Содержание:

Введение .............................................................................................. 1

1. Электронный документооборот в экономике:

1.1 Автоматизация учета в торговле.................................................. 2
1.2 Автоматизация фондовой торговли в России............................. 3

2. Системы электронного документооборота:

2.1 Документооборот в мире безбумажных технологий................. 5
2.2 Делопроизводство и документооборот в управлении предприятием................................................................................. 5
2.3 Системы управления электронным документооборотом.......... 8
2.4 Корпоративный электронный архив............................................11
2.5 Информационно - поисковые технологии для электронного делопроизводства...........................................................................13

3. Защита информации:

3.1 Безопасность электронной почты..................................................16
3.2 Защита электронного обмена данными.........................................17
3.3 Семейство продуктов PALINDROME...........................................17
3.4 Сетевое резервное копирование.....................................................19
3.5 Зеркальные серверы........................................................................ 24

4. Электронная цифровая подпись в электронном документообороте:

4.1 Что такое ЭЦП?................................................................................25
4.2 Шифрование.....................................................................................26
4.3 Управление ключевой системой.....................................................27
4.4 Пакет документов.............................................................................28
4.5 Центр удостоверения открытых ключей........................................28

5.Приложение........................................................................................31

6. Литература:

6.1 Список выявленной литературы.....................................................35
6.2 Список использованной литературы..............................................37

Введение

Основной целью данной работы является раскрытие понятия "системы электронного документооборота". Основой этой системы является документ. Документ - определенным образом упорядоченная информация. В свою очередь, система - это совокупность элементов, упорядоченно взаимодействующих друг с другом и с элементами подсистемы, предназначенная для выполнения определенных функций и обладающая определенными свойствами, сводящимся к свойствам элементов, точнее к их сумме. Этими элементами в системе электронного документооборота и являются документы.
Трудно представить нашу жизнь без документов: гражданина- без паспорта, водителя - без водительских прав, туриста - без туристической визы, студента - без студенческого билета и зачетной книжки и т.д. Особенно это затрагивает практически все сферы экономики: торговлю, управление, банковскую деятельность. Ни одна фирма, компания, корпорация не может обойтись без документа и, следовательно, без документооборота. Оборот документов является обязательной частью деятельности любой из выше перечисленных сфер экономики и организаций.
С развитием информационных технологий для документооборота открылись огромные возможности. С появлением и развитием глобальной сети Интернет и его важным атрибутом - электронной почтой, проблема расстояния перестала быть проблемой. По электронной почте электронный документ приходит к получателю в считанные минуты. Но, с устранением одной проблемы, появилась другая - защита информации, которую содержит электронный документ. Безопасность информации особенно важна в наше время, поэтому настоящая работа содержит некоторые возможности ее обеспечения.
Электронный документ, в отличие от обычного (бумажного), невозможно закрепить печатью или подписью. Поэтому в нем их функции выполняет электронная цифровая подпись (ЭЦП). ЭЦП также рассматривается в данной работе.

1.1 Автоматизация учета в торговле

Так как основой для торговой фирмы служит движение товаров и денег, автоматизация торговой деятельности предусматривает многовариантность организации закупок и торговых схем, гибкую и прозрачную схему складского и секционного учета, многокассовый, многобанковский учет денежных средств и контроль взаиморасчетов с поставщиками и покупателями.
В основу ряда комплексов положены схемы документооборота и основные принципы, аналогичные описанным выше. Например, в системе "Эйс" главными являются:
1. комплексный охват деятельности фирмы;
2. отслеживание движения товара на протяжении всего пути с момента его закупки до реализации по всем промежуточным операциям;
3. учет товаров в разрезе партий в учетных ценах;
4. получение текущей информации по состоянию складов, магазинов и прочих подразделений фирмы, а также взаимоотношение с покупателями и поставщиками;
5. организация различных видов торговой деятельности: опт, розница, консигнация, комиссия, и др.;
6. проведение маркетинговых исследований и финансового анализа по результатам деятельности фирмы за любой период времени;
7. ведение независимого учета по нескольким фирмам с возможностью объединения отчетов об их деятельности и автоматизации корпоративной структуры;
8. ведение многовалютного учета;
9. представление данных в российском или международном стандарте;
10. возможность выборки необходимой информации по сложному критерию и представление ее в любом удобном виде: в виде печатной формы, таблицы, экспорта в файл, передачи по электронной почте;
11. максимальная гибкость в настройке комплекса и в распределении прав доступа;
12. работа в сетях с большими объемами данных; распределенный характер системы;
13. максимальная открытость комплекса, в том числе возможность экспорта в популярные программные среды;
14. легкость в освоении и адаптируемость к задачам клиента;
15. возможность стыковки и интеграции с другими программными продуктами.
Рассмотрим более подробно управление складской деятельностью торговой фирмы (на складах и в торговых точках). При этом учитываются следующие факторы:
\* товар может иметь несколько независимых единиц измерения, например количество товара, количество упаковок, вес, стоимость;
\* товар может оцениваться в различных валютах;
\* товар может иметь несколько цен в зависимости от объемов и группы покупателей и поставщиков, а также состояния товара в процессе его хранения и реализуемости на рынке;
\* товар может иметь различный статус, например статус резервирования.
Особое значение имеет взаимосвязь с подсистемами торговых секций (напрямую или через внутренний склад последных), бухгалтерий и представлением аналитической и управленческой отчетности. В частности, анализ функционирования склада предусматривает получение полной картины о состоянии складов, магазинов и прочих подразделений фирмы, о закупках и продажах с формированием любых отчетных документов.

1.2 Автоматизация фондовой торговли в России

Информационные системы предназначены для повышения прозрачности рынка наиболее добротных ценных бумаг и увеличения оборота средств.
Для внебиржевой торговли ценными бумагами инвестиционными институтами, в том числе банками, создаются специализированные учреждения или подразделения, в том числе так называемые фондовые магазины. Для автоматизации их работы разрабатываются специальные системы, одна из которых - "Фондовый магазин" - представлена на рис. 3 (приложение).
Система предназначена для переуступки прав собственности по ценным бумагам, выпущенным в безбланковой форме. Она взаимодействует с системой учета прав собственности, обеспечивая гарантированную поставку безналичных ценных бумаг. Основными особенностями являются:
\* прием заявок на продажу и покупку ценных бумаг;
\* сведение заявок в режиме биржи и в режиме прямого указания;
\* гарантированное исполнение заключенных сделок за счет блокировки выставленных на продажу ценных бумаг в депозитариях и обязательного депонирования сумм, обеспечивающих покупку заявленного количества ценных бумаг;
\* проведение необходимых денежных расчетов, взимание налогов на доход от продажи ценных бумаг и налогов на операции с ценными бумагами;
\* учет движения денежных средств;
\* организация обмена с неограниченным количеством депозитариев.
С каждым днем электронный документооборот нарастает, особенно в связи с развитием Интернет - торговли на фондовом рынке. Безопасность торговли ценными бумагами через Сеть обеспечивается принципиально иными способами, чем при проведении торгов с использованием традиционных удаленных терминалов. Несанкционированный доступ к терминалам предотвращается путем их изоляции от внешнего мира: они устанавливаются в специальном помещении с особым режимом контроля и подключаются к торговой системе биржи с помощью выделенных каналов связи. Такая система достаточно надежна, но дорога, и потому круг ее пользователей существенно ограничен.
Интернет - трейдинг (онлайновая торговля ценными бумагами) в России начал активно развиваться после создания на Московской межбанковской валютной бирже универсального двунаправленного аппаратно-программного интерфейса (шлюза), позволяющего подключать к торговой системе биржи брокерские системы сбора клиентских заявок (приказов на покупку/продажу ценных бумаг), которые заполняются самими клиентами в электронной форме и передаются по компьютерным сетям.
Компьютерная обработка электронных заявок выполняется быстрее, чем ручная обработка бумажных заявок. Электронные приказы проходят входной контроль с помощью специального программного обеспечения. Один из этапов такого контроля - проверка авторства и подлинности заявки. Необходимо убедиться, что: а) заявка не была искажена в процессе доставки по компьютерной сети от отправителя к получателю; б) заявку направило именно то физическое/юридическое лицо, от чьего имени она пришла. Технология проверки должна быть настолько убедительной, чтобы в случае судебного разбирательства судьи согласились использовать ее результаты для вынесения решения по спорному вопросу. Именно для этих целей применяется электронно-цифровая подпись.

