Владычкина Наталья Васильевна

Магистрант НАЧОУ ВПО СГА

Направление: Информатика и вычислительная техника

Магистерская программа: Распределенные автоматизированные системы

Специфика и актуальные проблемы системы электронного документооборота

Аннотация. Данная статья рассматривает актуальные проблемы системы электронного документооборота, сложившейся в России относительно недавно и развивающейся стремительными темпами. Однако указанная система, которая существует на данный момент, имеет ряд существенных недостатков. В статье раскрываются настоящие проблемы электронного документооборота, а также способы их решения. Предполагаемой методикой решения проблемы, которая была выявлена в момент исследования текущих систем электронного документооборота, является использование анонимных криптографических сетей.

Ключевые слова: электронный документооборот, сеть i2p, электронная подпись.

Прежде чем приступить к рассмотрению специфики электронного документооборота, следует определить его сущность. Документооборот представляет собой циркулирование документа с момента его создания или получения до отправления или завершения операций с ним. Его специфика состоит в том, что документы создаются, хранятся и обрабатываются на компьютере, имеющем электронную подпись (ЭП), то есть аналог ручной подписи, подтверждающий подлинность и силу документа. Выполнение данного принципа дает возможность перейти от бумажных носителей к новым технологиям и более эффективно организовать работу с документацией.

В настоящее время популярность получили разнообразные системы документооборота, в частности, 1С: Документооборот, Alfresco (ECM-система), электронные офисные системы Germes, ЕВФРАТ и т. д. Различия между указанными системами обусловлены степенью их сложности, а также различными практическими целями и функциями.

Как известно, каждая система имеет свои преимущества и недостатки. Наиболее характерными признаками несовершенств электронного документооборота являются нижеприведенные факторы:

1. Существенные материальные затраты на реализацию электронного документооборота,

2. Избыточное количество компонентов, необходимых для функционирования системы.

Чтобы обеспечить функционирование электронного документооборота необходимо создать отдельный защищенный канал связи Интернет, обратиться к услугам криптопровайдера, кодирующего данные на канале связи и, кроме того, приобрести электронно-цифровую подпись (ЭЦП) и специальное программное обеспечение (ПО). Однако использование совокупности перечисленных компонентов, необходимых для обеспечения электронного документооборота, представляет собой побочную проблему: избыточность инструментария для функционирования системы.

На рисунке (рис. 1) изображена схема передачи электронного документооборота по каналам связи Интернет. Схема демонстрирует, что клиенту А необходимо отправить пакет документов клиенту Б, для отправки которого обязательно нужно подтвердить подлинность (силу) документа электронно-цифровой подписью. Далее осуществляется процедура кодирования пакета документов криптопровайдером, после которой происходит их отсылка клиенту Б. Суть автоматизации заключается в максимальном упрощении процесса: нет необходимости использовать услуги криптопровайдера, если существует зашифрованная сеть, то есть готовое решение проблемы [2, с. 213].

Имеется много разновидностей зашифрованных сетей, для демонстрации принципа их функционирования рассмотрим на примере сеть i2p.

I2p сеть является анонимной самоорганизующейся распределенной сетью, которая предоставляет приложениям простой транспортный механизм для анонимной и защищённой пересылки сообщений друг другу. Как правило, внешне сеть i2p не отличается от Интернет, однако ее преимущество состоит в анонимности и безопасности сети.

