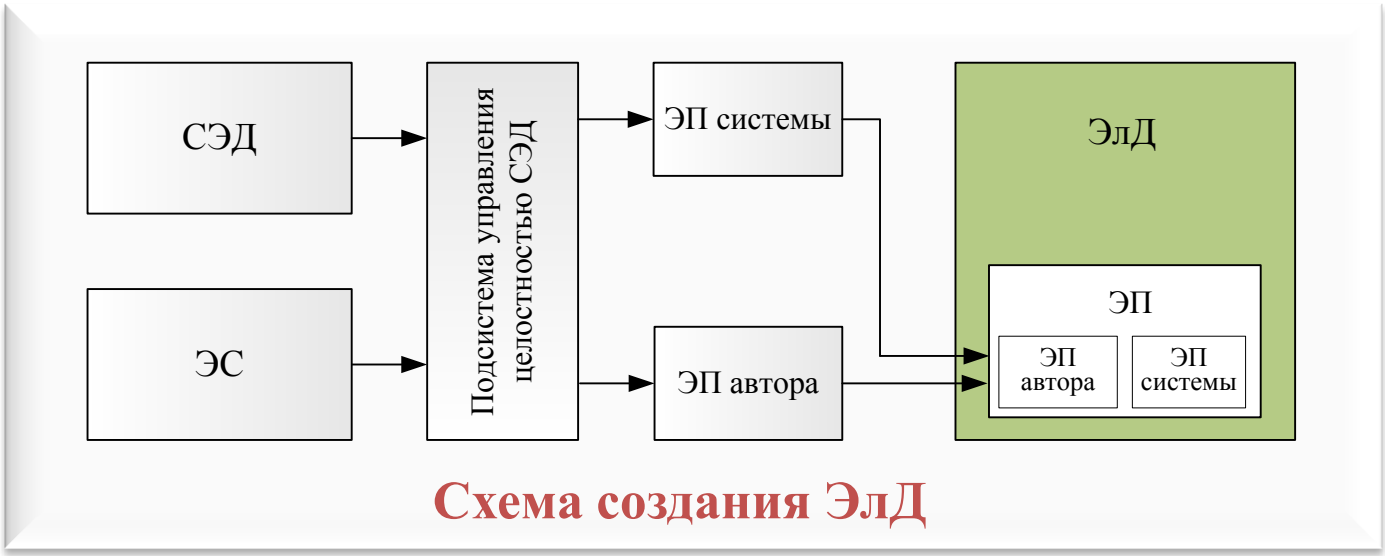


Схема создания ЭлД

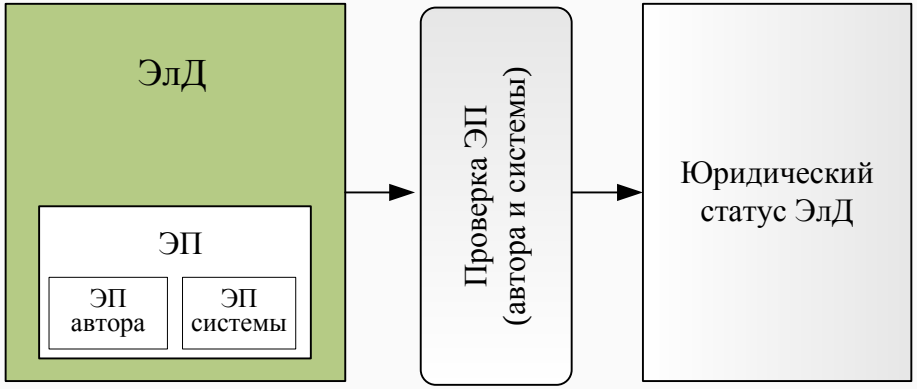


Схема проверки ЭлД

Целостность СЭД величина обратно пропорциональная удобству и стоимости. В этом случае должны учитываться риски, характерные для той или иной области применения СЭД. Как следствие целесообразно ввести уровни целостности СЭД, аналогично классам защищенности АИС.