2.1 Документооборот в мире безбумажных технологий

Увеличение информационных потоков в науке, бизнесе, производстве, культуре требует адекватной реакции со стороны информационных технологий. Для общества обременительно расходование огромного количества бумаги, да и информация, поступающая на таких носителях, менее динамична, чем электронная.
Концепция безбумажной технологии имеет за плечами не одно десятилетие. В это же время сегодня можно говорить лишь о частичной реализации этой идеи. Здесь ряд причин:
1. Можно указать на психологический аспект проблемы. Получение информации в электронном виде требует привычки;
2. Безбумажные технологии требуют основательной технической поддержки: соответствующей производительной вычислительной техники, высокой пропускной способности коммуникационных линий, технологичности алгоритмов;
3. Безбумажные технологии требуют основательной юридической поддержки (например, в России на данный момент ни одна налоговая инспекция не примет отчет только в электронном виде, ни один суд не примет договор, заверенный электронной подписью и т.п.).
Процесс управления предприятием в условиях рыночной экономики требует интенсификации и четкой организации всего предприятия, вплоть до каждого сотрудника. Таким образом, при наличии регламентации деятельности, прежде всего в отношении делопроизводства, информационные технологии как катализатор дальнейшего прогресса общества призваны обеспечить доступный и эффективный инструмент автоматизации на основе безбумажного делопроизводства и документооборота.

2.2 Делопроизводство и документооборот в управлении предприятием

Для эффективного менеджмента в деятельности любого предприятия информационные потоки должны представлять собой четко отслеживаемый и управляемые процесс. Типовым информационным объектом, фиксирующим и регламентирующим деятельность на предприятии, является документ. Деятельность по организации прохождения документов внутри предприятия принято называть делопроизводством данной конкретной организации. В основе делопроизводства лежит фундаментальное понятие структуры информационного обмена - документопоток.
Для любой организации можно выделить три основных потока документов: входящие, внутренние и исходящие, которые и определяют документопотоки.
Функции ведения делопроизводства состоят из обработки входящих документов, пересылки их внутри фирмы, отправки исходящих документов, учета, регистрации, контроля за исполнением, формирования дел, организации хранения и т.д.
В советские времена делопроизводство регламентировалось Единой государственной системой документационного обеспечения управления (ЕГСДОУ). Созданная схема хорошо структурирована и до сегодняшнего дня хорошо поддается автоматизации. Указанный стандарт регламентирует принципы работы с документами. В то же время сегодня желательна детальная регламентация работы по исполнителям (выполняемым или ролям), доведенная до регламентации в виде положений о подразделениях и должностных инструкциях специалистов.
Форма
документа
Документопоток

входящей информации
внутренних документов
исходящей
информации
Электрон - ные документы
Сообщения электронной почты

Факсимильная информация
Сообщения в корпоративной сети

Факсы
Ответы и письма по электронной почте

Факсимильная информация
Бумажные документы
Письма
Договоры и контракты

Законодательные акты

Нормативные документы

Периодические издания

Книги
Реклама
Анкеты
Приказы
Инструкции.
Отчеты
Служебные записки
Командировочные документы
Бухгалтерские документы
Письма
Договоры и контракты
Пресс - релизы

Автоматизация делопроизводства на этом уровне требует предварительного обследования документопотоков на предприятии с последующей фиксацией модифицированного регламента делопроизводства в инструкциях и положениях, а также настройки регламентов прохождения электронных документов по рабочим местам. Специальное структурное подразделение осуществляет: регистрацию документов, контроль за их исполнением, учет исполнения, систематизацию документов, формирование номенклатуры дел и контроль за состоянием самих дел.
Безбумажное делопроизводство предусматривает применение компьютера в управленческой деятельности для хранения, поиска и отображения информации, позволяя свести к минимуму или исключить полностью применение бумажных носителей.
Электронный офис предполагает организацию работы групп пользователей над совместным решением сложных распределенных задач в электронных компьютерных сетях с помощью средств вычислительной техники. Сегодня существует большое число концепций построения электронного офиса, в частности фирм Microsoft, Borland, Lotus. Все чаще обращаются к понятию "workflow" - стратегии обеспечения управления прикладными программами, необходимыми для прохождения потока работ в электронном офисе.
Использование сетей и средств электронной почты позволяет мгновенно пересылать документы из одного подразделения в другое без временных задержек на передачу бумажного документа. Упрощает хранение, контроль, поиск, архивирование, включая ведение долговременного архива документов. Здесь есть два существенных препятствия: внешнее и внутреннее.
Последнее зачастую связано с привычками и другими простыми человеческими особенностями и слабостями. Решение этой проблемы зачастую упирается в имидж фирмы.
Внешний срез проблемы упирается в большое число документов, предлагаемых в бумажном виде. Классическими примерами являются письма и факсы, периодические издания. Переход от бумажного ведения делопроизводства к электронному сдерживается из - за недостаточно развитой технологии оптического распознавания текстов (optical character recognition - OCR). Последние достижения в этой области послужили толчком к активному внедрению технологий электронного документооборота, в том числе и у нас в стране. Притягательность ввода текста без использования клавиатуры определяет интерес и к технологиям распознавания голоса. Совместно с технологиями архивирования, индексирования и поиска документов это создает основу построения системы управления электронным документооборотом.