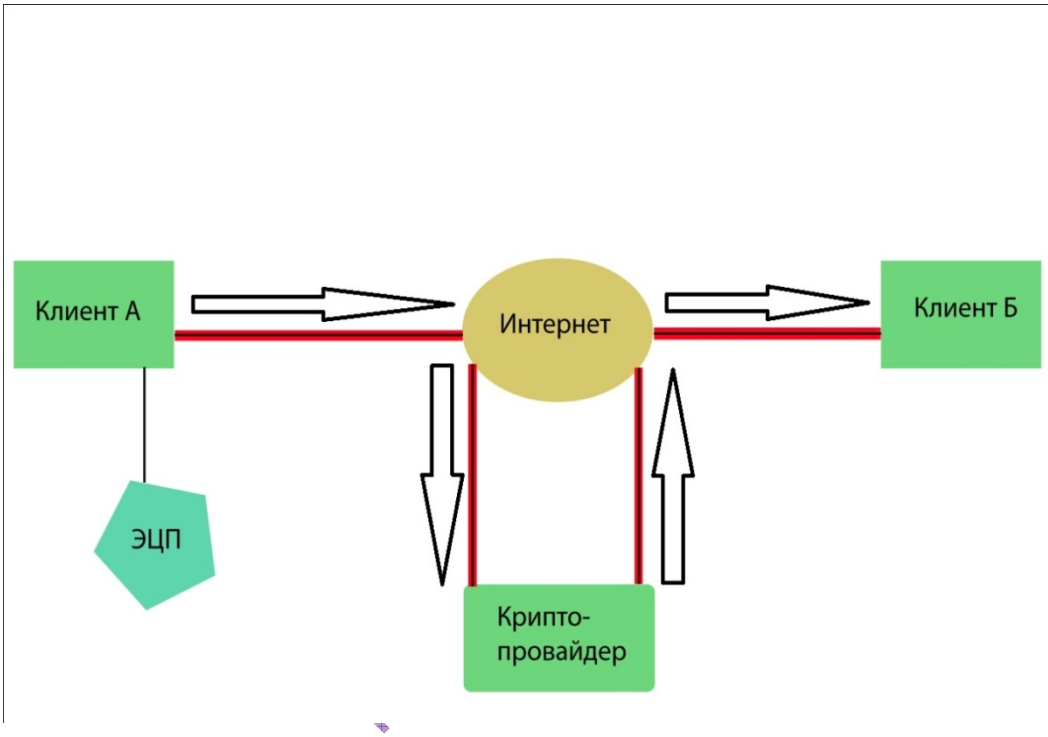

Рис. 1. Схема передачи ЭД по Интернету

Рассмотрим принцип действия анонимной сети i2p. Допустим, что клиенту А нужно отправить запрос клиенту Б, для отправки которого клиенту А необходимо построить туннель к клиенту Б, по которому и будет отправлен запрос. Запрос проходит через некоторое количество участников туннеля, где данные проходят процедуру шифрования (рис. 2). Указанный метод шифрования принято называть чесночным. Кроме того, сеть также использует следующие уровни кодирования: сквозное, туннельное и шифрование транспортного уровня. Перед данной процедурой в каждый сетевой пакет автоматически добавляется небольшое случайное количество некоторых байт, для того чтобы в большей степени обезличить передаваемую информацию и

затруднить попытки анализа содержимого и блокировки передаваемых сетевых пакетов. Каждое сетевое приложение прокладывает отдельный туннель, имеющий только одно направление. Следовательно, исходящий трафик идет по одному туннелю, а входящий – по другому. Все передаваемые сетевые пакеты имеют свойство расходиться по нескольким разным туннелям, что делает бессмысленным попытки прослушать и проанализировать с помощью сниффера проходящий поток данных.

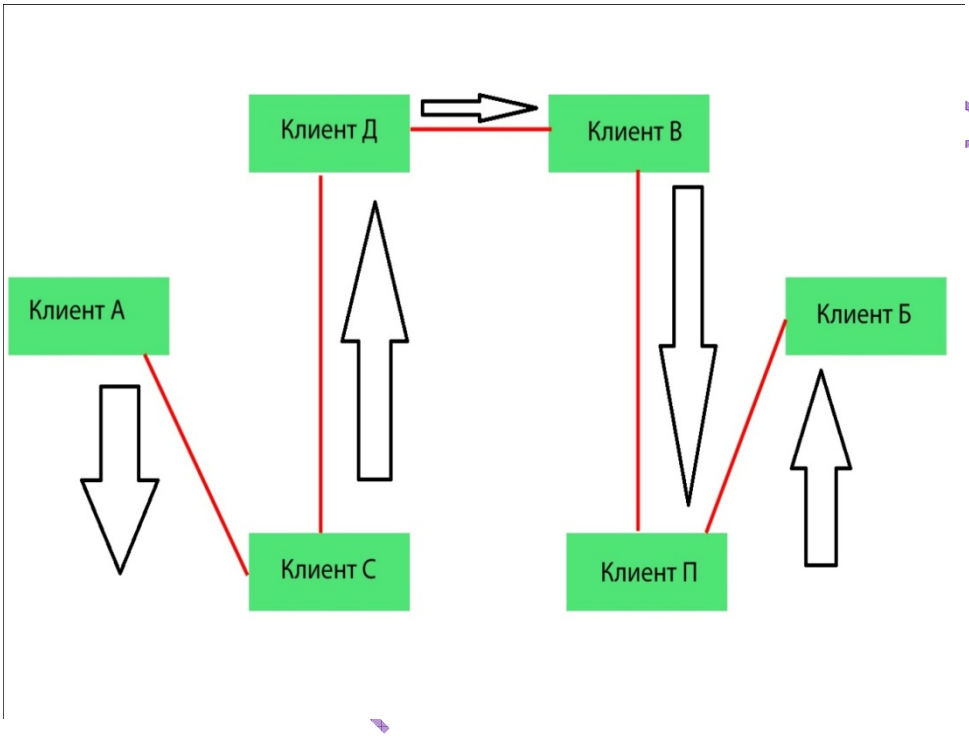

Рис. 2. Работа сети i2p

Решить проблему избыточной сложности устройства электронного документооборота (ЭД) возможно, построив новую систему, основывающуюся на сети i2p, что в целом позволит упростить процесс ЭД. Защищенная сеть содержит в себе несколько компонентов, следовательно, нет необходимости создавать отдельный канал связи и использовать услуги криптопровайдера.