Решение 2.
Унификация форматов представления электронных документов

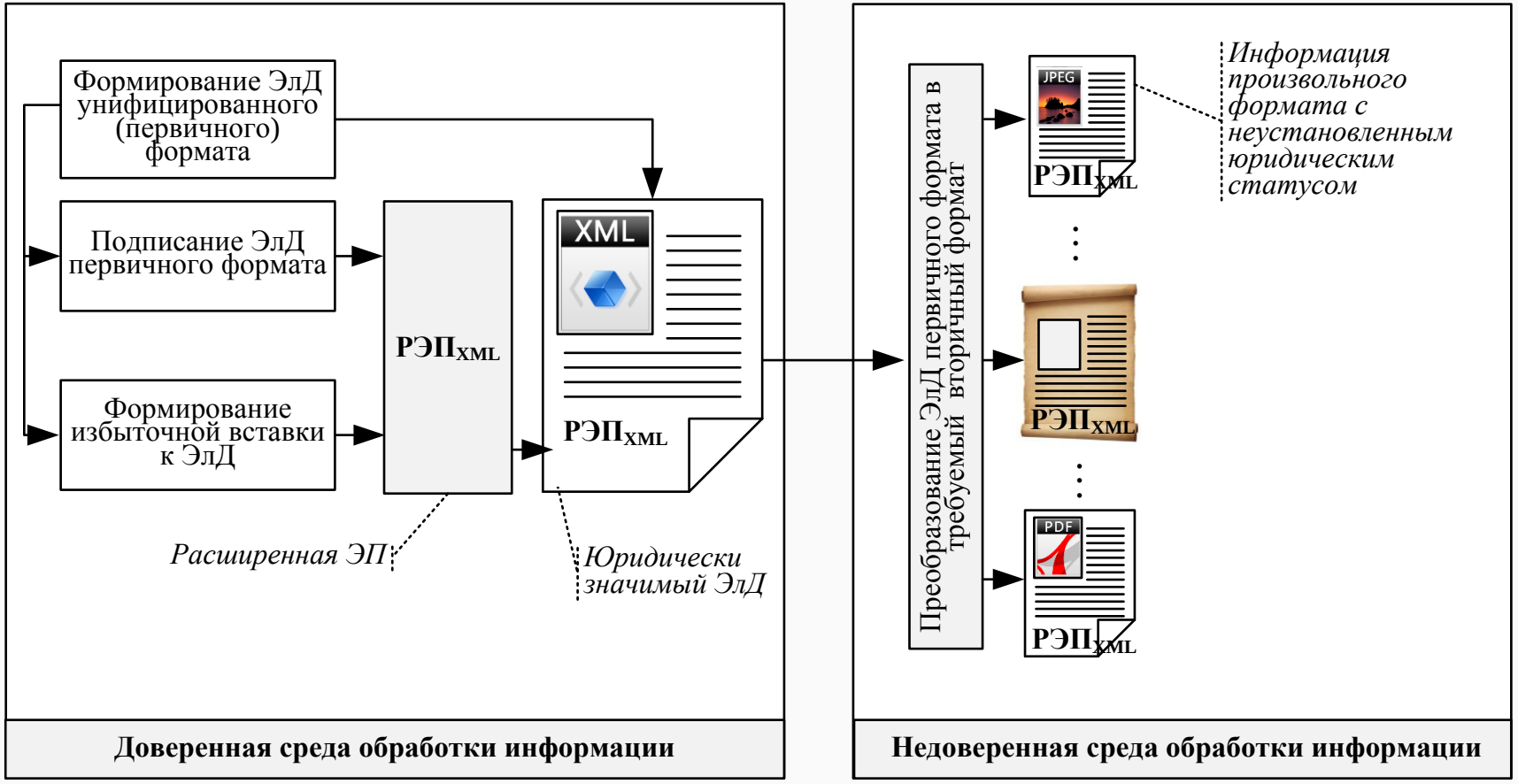


Схема обработки исходящих ЭлД

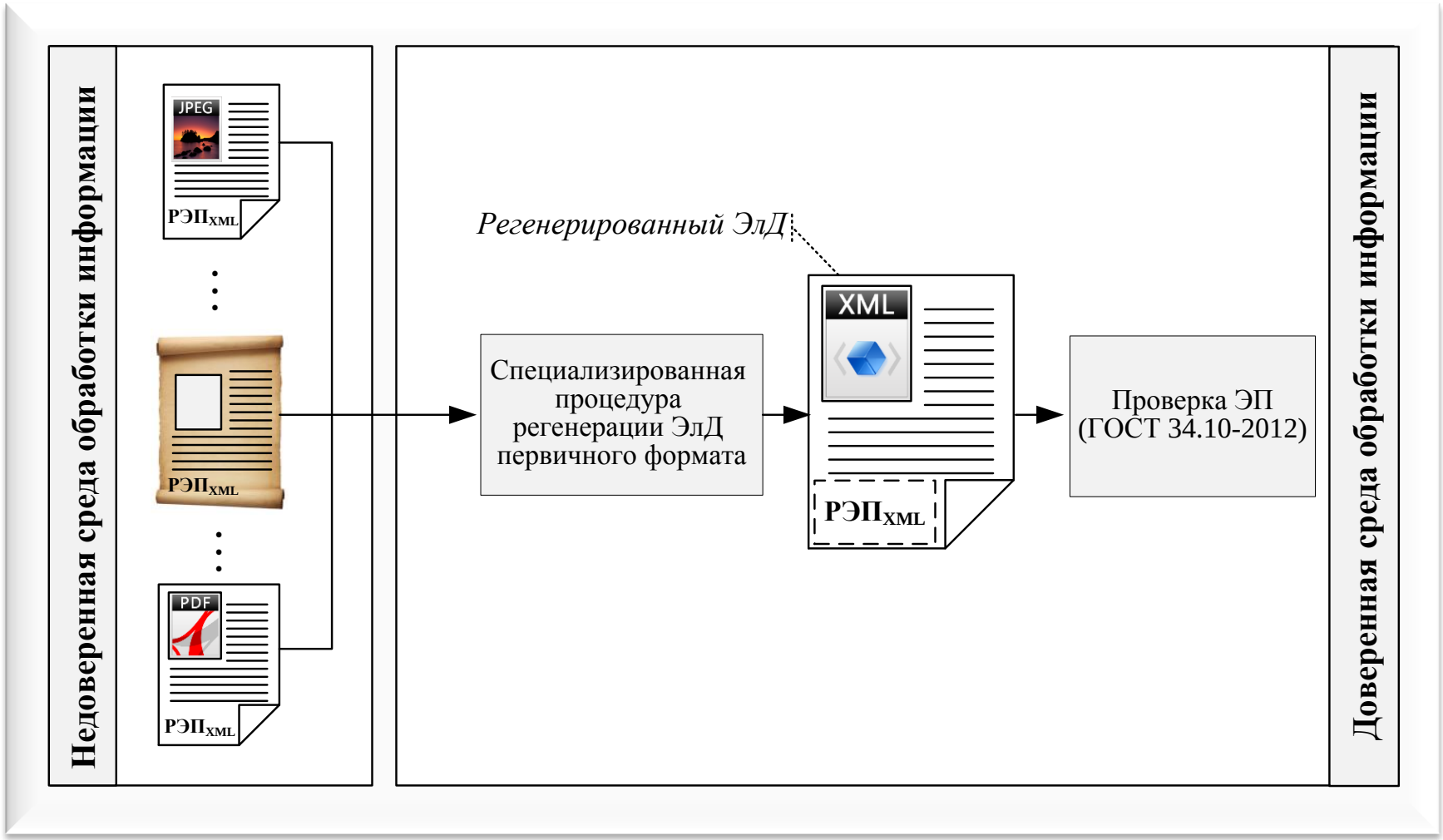


Схема обработки входящих ЭлД