2.3 Системы управления электронным документооборотом

Система управления электронным документооборотом (СУЭД) предназначена для следующих целей:
\* интеграции процессов документального обеспечения управления предприятием в рамках единой информационной системы;
\* повышение информированности руководства и специалистов за счет увеличения объемов информационного хранения, централизированной обработки информации, уменьшения времени поиска документов и соответственно подготовки отчетов и докладов, а также за счет повышения полноты и достоверности отчетов;
\* уменьшения стоимости документационного обеспечения управления предприятием за счет перехода от бумажного делопроизводства к электронному, снижения стоимости копирования и передачи бумажных документов;
\* уменьшения стоимости и сокращения времени поиска бумажных оригиналов документов в архивном хранении за счет получения точной адресации в электронном виде;
\* интеграции информационных процессов в рамках кооперации предприятий;
\* создание качественно новой информационной базы для последующего совершенствования процессов документационного обеспечения управления и технологии работы с документами.
СУЭД должна соответствовать существующей информационно - организационной структуре предприятия (группы предприятий) и обеспечивать модификацию по мере совершенствования этой структуры.
СУЭД (рис. 4 (приложение)) предназначена для автоматизации процессов документационного обеспечения управления предприятием, включая:
1. процессы подготовки, ввода, хранения, поиска и вывода организационно - распорядительных документов (подсистема "Электронный архив");
2. процессы подготовки, ввода, хранения, поиска и вывода стандартных форм документов (подсистема "Ввод стандартных форм документов");
3. управление делопроизводством (создание, обработка и систематизация архивного хранения документов - подсистема "Делопроизводство").
Объектом автоматизации являются процессы:
\* создание документов;
\* подготовки, учета, систематизации и архивного хранения, поиска и получения организационно - распорядительных, отчетно - статистических, учетных, плановых, информационно - справочных и других управленческих документов;
\* работы с документами (передача, учет, контроль исполнения и др.).
Основные требования к системе состоят в следующем. Для информационного обмена в системе должна использоваться корпоративная вычислительная сети, в которую включаются как локальные, так и удаленные пользовательские системы. СУЭД должна взаимодействовать с электронной почтовой системой и автоматизированными системами управления предприятием. Система должна допускать круглосуточный режим функционирования; иметь средства диагностики и индикации текущего состояния системы, используемых ресурсов; позволять наращивать количественные и расширять функциональные характеристики системы.
СУЭД должна обеспечивать изменение своих характеристик,
параметров, адресатов передачи документов и т.п. в зависимости от изменения регламента документооборота предприятия (норм, правил, порядка, форматов и т.п.).
Система должна строиться на основе открытых технологий, обеспечивающих ее дальнейшую модернизацию и развитие без переработки. В системе должна быть предусмотрена возможность использования масштабируемых аппаратных платформ, в частности технологически простой замены серверов и устройств хранения информации на более производительные (емкие).
Система должна обеспечивать с достаточной точностью распознавания документов на русском и основных европейских языках текстового формата А4, а также полнотекстовую индексацию текстового документа. Особое внимание должно уделяться объемам хранения, одновременному доступу к документам и срокам хранения документов.
Подсистема "Электронный архив" предназначена для следующих целей:
\* оперативного и потокового ввода документов, полеченных из бумажных документов путем сканирования (получение электронных графических образов) и OCR - распознавания (преобразование их в текстовые документы);
\* оперативного и потокового ввода электронных документов из других источников;
\* передачи электронных документов в подсистему "Делопроизводство";
\* реквизитного и полнотекстового индексирования документов;
\* хранения электронных документов всех видов и представлений (в том числе графических образов), их поисковых образов и индексов (атрибутных и полнотекстовых);
\* адресация оригиналов документов в бумажном архиве;
\* поиска и извлечения документов из электронного архива;
\* вывода документов из системы в виде твердой (бумажной) копии или в электронном виде, в том числе для дельнейшей доставки средствами связи;
\* связи представлений хранимых документов с фактографической частью базы данных;
Подсистема "Ввод стандартных форм документов" обеспечивает:
\* проектирование представлений стандартных форм документов для их последующего ввода;
\* потоковый ввод стандартных форм документов в фактографическую часть подсистемы "Электронный архив" (включая сканирование, OCR (ICR) - стилизованное распознавание, контекстный контроль и экспорт в БД).
Подсистема "Делопроизводство" обеспечивает:
\* создание электронных документов средствами подсистемы;
\* ведение версий (редакций) документов и их авторства;
\* защиту от конфликтов при попытке одновременной модификации документа;
\* электронное визирование документов (электронная подпись);
\* связывание документов в логические группы;
\* организацию потока работ с документами: задание маршрута (регламентного или ситуационного) движения документов и условий осуществления работ с ними;
\* допуск к документам и расширенным видам работ с ними в соответствии с установленными правами пользователей;
\* протоколирование видов работ, производимых пользователями с документами;
\* управление маршрутами движения документов;
\* контроль местонахождения документа и состояния его исполнения;
\* передачу и извлечение документов в/из подсистемы "Электронный архив".
Возможный состав программных инструментальных и технологических средств, ориентированных на управление документами и документооборотом, а также средств реализации процедур работы с документами может быть представлен следующим образом:
\* средства для ввода бумажных документов и распознавание образов;
\* средства для создания электронных документов;
\* средства для организации и работы с электронным архивом;
\* технологические средства, ориентированные на управление документооборотом;
\* технологические средства, ориентированные на управление документами;
\* инструментальные средства разработки приложений, реализующих специфические функции и технологии работы с документами.
Программные технологические пакеты, ориентированные на управление документами и документооборотом, должны быть открытыми для интеграции с приложениями, реализующими специфические функции, характерные при работе с документами на предприятии.
Инструментальные средства для разработки приложений должны быть такими, чтобы приложения, разработанные с их помощью, интегрировались в программную среду управления документами и документооборотом.
Рассмотрим организационно - функциональные особенности основных подсистем, ориентируясь на решения и предложения фирмы "Интеллектуальные технологии" (Cognitive Technologies) - одного из лидеров на российском рынке по технологиям создания СУЭД и распознавания образов.

