ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

На правах рукописи

УДК 004.056.5

ТУРСУНБАЕВ УЧКУН ТУРГУНОВИЧ

Исследование и оптимизация защиты систем электронного документооборота

5А330203 – Прикладная информатика

Диссертация на соискание академической степени магистра

Научный руководитель
к.т.н. Парпиев Н.Н.

Ташкент – 2014

С О Д Е Р Ж А Н И Е

ВВЕДЕНИЕ

На заседании Кабинета Министров Республики Узбекистан, посвящённого итогам социально-экономического развития страны в 2012 году и важнейшим приоритетным направлениям экономической программы на 2013 год, Президент Ислам Каримов подчеркнул важность реализации мер и проектов в сфере ИКТ. «Все большее значение приобретает ускоренная реализация мер и проектов в сфере информационно-коммуникационных и телекоммуникационных технологий. Мы должны отдавать себе отчет, что без кардинального, я бы сказал взрывного продвижения по пути широко внедрения во все сферы экономики, в нашу повседневную жизнь современных информационно-коммуникационных систем трудно видеть перспективу» - отмечает Президент Республики Узбекистан [7].

По итогам было принято решение ускорить разработку Концепции и комплексной программы формирования системы «электронное правительство» в нашей стране.

Система электронного документооборота (СЭД) является ключевым элементом «электронного правительства», поскольку успешное внедрение СЭД способствует повышению эффективности взаимодействия между органами государственной власти и управления, частным сектором и населением, а также формированию в стране информационного общества.

Мощным стимулом по внедрению СЭД в Узбекистане стало постановление Кабинета Министров «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах» от 4 мая 2011 года. В рамках реализации вышеуказанного постановления Государственным унитарным предприятием «UNICON.UZ» проведены работы по подключению

министерств и ведомств к единой защищенной СЭД «e-Hujjat», к которой на сегодняшний день подключены более 150 министерств, ведомств предприятий и организаций.

Актуальность темы. Одним из составляющих элементов платформы «электронного правительства» является система электронного документооборота[12]. В настоящее время в нашей стране всё большее распространение получают системы электронного документооборота. Действуют законы “Об электронном документообороте”, “Об электронной цифровой подписи” и другие законодательные документы, которые дают дополнительный импульс в развитии систем электронного документооборота. При внедрении электронного документооборота одним из первых требований является безопасность системы[8]. В настоящее время есть многочисленные защитные системы, но нет универсальной защищенной системы. Актуальность выбранной темы состоит в оптимизации и улучшении защиты систем электронного документооборота.

Предмет исследования: Предметом исследования являются действующие модули и технологии защиты систем электронного документооборота.

Объект исследования: Системы электронного документооборота и алгоритмы криптографической защиты информации.

Цель работы. Разработать методы, алгоритмы и программные обеспечения для совершенствования защиты системы электронного документооборота.

Задачи. Для достижения заданной цели необходимо решить следующие задачи:

- исследование систем электронного документооборота;
- анализ текущего положения защиты системы электронного документооборота;
- определения преимуществ и недостатков защиты;

- усовершенствования алгоритмов защиты систем электронного документооборота;
- оптимизация информационной безопасности системы по выявленным недостаткам.

Результатом выполнения поставленных задач, будут новые или исправленные модули защиты системы электронного документооборота.

Исправляемые и разрабатываемые модули защиты помогают, обеспечить высокий уровень защиты информации в системах электронного документооборота.

Значимость данного исследования заключается в том, что созданные и исправленные модули защиты могут быть применены при усовершенствовании и улучшении защиты системы электронного документооборота и обеспечении устойчивости от современных угроз.

Методы исследования. В данной диссертационной работе были применены основы информатики и математики, методы информационной безопасности, методы модульной арифметики и программирования.

Научная новизна проведенных исследований заключается в том, что в результате исследования разработана усовершенствованный алгоритм Диффи-Хелмана для обмена секретных ключей, используя элементы параметрической алгебры.

Практическая ценность. Представленная в работе программа позволяет создавать защищенная подключения в незащищенных каналах связи, легко встраивается на готовые программные продукты.

Структура и объём магистерской диссертационной работы.

Магистерская диссертация состоит из введения, трёх глав и заключения, изложена на ___ страницах машинописного текста, содержит ___ таблицы и ___ рисунков.