Особенности обработки графической информации

Схема обработки исходящих ЭлД

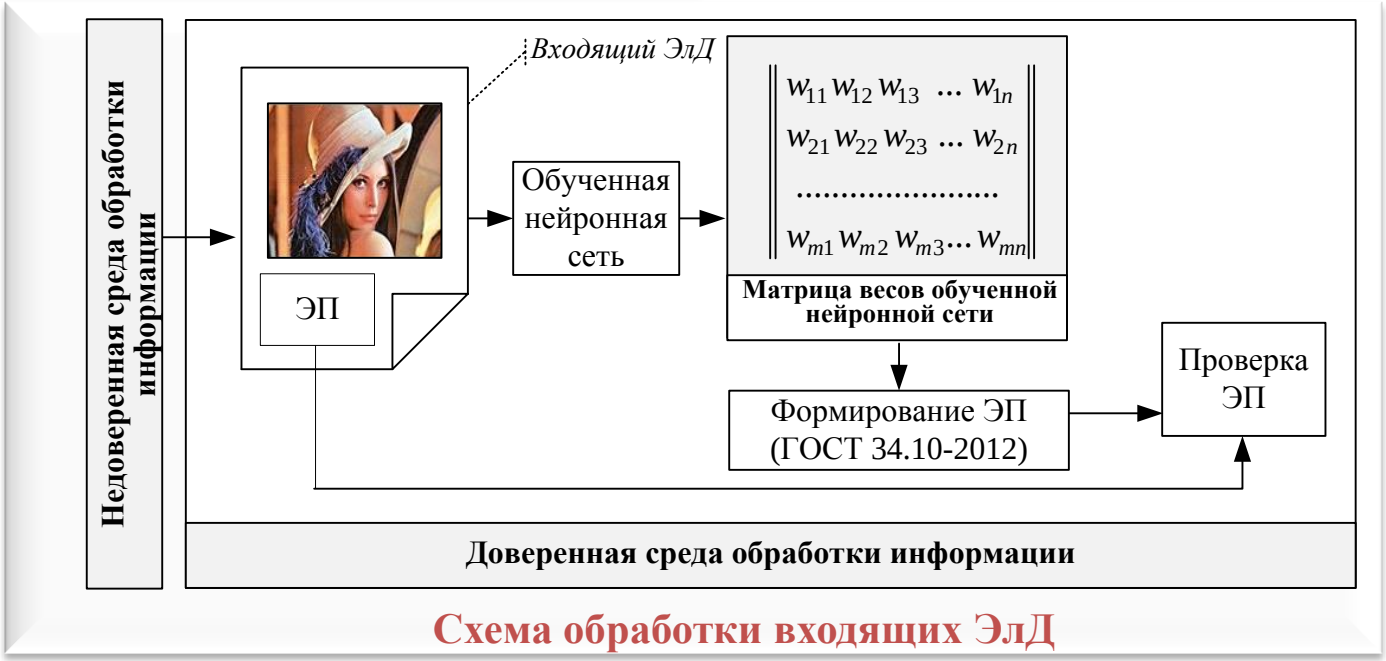


Схема обработки входящих ЭлД

Подсистема проверки целостности электронных документов, полученных из недоверенной среды