2.4 Корпоративный электронный архив

Функциональные возможности подсистемы "Электронный архив", предлагаемой фирмой "Интеллектуальные технологии", соответствуют приведенным выше требованиям. Рассматриваемое решение выполнено в архитектуре "клиент - сервер" и ориентировано на использование оборудования, изготовленного согласно промышленным стандартам. Решение масштабируемом и предполагает простую адаптацию к требованиям как по быстродействию, так и по количеству рабочих мест для ввода и поиска документов. Оно не накладывает никаких ограничений на формат документов, предусматривает обработку разнородных документов, хранение в одном архиве информации различного типа (например, технической документации, финансовых отчетов, документов и т.д.).
Основные преимущества предлагаемого решения заключаются в полной автоматизации следующих операций:
\* получение электронного образа документа (сканирование);
\* распознавание текста изображения документа (OCR - распознавание);
\* морфологического анализа (нормализация) текста документа;
\* полнотекстового индексирования текстовой информации в документе;
\* классификации, аннотирования и создания регистрационной карточки документа;
\* поиска и выборки электронного образа документа по значению его регистрационных атрибутов либо по текстовому содержанию.
Участие оператора требуется только на этапах формирования атрибутов и получения текста документа при использовании OCR - распознавания, если требуется редакторская правка распознанного текста. Выбор операций для конкретной реализации системы зависит от технологической цепочки при работе с разными типами документов.
Предлагаемая система предоставляет также дополнительные возможности:
\* разграничение доступа пользователей к документам на основе механизма привилегий;
\* ручное задание атрибутов документа в процессе его регистрации в системе.
Архитектура системы "Электронный архив" приведена на рис. 1. Она использует технологию "клиент - сервер" при структурировании программного обеспечения сервера в виде "сервера баз данных" и "сервера приложений". Сервер приложений выполняет комплексы прикладных программ, реализующих функции, запрашиваемые с отдельных рабочих мест. В процессе выполнения указанных функций сервер приложений обращается к серверу баз данных посредством SQL - запросов на чтение и запись данных соответствующей базы данных, а также выполняет необходимые вычисления. Полученные результаты сервер приложений передает пользователю, который обратился к этому серверу за выполнением нужной ему функции.
В качестве программного обеспечения сервера баз данных можно использовать сервер баз данных ORACLE7 SERVER фирмы oracle или другие типы развитых СУБД. Продукты этой фирмы вместе с услугами по техническому обслуживанию, обучению, консультированию и системной интеграции являются основой интегрированной, открытой, переносимой среды разработки приложений. Реализуя подход к проектированию на основе визульного моделирования объектов и автоматизируя все этапы жизни приложения, эти средства обеспечивают высокую производительность разработчиков и создание приложений в архитектуре "клиент - сервер"".
Сервер приложений подсистемы "Электронный архив" реализует выполнение основных функций, перечисленных выше при рассмотрении требований к системе, включая разграничение доступа и защиту информации от несанкционированного доступа.
На каждый документ в электронном архиве заполняется регистрационная карточка. Набор атрибутов в карточке для различных типов документов может различаться.
Документ хранится в базе данных в виде совокупности своих представлений, например графического образа и текстового представления. Графический образ может быть получен в результате сканирования исходного документа в виде файла в одном из стандартных графических форматов. Текстовое представление может быть получено в результате распознавания текста отсканированного документа.
Подсистема доступа реализована в виде ПО для поиска, просмотра, выборки и печати документов из архива. Поиск можно выполнять как по тексту, имеющемуся на документе, так и по значению регистрационных атрибутов.
Выбор платформы во многом определяется требованиями к производительности системы. В настоящее время широкое применение получили многопроцессорные платформы с наращиваемой производительностью (за счет увеличения количества процессоров) с использованием операционных систем UNIX или Windows NT, которые поддерживают многопроцессорную архитектуру.

2.5 Информационно - поисковые технологии для электронного делопроизводства.

Информационно - поисковые технологии представлены в рассматриваемом комплексе подсистемой поиска и воспроизведения.
В системе предусмотрены развитые возможности индексирования, хранения и поиска документов, включая полнотекстовое индексирование (рис. 2).
Индексирование документов означает:
\* реквизитную индексацию;
\* ручное управление структурами хранения документов;
\* настройку состава полей, типа и длины контрольных карточек документа в архиве;
\* автоматическую полнотекстовую индексацию документов;
\* автоматическое распознавание формата файла электронного документа;
\* индексацию текста документа сразу при его вводе;
\* морфологический анализ индексируемых текстов для приведения помещаемых в индекс слов к канонической форме (нормализация текста в индексе);
\* наличие стоп - словарей при полнотекстовой индексации и обеспечение их настройки;
\* выделение из текста сложных (составных) терминов и понятий;
\* поддержку и настройку словарей и тезауруса;
\* технологию реквизитной разметки документов;
\* настройку набора реквизитов;
\* возможность различных режимов реквизитной разметки документов (ручной, автоматический, полуавтоматический);
\* интеграцию с произвольными программами создания, просмотра и изменения электронных документов.
Хранение документов включает в себя возможность:
\* работы с библиотеками магнитооптических дисков, магнитных лент, компакт - дисков для хранения больших объемов информации;
\* управление внешними носителями;
\* хранение электронных документов произвольного формата, аннотированных текстов, по которым производится поиск;
\* хранения в системе для каждой страницы как исходного изображения, так и распознанного текста.
Поиск предусматривает:
\* наличие стандартного языка запросов к БД;
\* реквизитный поиск документов;
\* полнотекстовый поиск, точность поиска;
\* поиск по именам документов и аннотациям;
\* формирование сложных запросов с использованием логических операций;
\* контекстный поиск и меру близости слов при поиске;
\* адекватность результата поиска запросу;
\* морфологический анализ при построении запроса;
\* возможность работы с системой удаленных пользователей.
Поиск может быть составным и включать несколько поисковых атрибутов из перечисленных выше типов. Результатом поиска служат образ найденных документов и содержание аннотаций, построенных в процессе индексирования или его ручного атрибутирования. Найденные образы могут быть распечатаны или переданы по корпоративной сети для просмотра с другого рабочего места.
Запрос строится путем заполнения шаблона ключевыми словами, содержание которых пользователь может задавать произвольно. Поиск документов по запросу осуществляется на двух уровнях: сначала происходит поиск в справочнике данных, а по ссылкам ищется (при задании пользователем соответствующих атрибутов) сам документ. Как правило, хранение документов осуществляется автономно из - за больших объемов архива и необходимости использования оптических накопителей информации. Такая архитектура, кроме всего, позволяет минимизировать время, затрачиваемое на физический доступ к документам в режиме множественных запросов, а также обеспечивает доступ данных из неоднородных (гетерогенных) сетей.
Следует отметить, что образ документа может храниться как в текстовом, так и в графическом формате. В последнем случае он, как правило, является результатом использования OCR - технологий.

3.1 Безопасность электронной почты

1. Фальшивые адреса отправителя. Адресу отправителя в электронной почте нельзя доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с SMTP - портом на компьютере, от имени которого он хочет отправить письмо, и ввести текст письма.
2. Перехват писем. Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Internet. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение.
3. Почтовые бомбы. Почтовая бомба - это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и того, как он сконфигурирован.
Анализируя атаки на электронную почту, приходится констатировать, что наиболее часто из низ встречаются следующие:
1. атаки, связанные с перехватом сообщений электронной почты, что может нанести ущерб репутации фирмы, создать о ней неверное представление;
2. из - за уязвимости почтового ПО возможно нарушение качества обслуживания;
3. источником риска может быть "враждебное" ПО, например, вирус.
Укажем некоторые средства защиты электронной почты.
1. Защита от фальшивых адресов. От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш - функция письма шифруется, используя секретный ключ отправителя. Получатель использует открытый ключ отправителя для расшифровки хэш - функции и сравнивает его с хэш - функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле написано отправителем, и не было изменено в пути. Правительство США требует использования алгоритма Secure Hash Algorithm (SHA) и Digital Signature Standard там, где это возможно. А самые популярные коммерческие программы используют алгоритмы RC2, RC4, или RC5 фирмы RSA.
2. Защита от перехвата. От него можно защищаться с помощью шифрования содержимого сообщения или канала, по которому оно передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все - таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой. Одним из самых популярных приложений является PGP. В прошлом использование PGP было проблематичным, так как в ней использовалось шифрование, попадавшее под запрет на экспорт из США. Коммерческая версия PGP включает в себя встраиваемые средства для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA.
3. Защита от спэма. Помочь выявить рассыльщиков спэма можно, используя методы фильтрации спэма на сетевом уровне. Фильтры бывают двух видов. Одна часть из них направлена непосредственно против конкретных отправителей, а другая часть состоит из персональных ассистентов, которые читают сообщения из Internet и выдают пользователю только те, которые касаются заданной тематики.