Глава 1. Исследование основных проблем обеспечения защиты информации в системах электронного документооборота

1. Изучение нормативно-правовой базы по делопроизводству внутри организации

В Республике Узбекистан принято несколько нормативных документов, которые регулируют правила организации делопроизводства и организации контроля исполнения в органах государственной власти и управления. Основными законами являются:

1. Закон Республики Узбекистан «Об обращениях граждан»;
2. Постановления Кабинета Министров «Об утверждении нормативных документов по делопроизводству и организации контроля исполнения в органах государственной власти и управления Республики Узбекистан»;
3. Постановления Кабинета Министров «О мерах по укреплению исполнительской дисциплины».

Закон Республики Узбекистан «Об обращениях граждан» был принят в 6 мая 1994 года и 13 декабря 2002 года внесены изменения и дополнения. В соответствии настоящим законом граждане Республики Узбекистан имеют право обращаться в государственные органы с заявлениями, предложениями и жалобами. Все заявления и обращения граждан, согласно статье 18 данного Закона, должны рассматриваться в срок до одного месяца со дня поступления в государственный орган, который обязан разрешить вопрос по существу. Более того, заявления, не требующие дополнительного изучения и проверки, нужно рассмотреть не позднее 15 дней. И лишь в исключительных случаях, когда для рассмотрения жалобы или заявления необходима дополнительная проверка или истребование дополнительных материалов, сроки могут быть

продлены руководителем соответствующего государственного органа, но не более чем на месяц. Об этом обязательно сообщается заявителю.[1]

В постановлении Кабинета Министров «Об утверждении нормативных документов по делопроизводству и организации контроля исполнения в органах государственной власти и управления Республики Узбекистан» от 29 марта 1999 года, утвержден необходимые нормативные документы. А также постановления Кабинета Министров «О мерах по укреплению исполнительской дисциплины» от 12 января 1999 года и её приложении и схемы определяет четкое понятие о структуре ведении делопроизводства и организации контроля.

При дальнейшем урегулировании делопроизводства принято ещё несколькие нормативные документы, которые уже улучшают делопроизводства в электронном виде. Ниже приведены нормативные документы об электронном документообороте:

1. Закон Республики Узбекистан «Об электронной цифровой подписи»;
2. Закон Республики Узбекистан «Об электронном документообороте»;
3. Постановления Кабинета Министров «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате кабинета министров, органах государственного и хозяйственного управления, государственной власти на местах»
4. Правила электронного документооборота государственный органов управления и власти Республики Узбекистан.

Закон Республики Узбекистан «Об электронной цифровой подписи» был принят в 11 декабре 2003 года [2], он определяет необходимую юридическую структуру, который станет фундаментом для создания электронного документооборота. В нем указаны значения ключевых слов, как электронная цифровая подпись, открытый и закрытый ключ, а также

дано, объяснение структуры взаимодействия ответственных организации за применение цифровой подписи.

Закон Республики Узбекистан «Об электронном документообороте» был принят в 29 апреля 2004 года [3]. В Законе определен государственная политика Республики Узбекистан в области электронного документооборота, свойства и назначение электронного документа, и юридическая сила электронного документа. Также указано правила обращения и обмена электронными документами.

Таким образом, к настоящему моменту созданы благоприятные условия разработки стратегии внедрение электронного документооборота в органы государственной власти и управления. Вышеуказанные нормативные документы представляют основные принципы и стандарты использования ИКТ в деятельности государственных органов, освещают международную практику решения этой проблемы, предлагают собственные оценки ряда систем электронного документооборота в соответствии с предварительно выработанными требованиями к таким системам.

2. Анализ достоинств и недостатков систем электронного документооборота

Электронный документооборот имеет своих достоинств и недостатков, так называемых «плюсов» и «минусы» в использовании на производственной практике.

Взвесить «всё за и против» внедрения системы электронного документооборота предприятий, это очень важная часть при планировании структуры предприятия и типа ее документооборота. Хотя многие руководители не уделяют достаточного внимания вопросу автоматизации документооборота и бизнес-процессов в целом, которые не осведомлены о преимуществах электронного документооборота.

Основные достоинства электронного документооборота проявляется в том, что при его использовании на всех подразделениях и структурах предприятия будут работать в одном информационном пространстве. В связи с этим, очень сильно возрастает скорость обработки документов внутри предприятия. Также, немаловажным фактором, ставящий электронный документооборот на порядок выше обычного, является сохранность и безопасность документов. В современных системах используется шифрования данных, которое помогает при пресечений попытки создания утечки информации. При использований такого типа документооборота, возрастает производительность сотрудников и снижается вероятность ошибок в обработке документов, которая зависит от квалификации работника. Внедрение системы электронного документооборота дает значительный экономический эффект, однако количественная его оценка является сложным процессом, т.к. приходится учитывать множество факторов.