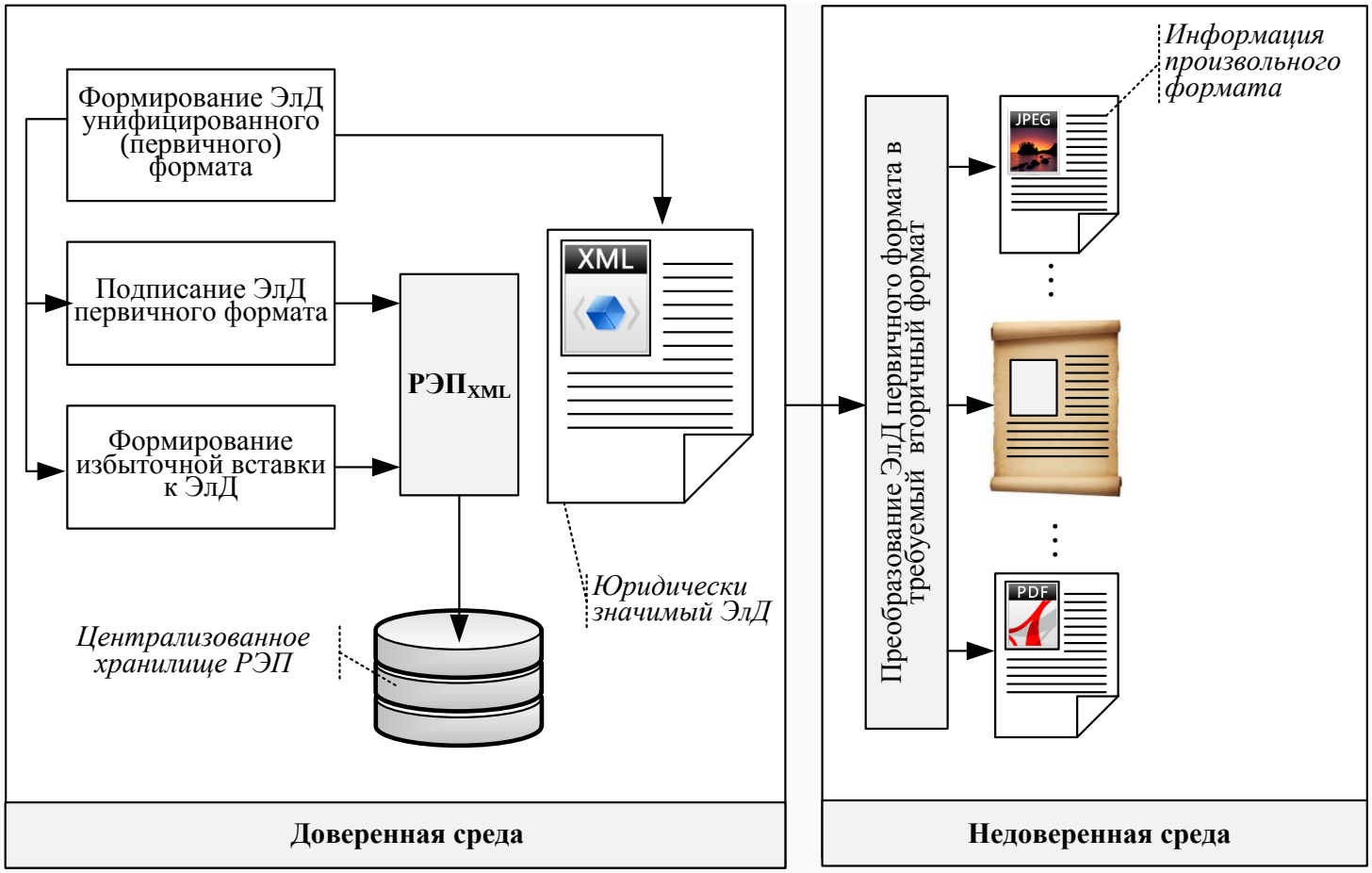


Схема обработки исходящих ЭлД

Схема обработки входящих ЭлД

Достоинства предложенных решений

Предложены не противоречащие законодательству решения, обеспечивающие, при некоторых условиях, юридическую значимость ЭлД, представленных во вторичных форматах.

Положительный эффект:

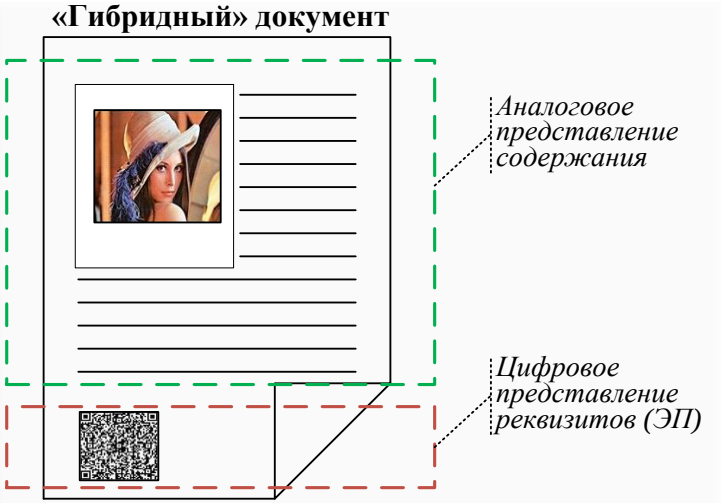
•отсутствие необходимости повторного подписания ЭлД, представленного в новом формате, как следствие снижение нагрузки на подсистему ЭП;