3.2 Защита электронного обмена данными

Защита электронного обмена данными (EDI) является важным фактором информационной безопасности.
Решением задач защиты EDI занимается, например, фирма Premenos Corp. Она выпустила семейство программных продуктов, названное Templar, реализующее защищенную передачу данных.
Рассмотрим некоторые средства для обеспечения безопасности электронного обмена данными.

3.3 Семейство продуктом PALINDROME

Семейство продуктов PALINDROME реализует архитектуру распределенного хранения данных - DSMA, основными компонентами которой являются:
\* кроссплатформенная совместимость (поддержка неоднородных платформ);
\* централизованный контроль над распределенными данными;
\* соответствие отраслевым стандартам;
\* масштабируемость (возможность увеличения числа подсоединяемых частей) в рамках всего семейства;
\* высокая производительность (резервное копирование выполняется со скоростью до 42,5 Гбайт/ч);
\* простота инсталляции, работы и эксплуатации;
\* использование технологии фирмы PALINDROME, называемой SafeStore.
Семейство продуктов PALINDROME предоставляет наилучшие возможности в шести важных областях применения: планирование восстановления после аварий; иерархическое хранение данных; резервное копирование; управление устройствами и библиотеками; архивация и перемещение информации; централизованное управление хранением данных.
Безопасность (например, переводов денежных средств) достигается не отдельными решениями, а системой хорошо продуманных мер. Угрозы безопасности в данном случае очень многообразны, например:
\* разрыв или сбой (дисфункция сети);
\* модификация информации;
\* маскировка с целью выдать себя за автоматизированного отправителя или получателя;
\* многократное повторение сообщения;
\* разглашение информации;
\* анализ рабочей нагрузки линии связи;
\* нарушение защиты передачи, при котором ухудшаются различные параметры системы безопасности сетей;
\* незаконный доступ к аудиторским журналам, позволяющий скрыть следы возможных растрат;
\* проникновение в центральную систему через сеть с целью изменения программ, уничтожение некоторой информации или незаконного перечисления денежных средств.
Перечисленные угрозы в разной степени подвергают опасности доступность, секретность и целостность информации. Чтобы обеспечить выполнение этих трех основополагающих условий (без которых невозможно проводить, например, денежные переводы по электронным сетям) и обеспечить защиту электронного обмена данными, необходимо принять некоторые меры безопасности.
1. Аутентификация информационных объектов, с которыми осуществляется связь. Механизмы аутентификации могут быть различными. Наиболее широко применяются такие криптографические алгоритмы, как RSA.
2. Контроль доступа, дополняющий аутентификацию. Логический контроль доступа позволяет определять для каждого файла и для каждой прикладной программы правомочных пользователей и их права (при переводах денежных средств - это чаще всего право подписывать и передавать данные переводы.)
3. Конфиденциальность. Обычно достигается криптографическими методами: информация кодируется так, чтобы оставаться непонятной для неправомочных лиц, а также лиц, не владеющих ключами к шифру.
4. Сохранение целостности информации - метод защиты от искажения или уничтожения чего - либо в данном сообщении. Использует сжатие информации и криптографию.
5. Метод восстановления, обеспечивающий работоспособность системы после устранения возникших проблем с безопасностью.
6. Метод защиты, который сохраняет информацию и дает возможность перезапустить систему при сбоях в сети и других угрозах безопасности.
7. Наблюдение за сетью. С помощью этого метода можно выявить отклонение от нормы технических параметров систем передачи информации (например, сбои в электропитании), а в некоторых случаях и попытки проникновения.
8. Ведение учетных журналов. Позволяет воспроизвести последовательность выполнения операций со стороны центральной системы или со стороны терминала.
9. Хронология. Дает возможность избежать повтора последовательности операций. Этот метод является необходимой защитой в области перевода денежных средств. Он использует, прежде всего, проставление даты и времени и составление журнала порядка переводов с порядковыми номерами, определенными для каждого адресата (получателя).
10. Система безопасности отдельного информационного комплекса. Позволяет удостовериться, что совокупность систем делает только то, что должны делать. Чтобы добиться этого, прибегают к сертификационной оценке программного и аппаратного обеспечения.