Прямой эффект от внедрения системы позволяет экономить финансовые средства, затрачиваемые на расходные материалы, оплату служб почтовой и курьерской доставки, копирования материалов, уменьшает трудозатраты. Косвенным эффектом являются преимущества управления, которые значимы для функционирования организаций: прозрачность управления, контроль исполнительской дисциплины, возможность протоколирования действий и другие. Внедрение систем электронного документооборота позволяет[13]:

1. Полностью автоматизировать процесс работы с документами;
2. Обеспечить работы организаций с удаленными пользователями и группами пользователей;
3. Обеспечить интеграцию с внешними системами электронной почты;

4. Наращивать базовые возможности системы электронного документооборота с помощью модульности и наличия встроенных инструментальных средств;

5. Обеспечить процесс одновременной работы в системе неограниченного числа пользователей;

6. Повысить эффективность работы с документами;

7. Значительно уменьшить объемы бумажного документооборота;

8. Значительно сократить время на обработку и пересылку документов, время поиска документов, время согласования и утверждения проектов документов;

9. Упорядочить процесс регистрации всех видов документов (регистрация из электронной почты и web-форм, поддержка потокового сканирования, регистрация файлов любого формата);

10. Обеспечить управления потоками делопроизводства (передача документов между исполнителями);

11. Обеспечить процесс работы с взаимосвязанными документами;

12. Обеспечить управления документом на протяжении всего жизненного цикла;

13. Обеспечить прозрачность всех процессов с момента создания документа до момента его сдачи в архив;

14. Сохранение истории работы с документами (учет времени и авторов, всех действий с документом, сохранение рабочих комментариев, поддержка версионности присоединенных файлов);

15. Обеспечить четкий процесс согласования и утверждения документов;

16. Выстроить отлаженную систему поручений;

17. Производить сортировку документов по любым критериям;

18. Обеспечить поиск информации по различным атрибутам и полнотекстовый поиск;

19. Обеспечить автоматизацию сбора и анализа статистических данных о движении документов;

20. Обеспечить архивное хранение электронных образов документов;

21. Обеспечить регламентацию прав доступа;

22. Увеличить производительность труда;

23. Обеспечить ведение информационно-справочной базы;

24. Поддержка маршрутов движения документов (последовательные, параллельные, свободные маршруты, маршруты с условиями, отсрочки)

25. Поддержка смешанного документооборота (подготовка бумажных документов и отчетов по шаблонам, вывод на печать регистрационной карточки документа, учет места хранения оригиналов документов);

26. Наличие инструментов для анализа документооборота, создания отчетов, а также контроля исполнительской дисциплины сотрудников (возможность построения отчетов и аналитических справок, автоматическое ведение журналов);

27. Обеспечение информационной безопасности (поддержка электронно-цифровой подписи, шифрования данных, протоколирования, разграничения прав доступа и системы ролей, наличие встроенных средств контроля целостности данных и автоматического резервного копирования).

Но при всех достоинствах системы электронного документооборота, она имеет свои недостатки. Их стоит брать во внимание при принятии решений о внедрении систем электронного документооборота. Если предприятия внедряет систему электронного документооборота с самого своего основания, то трудностей у сотрудников оно не вызовет. А если решение принимает предприятия, у которой уже достаточно долгое время действует обычный документооборот, то нужно принимать во внимание то, что реформирование системы может вызвать ряд трудностей у сотрудников. Все новое, принимается с трудностями. Также, нужно

принять во внимание тот факт, что предприятия может понести затраты на приобретение программ и систем документооборота, а также на их внедрение и дальнейшее обслуживание[14].

Также существуют пробелы в информационной безопасности. Недобросовестному конкуренту получить информацию, размещенную на бумажных носителях, сложнее: документы могут храниться в разных помещениях, шкафах (столах, сейфах), разрозненных папках. С электронными базами данных проще. Современные злоумышленники посредством удаленного доступа взламывают дорогостоящие программы с высочайшей степенью защиты.

Следующий недостаток это резкое увеличение потока документооборота. Как результат – серверы не справляются, падает производительность труда. При наличии бумажного документооборота такой резкий рывок невозможен.

И еще один недостаток – это увеличение трудозатрат как следствие увеличения документооборота. Работодатель не успевает адекватно реагировать на подобные скачки в принятии решений по кадровым вопросам. Объемы возрастают, тогда, как штатный состав остается прежним.

После рассмотрения системы электронного документооборота можно сделать вывод, что оно имеет своих достоинств и недостатков и внедрение её внутри предприятий зависит от руководителя.