•наделение ЭлД новым свойством помехоустойчивости;

•возможность юридически значимой проверки ЭлД, полученных в произвольном формате на произвольном носителе, в том числе при отсутствии ЭП в составе сообщения;

•обеспечение непрерывности функции защиты оригинальной ЭП в условиях межформатных преобразований, **в том числе при выводе ЭлД на бумажный носитель! Это может позволить от части решить проблему «гибридного» документооборота.**

Синтез системы «гибридного» документооборота



Структура «гибридного» документа

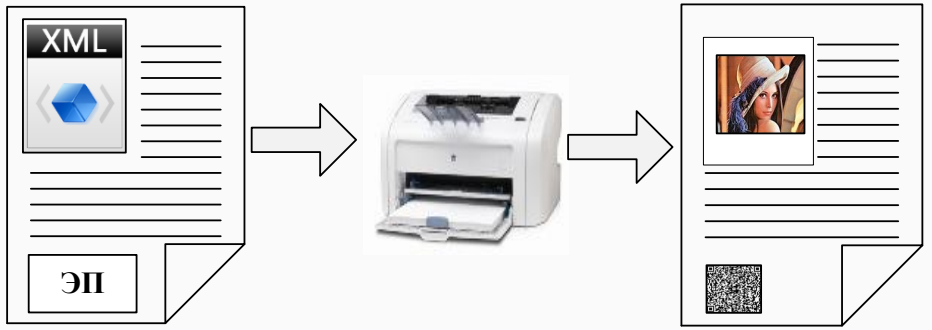


Схема создания «гибридного» документа

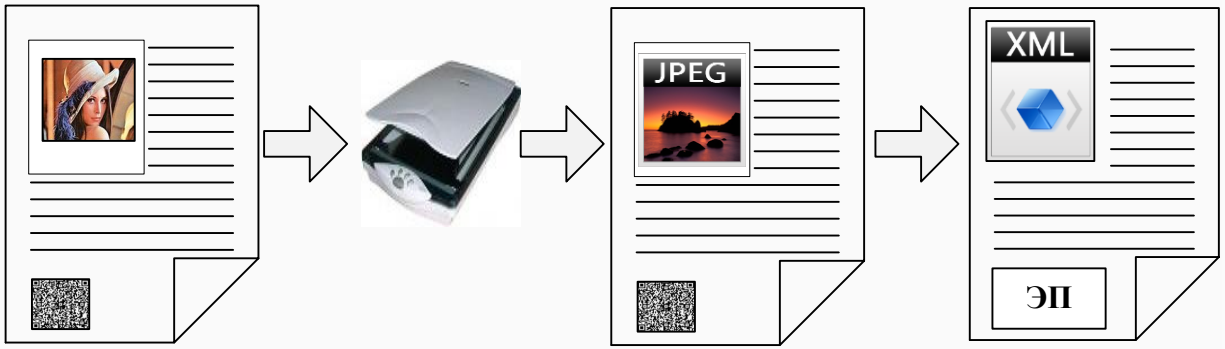


Схема проверки «гибридного» документа

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2591655

СПОСОБ КОНТРОЛЯ ЦЕЛОСТНОСТИ И ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ТЕКСТОВОГО ФОРМАТА, ПРЕДСТАВЛЕННЫХ НА ТВЕРДЫХ НОСИТЕЛЯХ ИНФОРМАЦИИ

Патентообладатель(ли): *федеральное государственное казенное военное образовательное учреждение высшего образования "Краснодарское высшее военное училище имени генерала армии С.М.Штеменко" Министерства обороны Российской Федерации (Краснодарское высшее военное училище) (RU)*

Автор(ы): *см. на обороте*

Заявка № 2015111578

Приоритет изобретения 30 марта 2015 г.

Зарегистрировано в Государственном реестре изобретений Российской Федерации *22 июня 2016 г.*

Срок действия патента истекает 30 марта 2035 г.

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

По решению экспертов ФИПС изобретение рекомендовано для включения в базу «Перспективных изобретений» и рассмотрения его в рамках формирования перечня «100 лучших изобретений России»

Решение 3.
«Ядерная» структура СЭД

Проблема хранения электронных документов:

Требования нормативных документов по обеспечению длительного хранения ЭлД

Утрата криптографических свойств ЭП с течением времени

ПРОТИВОРЕЧИЕ

Двухядерная архитектура подсистемы хранения СЭД

Изолированное (порождающее) ядро

Общедоступное (порождаемое) ядро

Функциональные характеристики подсистемы хранения ЭлД

Основные характеристики подсистемы долговременного существования ЭлД:

- высокозащищенная среда ограниченного доступа;
- ЭлД существуют в одном или не многочисленном количестве форматов, которые являются порождающими для всего спектра форматов, используемых в подсистеме кратковременного существования ЭлД;
- форматы представления ЭлД долговременного ядра СЭД изначально ориентированы на удобство технической системы;
- ЭП автора существует только в защищенном ядре и не доступна для пользователей среды кратковременного существования ЭлД;
- ЭП документов долговременного существования являются порождающими для ЭП документов кратковременного существования.