3.4 Сетевое резервное копирование

Быстрым восстановлением данных в случае потери занимаются системы резервного копирования и восстановления данных. Сетевая система резервного копирования (СРК) должна обеспечивать сохранение данных со всех узлов сети. В целом к сетевой СРК выдвигаются следующие сетевые требования.
Построение системы по принципу клиент/сервер. В применении к резервному копированию это означает следующее: компонент СРК, обеспечивающий управление всеми процессами и устройствами называется сервером, а компонент, отвечающий за сохранение или восстановление конкретных данных, - клиентом. В частности, такая система должна обеспечивать:
\* управление резервным копированием во всей сети с выделенных компьютеров;
\* удаленное резервное копирование данных, содержащихся на серверах и рабочих станциях;
\* централизованное использование устройств резервного копирования.
Многоплатформенность. СРК должна полноценно функционировать в современной гетерогенной сети, т.е. предполагается, что ее серверная часть будет работать в различных ОС, и поддерживать клиентов на самых разных аппаратно - программных платформах.
Автоматизация типовых процессов. Процесс резервного копирования неизбежно содержит много циклов различных операций. СРК должна выполнять циклические работы в автоматическом режиме и минимизировать число ручных операций. В частности, она должна поддерживать:
\* выполнение резервного копирования по расписанию;
\* ротацию носителей (последовательная замена носителей резервных копий);
\* обслуживание устройств резервного копирования по расписанию.
Поддержка различных режимов резервного копирования. СРК должна поддерживать возможность сохранения только той информации, которая была изменена с момента создания предыдущей копии.
Быстрое восстановление серверов сети после аварии. Сервер сети может выйти из строя по различным причинам, например из - за аварии жесткого системного диска или вследствие ошибок программного обеспечения, приведших к разрушению системной информации. В этом случае его восстановление требует переустановки ОС, конфигурирования устройств, инсталляции приложений, восстановления файловой системы и учетных записей пользователей. Все эти операции очень трудоемки, и на любом из этапов данного процесса возможно возникновение ошибок. Для восстановления сервера необходимо иметь резервную копию всей хранящейся на нем информации, включая системные данные, чтобы, как можно быстрее, привести его в рабочее состояние.
Резервное копирование данных в интерактивном (on - line) режиме. Зачастую информационная система включает в себя различные приложения клиент/сервер, которые должны функционировать круглосуточно. Примером тому являются почтовые системы, системы коллективной работы и SQL - серверы. Осуществить резервное копирование баз данных таких систем обычными средствами невозможно, поскольку они все время открыты. Поэтому в них часто встроены собственные средства резервного копирования, но их использование, как правило, не вписывается в общую технологию, принятую в организации. Исходя из этого СРК должна обеспечивать сохранение баз данных приложений клиент/сервер в интерактивном режиме.
Развитые средства мониторинга и управления. Для управления процессами резервного копирования и отслеживания их состояния СРК должна иметь графические средства мониторинга, управления и широкий набор средств оповещения о событиях.
Сетевая СРК состоит из аппаратных и программных компонентов.
Аппаратные компоненты предназначены для записи и хранения резервных копий с целью возможного восстановления данных с них.
В качестве носителя наиболее часто используются накопители на жестких дисках, магнитооптических дисках и магнитных лентах.
Для разового сохранения данных небольшого объема вполне подойдет жесткий диск или магнитооптический накопитель. Если речь идет о выборе аппаратного средства для проведения полного резервного копирования, да еще и в автоматическом режиме, то следует остановиться на ленточных накопителях: по скорости восстановления они не уступают магнитооптическим моделям, а по скорости записи даже превосходят их.
Для работы с магнитными лентами в СРК используются так называемые накопители с магазином автоматической подачи кассет (autochanger), или ленточные библиотеки. Ленточная библиотека состоит из двух функциональных устройств:
1. устройства чтения/записи, или стримера, предназначенного для записи информации на кассету и чтения с нее. В каждый момент времени стример способен работать только с одной кассетой;
2. устройства автоматической подачи кассет, или робота (robot), состоящего из магазина кассет и механизма, который выполняет подачу требуемой кассеты в стример и ее последующее извлечение.
Во всех производимых в настоящий момент стримерах реализованы технологии чтения/записи, обеспечивающие высокую плотность записи информации и, следовательно, высокую надежность ее хранения и большой объем.
Довольно распространены стримеры, построенные по технологии DLT. Ее отличительные черты - высокая плотность записи, быстрота передачи данных и надежность. В настоящий момент все производитель ленточных библиотек в своих новых моделях в основном используют DLT - стримеры. Другими достаточно распространенными стандартами магнитной записи стали DDS - 2 и DDS - 3.
Вся логика сетевого резервного копирования сосредоточена в программных компонентах и реализуется ими. Они управляют устройствами, процессом резервного копирования и восстановления данных, поддерживают расписание работ и реализуют дополнительные сервисные функции. Среди программ резервного копирования большой популярностью пользуется система ARCserve компании Cheyenne (подразделение Computer Associates). Программный пакет ARCserve выполнен в архитектуре клиент/сервер. На выделенном узле сети устанавливается серверная часть системы ARCserve, отвечающая за управление накопителями, подключенными к данному серверу, организацию всего процесса резервного копирования и управление служебными операциями. Резервное копирование и восстановление информации клиентов осуществляется по запросу от серверной части, клиенты только передают информацию серверу, который осуществляет ее сохранение на внешний носитель. Клиентами системы ARCserve являются как настольные компьютеры, так и серверные сети.
ARCserve разработана как многоплатформенная система сетевого резервного копирования. Ее серверная часть функционирует под управлением Microsoft Windows NT, Novell NetWare и различных клонов Unix.
ARCserve обеспечивает автоматизацию всех процессов, связанных с резервным копированием. Прежде всего, он выполняет резервное копирование по расписанию. Для каждого фрагмента информации (группа каталогов, база данных) регламентом определяется время начала копирования, внешнее устройство и тип копии (например, полная копия или копия изменений).
Система ARCserve поддерживает развитые схемы ротации носителей резервных копий. Она обеспечивает создание и хранение резервных копий данных каждый день в течение недели, раз в неделю в течение месяца и раз в месяц в течение года.
При реализации любой схемы ротации носителей ARCserve предварительно проверяет записанную на носитель информацию для предотвращения случайной порчи недавно сделанной копии.
Система резервного копирования ARCserve поддерживает различные механизмы создания резервных копий данных. В ARCserve существуют три вида резервных копий:
1. полная копия (Full Backup), представляет собой точный образ сохраняемых данных;
2. дифференциальная копия (Differential Backup), содержит только файлы, измененные со времени создания последней полной копии;
3. инкрементальная копия (Incremental Backup), содержит только файлы, измененные со времени создания последней полной, дифференциальной или инкрементальной копии.
Для эффективного восстановления серверов под управлением Windows NT и NetWare после аварии система ARCserve предлагает опцию аварийного восстановления (Disaster Recovery Option). В случае изменения параметров сервера, например, после установки пакетов исправления ошибок (Service Packs и Patches), для него создается комплект дискет аварийной копии.
Для сохранения баз данных прикладных систем в интерактивном режиме система ARCserve содержит ряд специальных программ - агентов. Каждая из них служит для сохранения баз данных конкретной система и функционирует как клиент системы ARCserve.
Кроме интерактивного резервного копирования баз данных, эти агенты обеспечивают и фрагментальное восстановление информации с резервных копий.
Помимо агентов для сохранения открытых баз данных, система ARCserve имеет агента для сохранения открытых файлов. Используя его, ARCserve может сохранять как сетевые файлы, открытые приложениями, так и базы данных прикладных систем, для которых не разработаны специализированные программы-агенты.
Управление системой ARCserve и всеми работами резервного копирования осуществляется из интерактивной графической программы - менеджера. Она предоставляет администратору и операторам системы резервного копирования следующие возможности:
\* задание регламента резервного копирования, схемы ротаций лент, типов резервных копий, режимов чистки устройств;
\* управление устройствами резервного копирования;
\* просмотр содержимого архивов и поиск требуемой информации в них;
\* контроль за процессом резервного копирования;
\* сбор служебной информации и статистики.
Для оперативного оповещения о событиях, возникающих в процессе копирования, система ARCserve позволяет автоматически передавать сообщения через сеть, электронную почту, пейджинговую или факсимильную связь или же выводить протокол всех событий на принтер.
Компания Connected предлагает развитую службу резервного копирования DataSafe, которая выполняет защиту данных с помощью паролей, а также шифрование информации по стандартному алгоритму DES (Data Encryption Standard), давно применяемому в банках и других финансовых учреждениях. Информация пользователей размещается в двух зеркальных центрах хранения данных Connected, предусматривающих несколько уровней избыточности компонентов, что исключает возможность ее потери. Эти служба ориентирована на мелкие фирмы или отделения крупных корпораций, не имеющие собственных специалистов по резервному копированию.
Шифрование данных, помогая решать проблему безопасности, снижает пропускную способность системы. Именно поэтому потребители пока не спешат с внедрением СРК.

3.5 Зеркальные серверы

Существует еще одна возможность защиты EDI - создание системы "зеркал" (mirror) серверов, дублирующих информацию главных серверов.

4.1 Что такое ЭЦП?