Главным свойством конфиденциальности в сети i2p является число уровней шифрования: чем больше их количество, тем выше уровень информационной безопасности при увеличении сложности криптографического воздействия на запросы. Однако, к сожалению, усложнение шифрования значительно повышает потребление пропускной способности канала связи и

вычислительных ресурсов, что в значительной мере увеличивает интервал времени отклика системы. Как правило, для электронного документооборота в режиме оффлайн данный аспект не сопровождается негативными последствиями, при этом в некоторых случаях необходимо оперативно формировать трафик ЭД между рядом организаций. Исходя из этого, следует значительно сократить время отклика системы.

Сеть i2p основана на клиентской системе сообщения между вычислительными точками (компьютерами). Под клиентской системой подразумевается использование специального программного обеспечения для доступа в анонимную сеть. Одним из преимуществ данного ПО является гибкость конфигурирования, которая даёт возможность реабилитировать утраченную скорость. Следовательно, используя корректно составленный алгоритм конфигурации системы, можно предупредить проблему низкой производительности сети с учетом сложного шифрования.

На базе организованной сети следует разработать собственное программное обеспечение, реализующее возможность беспрепятственного функционирования процесса ЭД. Для разработки приложения следует учитывать функциональную возможность сети i2p и ее производительность. По проведении исследования на предмет производительности сети было выявлено, что наиболее удобным методом организации ЭД является разработка WEB-интерфейса, доступного каждому пользователю, подключенному к сети. Однако использование системы должно осуществляться лишь после процесса регистрации на физическом и на виртуальном уровнях.

Организация WEB-интерфейса в сети i2p дает возможность обеспечить безопасность передаваемой информации в десятки раз выше, чем в сети Интернет. При этом, не затрачивая дополнительных материальных средств на усовершенствование системы, можно обеспечить защиту общедоступному объекту, чтобы злоумышленник не имел возможности проникнуть в систему, открыть базу данных и впоследствии воспользоваться конфиденциальной информацией.

Разработать абсолютную защиту от атак по проникновению в систему с целью завладения конфиденциальной информацией практически невозможно, однако следует перестраховать свою систему, создав распределенную базу данных и многоуровневую систему аутентификации, которая позволит отследить легитимность пользователя, пытающегося получить доступ к базе, на каждом из уровней.

Помимо обеспечения информационной безопасности, необходимо предусмотреть удобную работу с системой, учитывая тот факт, что сеть i2p является более медленной, чем Интернет. Для достижения этой цели следует максимально разгрузить канал связи, используя оффлайн работу с данными, т.е. обработку и хранение информации на стороне клиента. Это даст возможность синхронизировать информацию между сервером и клиентом, не поддерживая постоянное соединение для передачи данных с целью переработки на сервере [1, с. 49].

Разработать данную методику обмена и обработки информации позволит технология HTML5, которая дает возможность организации собственной базы данных на стороне клиента. На сегодняшний день эту технологию поддерживают ряд современных браузеров, в том числе таких, как Google Chrome, Opera, Firefox Mozilla [3, с. 135].

Исходя из вышеописанного, следует, что для организации действующей системы электронного документооборота нет принципиальной необходимости в затрате большого объема материальных средств. Таким образом, выполняется процесс повышения информационной безопасности системы посредством реализации передачи данных по уже существующей анонимной сети i2p. Так, для разработки ПО нет необходимости использования платных программных продуктов, что также является максимально рентабельным. Еще одним преимуществом данного метода разработки системы ЭД является сокращение инстанций, к которым необходимо обращаться пользователю для регистрации в системе, а также сокращение затрат на закупку программного обеспечения, предоставляющего возможность туннелирования или криптографирования

данных. Следовательно, исходя из результатов проведенного исследования, разработка системы ЭД в сети Интернет является нерентабельной и нецелесообразной.

Литература

1. Ажмухамедов И.М. Электронные удостоверения личности на основе стеганографических и криптографических алгоритмов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2009. № 2.
2. Куняев Н.Н., Демушкин А.С., Фабричнов А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот. М.: Логос, 2011.
3. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. СПб.: БХВ-Петербург, 2005.