Основные характеристики подсистемы кратковременного существования ЭлД:

- ЭлД хранятся и используются в различных технически и физически удобных форматах представления данных;
- более низкие требования к криптографической стойкости ЭП, определяемые не значительными сроками существования ЭлД;
- отсутствие необходимости длительное время поддерживать ЭП в актуальном состоянии (сертификаты ЭП, сертификаты средств ЭП и т.д.).

Достоинства двухядерной архитектуры подсистемы хранения ЭлД

Предложенные решения позволяют обеспечить гибкость в выборе архитектуры СЭД с учетом решаемых задач.

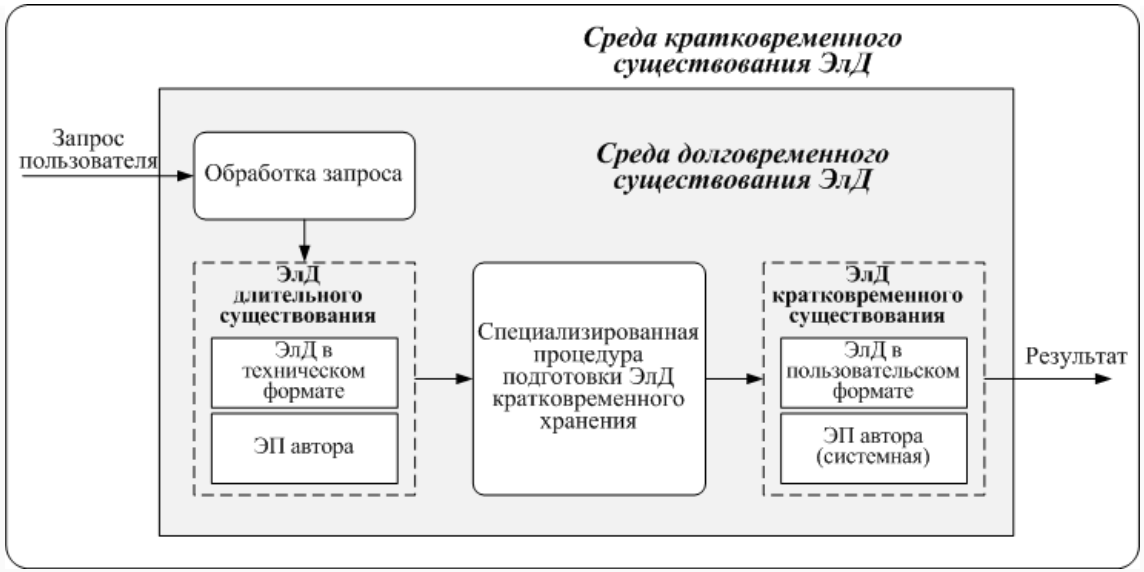
Например, если для ЭлД в СЭД изначально предполагается не значительный срок жизненного цикла, то может использоваться традиционная архитектура СЭД. В другом случае, СЭД могут строиться на основе гибридной архитектуры: ядро, реализующее традиционные функции СЭД (для документов определенного класса) и защищенное ядро, обеспечивающее более стабильные параметры ЭлД в течении длительного срока.

Варианты генерации ЭлД кратковременного существования:

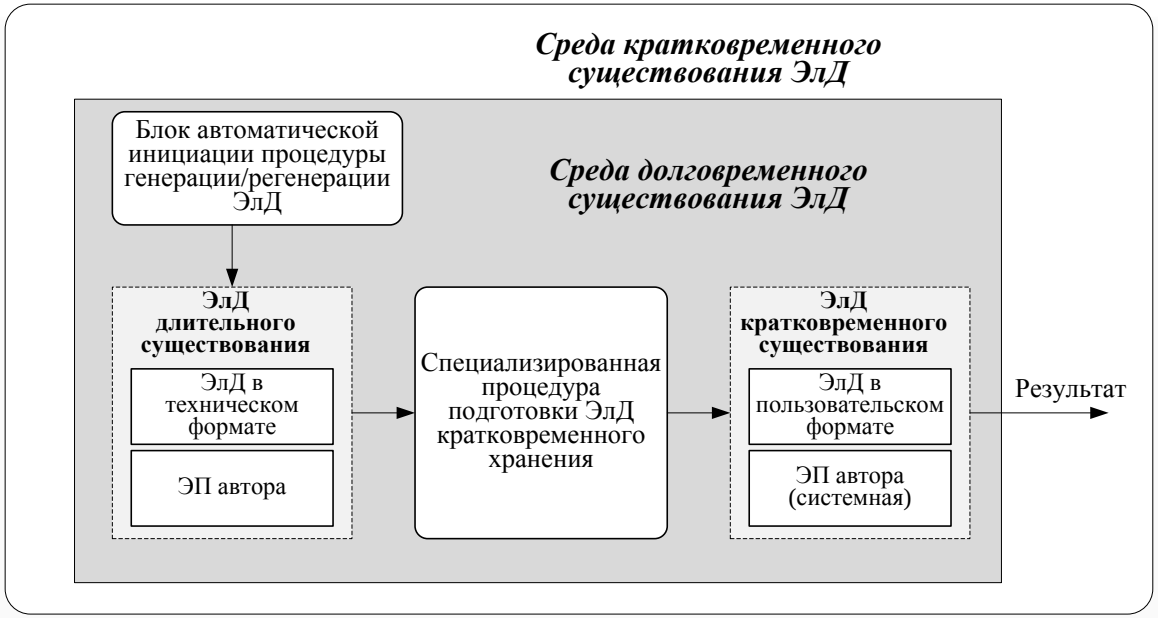
1. По запросу пользователя. В этом случае ЭлД в общедоступном ядре нет. Он генерируется только по запросу пользователя и существует требуемый (кратковременный) срок. При необходимости запрос может быть повторен.