Известно, что содержимое любого документа (файла) представлено в компьютере как последовательность байтов и потому может быть однозначно описано определенным (очень длинным) числом или последовательностью нескольких более коротких чисел. Чтобы "укоротить" эту последовательность, не потеряв ее уникальности, применяют специальные математические алгоритмы, такие как контрольная сумма (control total) или хеш-функция (hash function). Если каждый байт файла умножить на его номер (позицию) в файле и полученные результаты суммировать, то получится более короткое, по сравнению с длиной файла, число. Изменение любого байта в исходном файле меняет итоговое число. На практике используются более сложные алгоритмы, исключающие возможность введения такой комбинации искажений, при которой итоговое число осталось бы неизменным. Хеш-функция определяется как уникальное число, полученное из исходного файла путем его "обсчета" с помощью сложного, но известного (открытого) алгоритма. Один из этих алгоритмов закреплен в ГОСТе Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хеширования".
Теперь рассмотрим, как получается электронная подпись. Здесь требуется небольшое отступление. С древних времен известен криптографический метод, позднее названный шифрованием с помощью симметричного ключа, при использовании которого для зашифровки и расшифровки служит один и тот же ключ (шифр, способ). Главной проблемой симметричного шифрования является конфиденциальность передачи ключа от отправителя к получателю. Раскрытие ключа в процессе передачи равносильно раскрытию документа и предоставлению злоумышленнику возможности его подделать.
В 70-х гг. был изобретен алгоритм асимметричного шифрования. Суть его состоит в том, что зашифровывается документ одним ключом, а расшифровывается другим, причем по первому из них практически невозможно вычислить второй, и наоборот. Поэтому если отправитель зашифрует документ секретным ключом, а публичный, или открытый, ключ предоставит адресатам, то они смогут расшифровать документ, зашифрованный отправителем, и только им. Никто другой, не обладая секретным ключом отправителя, не сможет так зашифровать документ, чтобы он расшифровывался парным к секретному открытым ключом.
Отправитель, вычислив хеш-функцию документа, зашифровывает ее значение своим секретным ключом и передает результат вместе с текстом документа. Получатель по тому же алгоритму вычисляет хеш-функцию документа, потом с помощью предоставленного ему отправителем открытого ключа расшифровывает переданное значение хеш-функции и сравнивает вычисленное и расшифрованное значения. Если получатель смог расшифровать значение хеш-функции, используя открытый ключ отправителя, то зашифровал это значение именно отправитель. Чужой или искаженный ключ ничего не расшифрует. Если вычисленное и расшифрованное значения хеш-функции совпадают, то документ не был изменен. Любое искажение (умышленное или неумышленное) документа в процессе передачи даст новое значение вычисляемой получателем хеш-функции, и программа проверки подписи сообщит, что подпись под документом неверна.
Таким образом, в отличие от собственноручной подписи, ЭЦП неразрывно связана не с определенным лицом, а с документом и секретным ключом. Если дискетой с вашим секретным ключом завладеет кто-то другой, то он, естественно, сможет ставить подписи за вас. Однако вашу ЭЦП нельзя перенести с одного документа на какой-либо другой, ее невозможно скопировать, подделать - под каждым документом она уникальна. Процедуры хранения, использования, обновления и уничтожения ключей достаточно подробно расписаны в различных методических рекомендациях к системам ЭЦП.

4.2 Шифрование

Рассмотрим шифрование информации асимметричными ключами. Если поменять ключи местами, иными словами, секретным сделать ключ расшифровывания, а открытым (публичным) - ключ зашифровывания, то отправитель может зашифровать письмо открытым ключом получателя, и тогда прочитать письмо сумеет лишь тот, у кого имеется парный секретный ключ, т. е. только сам получатель. Великое преимущество асимметричной схемы шифрования в том и заключается, что отпадает необходимость в конфиденциальной передаче ключей. Открытый ключ можно сделать доступным на Web-сайте, передать по электронной почте и т. п., не опасаясь негативных последствий доступа к нему третьих лиц.
Для удобства шифрования и использования ЭЦП в корпоративных системах с большим числом абонентов применяются справочники открытых ключей. Каждый ключ имеет тело и номер, одинаковый для секретной и открытой частей ключа и уникальный для каждого абонента. Номер передается в открытом виде в заголовке зашифрованного документа или в заголовке ЭЦП. Получатель по этому номеру из соответствующего справочника выбирает сам ключ, который подставляется в процедуру расшифровывания или проверки подписи. Выполняется такая выборка, как правило, с помощью специальных программ, и вся процедура занимает доли секунды.

4.3 Управление ключевой системой

Важную роль в системе электронного документооборота играет администрация системы. Она обеспечивает контроль за соблюдением абонентами единых правил работы, участвует в разборе конфликтных ситуаций, управляет ключевой системой и, что очень важно, поддерживает у всех абонентов справочники открытых ключей в актуальном состоянии. Справочники меняются регулярно: при любом изменении списка участников, при замене каких-либо ключей. Необходимость замены ключей возникает, скажем, в случае их компрометации - под этим понимают ряд событий, при которых ключевая информация становится недоступной или возникает подозрение о несанкционированном доступе. К таким событиям относятся утрата ключевых дискет; утрата дискет с последующим обнаружением; повреждение дискет; увольнение сотрудника, имевшего доступ к ключевой информации; нарушение правил хранения и уничтожения (после окончания срока действия) секретных ключей и др.
При возникновении подобного события участник системы обязан незамедлительно уведомить администрацию системы (или ее подразделение - центр управления ключевой системой) о факте компрометации. В свою очередь, администрация должна блокировать открытый ключ участника в справочнике и оповестить об этом других участников (обновить у них справочники). Фиксация момента уведомления администрации о компрометации ключей очень важна. Действительными считаются только те документы участника, которые были получены до этого момента. Данный факт учитывается при разборе конфликтных ситуаций: прежде всего проводится проверка, являлся ли ключ отправителя действующим на момент получения документа адресатом.
В том случае, когда в корпоративной системе документооборота предусмотрен обмен электронными документами лишь между центром (банком, брокерской фирмой, холдингом) и его клиентами, клиентам достаточно знать только один открытый ключ ЭЦП этого центра, последний же использует справочник открытых ключей всех клиентов. Если же в системе предусмотрена возможность обмена электронными документами между абонентами напрямую, то справочники с перечнями открытых ключей должны быть у всех участников и обновляться одновременно.

4.4 Пакет документов

Организация системы электронного документооборота не сводится к установке программного обеспечения. Значительно более сложным и трудоемким процессом (по крайней мере, на начальном этапе) является подготовка документов, подробно описывающих все процедуры функционирования системы, а также обучение сотрудников, которые будут обеспечивать ее работу. Упрощает ситуацию то, что образцы подобных документов уже существуют и можно заказать разработку всего пакета компании, имеющей опыт успешного применения ЭДО. Идеально, если эти документы прошли "проверку боем", то есть на их основе рассматривался конфликт в суде. Администрацию системы можно организовать на базе сторонней фирмы, располагающей соответствующими службами, квалифицированными сотрудниками, необходимыми комплектами договоров, определенным опытом обслуживания таких систем. Риск раскрытия конфиденциальной информации при этом отсутствует, поскольку секретными ключами участников администрация не обладает - она оперирует только справочниками открытых ключей. Важно, чтобы генерация ключей (включая секретные) проводилась уполномоченными сотрудниками участников (пусть и на территории лицензированной администрации.