3. Классификация основных угроз информации в системах электронного документооборота

Угрозы СЭД можно сгруппировать по нарушаемым свойствам безопасности, к которым относятся[27].

- угроза конфиденциальности;
- угроза целостности;

- угроза доступности.

В целом СЭД включает в себя три типа компонентов:

1. Серверы.

2. Рабочие места.

3. Каналы связи.

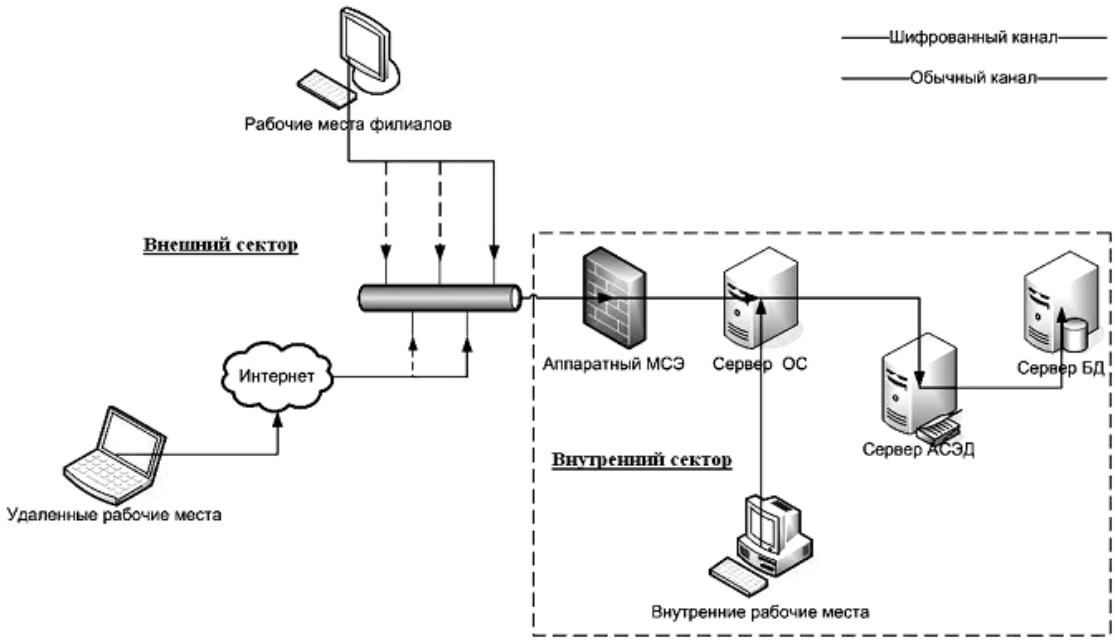

Рис. 1. Общая модель СЭД

Угрозы конфиденциальности – это угрозы несанкционированного доступа и ознакомления с учетом тонких политик безопасности СЭД[25]. По вышеописанной модели (рис. 1) можно составить список угроз новых способов несанкционированного доступа к СЭД, целью которых является нарушение конфиденциальности хранимой информации. К данным нарушениям относятся:

1. *Угроза рабочих мест* (внутренних, удаленных и филиалов) – это непосредственно физический доступ к ЭВМ, когда нарушитель уже имеет данные идентификации (логин и пароль, сертификат защищенного протокола HTTPS) законно зарегистрированного пользователя или администратора СЭД. Данный вид угрозы позволяет получить доступ к

документам пользователя, у которого были похищены данные идентификации. В случае хищения данных идентификации администратора СЭД возможно получение злоумышленником доступа ко всем документам СЭД.

2. *Угроза сервера ОС* – получение доступа к серверу ОС позволит загружать в память сервера вредоносные программы (вирусы, программы-шпионы), которые могут существенно облегчить взлом СЭД. При получении злоумышленником доступа к серверу ОС он может создать новое незаконное рабочее место СЭД, подменить законное рабочее место на незаконное, имитировать законное рабочее место, получить доступ к базы данных (БД) СЭД, получить частичный или полный контроль над сервером СЭД.

3. *Угроза сервера автоматизированной СЭД* – получение доступа к серверу автоматизированной СЭД может позволить злоумышленнику подключиться напрямую к СЭД, минуя сервер ОС и тем самым минуя основную систему безопасности, которую и обеспечивает сервер ОС. При подключении злоумышленником своего рабочего места последствия аналогичны последствиям угрозы рабочих мест.

4. *Угроза сервера БД* – получение доступа к серверу БД позволит злоумышленнику получить частичный или полный контроль над СЭД, а также к хранящимся документам. Данный вид угрозы наиболее опасен, т. к. в БД хранятся все документы, которые составляют основную ценность как для владельца СЭД, так и для заинтересованного злоумышленника.