2. Автоматическая генерация. Генерируется долговременным ядром автоматически однократно (однократное превентивное формирование) с ограниченным сроком хранения, кратностью использования или мажоритарными принципами. После чего ЭлД перестает существовать. В этом случае, сроки превентивного создания, хранения и другие параметры объектов и процессов должны определяться статистически, или с использованием оптимизационных методов (например, соотношение цена/срок хранения).

3. Периодическая регенерация (обновление). ЭлД генерируется долговременным ядром на короткий срок на новых ключах в течении необходимого срока поддержания его актуальности (например, в течении 10 лет ЭлД порождается на новых ключах каждый квартал).

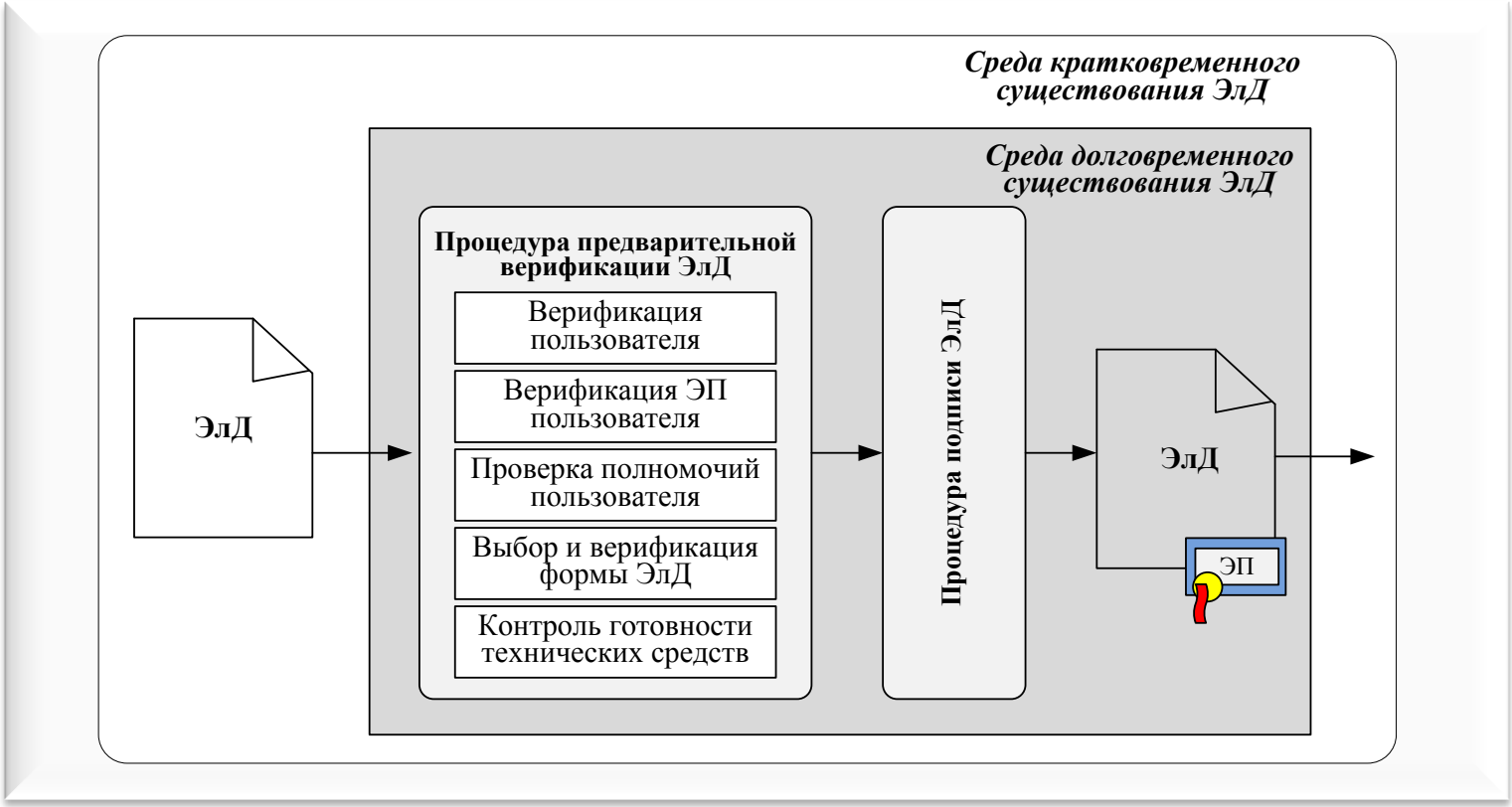


Вариант схемы генерации ЭлД «по запросу пользователя»