4.5 Центр удостоверения открытых ключей

Решением проблемы распространения сертификатов открытых ключей среди всех заинтересованных в этом лиц является участие в электронном документообороте третьей, независимой, стороны, осуществляющей регистрацию и последующее распространение открытых ключей участников электронного документооборота. Такой третьей стороной является Центр удостоверения открытых ключей.
Для осуществления своих функций Центр удостоверения ведет специальный реестр, в котором содержится информация обо всех зарегистрированных в Центре удостоверения открытых ключах. При обращении любого лица с целью удостоверения открытого ключа какой-либо электронной цифровой подписи Центр удостоверения выдает Сертификат, в котором содержится информация о самом открытом ключе, об обладателе данной ЭЦП, информация о периоде, в течение которого действует ЭЦП, информация о наложенных обладателем данной ЭЦП ограничениях на область ее применения.
Услуги Центров удостоверения, предоставляемые посредством интернета, осуществляются автоматизированными компьютерными системами, поэтому доступ к таким услугам предоставляется все 24 часа в сутки без каких-либо перерывов или выходных. При этом услуги по удостоверению открытых ключей ЭЦП предоставляются центрами любому желающему и на безвозмездной основе. Зарабатывают на свое существование центры за счет сборов с обладателей ЭЦП за осуществление процедур регистрации открытых ключей, а также предоставления иных платных услуг.
Как уже ранее указывалось, электронный Сертификат вырабатывается автоматизированной системой Центра удостоверения при поступлении соответствующего запроса. Для того, чтобы исключить возможность подделки, электронный Сертификат заверяется электронной цифровой подписью Центра удостоверения. Проверка электронной цифровой подписи Центра удостоверения осуществляется с помощью соответствующего открытого ключа. Открытый ключ электронной цифровой подписи Центра удостоверения должен являться общеизвестным, с этой целью он должен периодически публиковаться в соответствующих печатных изданиях, а также содержаться на информационном сайте самого Центра удостоверения. Открытый ключ электронной цифровой подписи Центра удостоверения должен также указываться в выданной соответствующим государственным органом Центру удостоверения лицензии.
Центры удостоверения несут ответственность за убытки, понесенные пользователем открытого ключа в результате доверия к представленной в Сертификате информации, в случае, если она не соответствует действительности. Поэтому предоставление именно достоверной информации является основой деятельности Центров удостоверения.
Таким образом, разработанные процедуры деятельности Центров удостоверения в полной мере обеспечивают требования относительно безопасности проведения идентификации участников электронного документооборота. Осуществление процедур регистрации, распространения и идентификации открытых ключей не самими участниками электронного документооборота, а независимой третьей стороной, действующей публично, по сути дела, избавляет участников электронного документооборота от той рутинной работы, которая связана с осуществлением данных процедур. К тому же осуществление данных процедур Центрами удостоверения переводит правоотношения, связанные с распространением открытых ключей, из частно-правовой плоскости в публичную.

Рис .1

Рис. 2

Рис. 3

рис.4

6.1 Список выявленной литературы:

1. Распределительная система управления документами эпохи WEB - технологий // F1. - 1998. - №2. - c.34 - 37. - Рус.
2. Документация в информационном обществе: электронное делопроизводство и электронный архив / Кобелькова Л.А. // Отеч. архив. - 2000. - №1 - с.110 - 112. - Рус.
3. От изоляции к кооперации: Развитие систем электронной доставки документов и электронного МБА в региональных библиотеках / Терехович В.А. // 6 -ая Междунар. конф. "Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества", Судак и др., 5-13 июня, 1999 г., "Крым 99": Матер. конф. Т.1. - Симферополь, 1999.- с. 71-74.- Рус., рез. англ.
4. Развитие электронной доставки документов в библиотеках России. Глухов В.А., Лаврик О.Л. 275 лет на службе науке: библиотеки и институты информации в системе РАН: Сборник науч. трудов. Инф.- библ. совет. М.: Изд-во Инф.- библ. совет., 2000, с. 192-204. Библ. 18. Рус.
5. Создание корпоративной системы электронной доставки документов г. Новосибирска. Лаврик О.Л., Баженов С.Р. 8-ая Междунар. конф. "Крым - 2001". "Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества", Судак, 9 - 17 июня, 2001: Тема 2001 г. "Производители и пользователи печатной и электронной информацией на пути к информационному обществу": Труды конф. Т. 2. М.: Изд-во ГПНТБ России, 2001., с. 780 - 784, 1 кл., табл.1, Библ. 7. Рус, рез. англ., укр.
6. Интернет - документ как объект архивного хранения. Боброва Е.В. Инф. бюл. Ассоц. "История и компьютер". 2000, № 26-27, с. 108-113. Библ. 3 . Рус.
7. Доставка электронных документов в ЦНСХБ, Аветисов М.А., Крамчанинов Е.В., Пожилов В.В. Библиотечное дело - 2001: российские библиотеки в мировом информационном пространстве: тезисы докладов 6-ой Междунар. научной конференции, Москва, 26-27 апр., 2001. Ч. 2. М.: Изд-во МГУКИ. 2001, с. 266. Рус.
8. Электронные документы и архивы: теория и практика / Юмин И.Ф. // Оте. арх. - 1999.- № 3. - с. 109-112 . - Рус.
9. Австралийский проект JEDDS. The Australian JEDDS project / Cunningham Adrian // CDNLAO Newslett. - 1998.- №32.- c.1-2.- Англ.
10. Электронные документы в корпоративных сетях: второе пришествие Гутенберга / С. В. Клименко, И. В. Крохин, В.М. Кущ, Ю. Л. Гагутин .- М. : Анкей : Экотрендз, 1999 .- (инженерная энциклопедия). - (технологии электронных коммуникаций). - 271 с. : ил.
11. Карминский А. М., Нестеров П. В. Информатизация бизнеса. - М.: Финансы и статистика, 1997. - 416 с.: ил.
12. Балабанов И.Т. Интерактивный бизнес. - СПб: Питер, 2001. - 128 с.: ил. - (серия "Краткий курс").
13. Милославская Н. Г., Толстой А. И. Интрасети: доступ в Internet, защита: Учеб. пособие для вузов. - М.: ЮНИТИ - ДАНА, 2000 - 527 с.
14. Куперштейн В.И. Современные информационные технологии в делопроизводстве и управлении. - СПб. и др.: БХВ, 1999. - (изучаем вместе с BHV). - 248 с.: ил.
15. Документальные компьютерные технологии: Учеб. пособие/ Моск. гос. техн. ун-т им. Н. Э. Баумана. - М.: Б. и., 1997 -.Ч. 2: Управление информационными процессами в офисных системах. - 1997. - 122 с.: ил.
16. Специальная информатика: Учеб. пособие/ С. В. Симонович, Г. А. Евсеев, А. Г. Алексеев. - М.: АСТ - Пресс: Инфорком - Пресс, 2000. - 479 с.: ил.
17. Имери В. Как сделать бизнес в Internet/ Пер. с англ.: А.А. Борисов и др. - Киев и др.: Диалектика, 1998. - 463, [4] с.: ил.
18. Вершинин А. И. Электронный документ: правовая форма и доказательство в суде: Учеб. - практ. пособие/ А.П. Вершинин. - М.: Городец - издат, 2000. - 247 с.
19. Гражданско - правовое регулирование банковской деятельности: Учеб. пособие/ В. А. Белов и др.; Под ред. Е. А. Суханова. - М.: Учеб. - консультац. центр "Юринфор", 1994. - (библиотека "Юринфор"). - 250, [1] с.
20.Системы управления и информационные технологии: Межвузов. сб. науч. тр./ Воронеж. Гос. техн. ун - т; Науч. ред. С. Л. Подвальные. - Воронеж: Из-во Воронеж Гос. техн. ун - т., 1998. - 201 с.
21.www. osp. ru
22.www. kv. by
23.www. referatov. net
24.www. referat. ru
25.www. ixbt. ru
26.www. computerra. ru