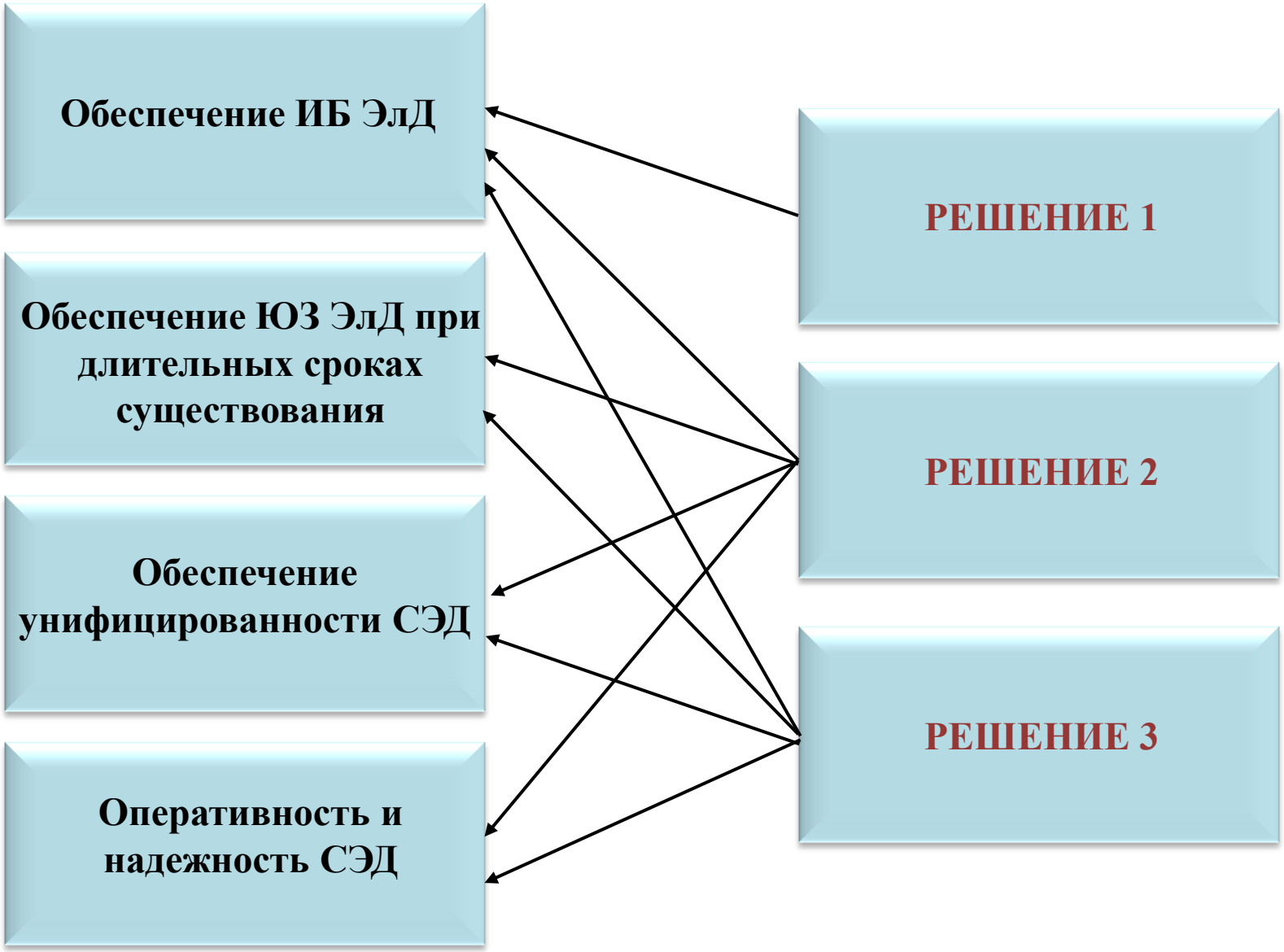


Вариант схемы автоматической генерации/регенерации ЭлД

Схема процедуры включения ЭлД в долговременное ядро



Предлагаемые решения позволяют за счет управления темпоральными свойствами ключевого пространства СЭД более эффективно перераспределять ресурсы системы с учетом необходимых и достаточных соотношений времени хранения и криптографической стойкости. Кроме того снижается избыточная нагрузка на оперативный контур СЭД ввиду отсутствия необходимости хранения и поддержания всех ЭлД в актуальном состоянии. При необходимости ЭлД может быть вновь порожден с актуальными параметрами и необходимыми сроками действия.


Обеспечение ИБ ЭлД
Обеспечение ЮЗ ЭлД при длительных сроках существования
Обеспечение унифицированности СЭД
Оперативность и надежность СЭД
РЕШЕНИЕ 1
РЕШЕНИЕ 2
РЕШЕНИЕ 3

СПАСИБО ЗА ВНИМАНИЕ!

Контакты:
Елисеев Николай Иванович,
n.i.eliseev@yandex.ru

Финько Олег Анатольевич,
ofinko@yandex.ru
www.финько.рф