5. *Угроза каналов связи* между компонентами системы может позволить злоумышленнику перехватывать пакеты между рабочими местами и основными серверами системы путем подключения к каналу связи. Использование шифрованного протокола HTTPS может значительно усложнить попытки перехвата пакетов.

Угрозы целостности – угрозы, при реализации которых информация теряет заранее определенные системой вид и качество[25]. На рис. 2

изображена схема степени ценности компонентов СЭД с точки зрения обеспечения целостности хранимой информации.

В СЭД объектами данной угрозы могут быть все компоненты описанной выше общей модели СЭД.

Документы – данные, хранящиеся на сервере БД, резервные копии документов. Это звено является самым важным и ценным, т. к. именно сами документы содержат конфиденциальную информацию, для безопасности которой организована вся система политики безопасности автоматизированной СЭД.

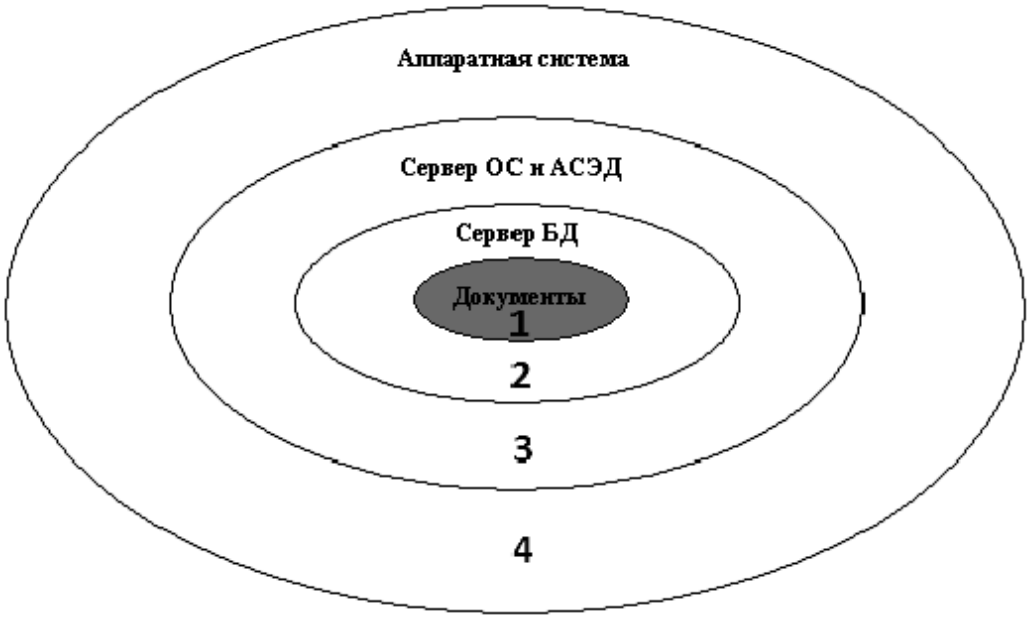

Рис. 2. Степень ценности компонентов СЭД

Степень ценности данного компонента охвачена сектором, отмеченным номером 1.

Сервер БД – среда хранения электронных документов. Целостность сервера БД является второй по значимости после целостности документов – сектор 2.

Сервер ОС и автоматизированной СЭД – операционная система и интерфейсная часть (оболочка) СЭД, установленные на серверах и рабочих станциях, включая клиентов СУБД; протоколы передачи данных;

криптографические методы обеспечения безопасности. Безопасность данных компонентов не столь критична, т. к. при их выходе из строя целостность хранимой информации (документов) не будет нарушена. Следует также учесть, что при внештатных ситуациях в рамках этих компонентов частично или полностью могут быть нарушены транзакции информации внутри СЭД. Компоненты отнесены к сектору под номером 3.

Аппаратная система – каналы связи между компонентами, аппаратный межсетевой экран – сектор с номером 4. Выход из строя аппаратных комплектующих и коммуникационных проводов не приведет к разрушению хранимых документов, а неисправные комплектующие и провода можно заменить на новые.

Угрозы доступности – характеризуют возможность доступа к хранимой и обрабатываемой в СЭД информации в любой момент [25]. Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих компоненты СЭД.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники(таковы обычно ошибки администрирования).

Используя халатное отношение при работе удаленного пользователя, злоумышленник может реализовать несанкционированный доступ. Доступность же коммуникационных каналов во внешнем секторе СЭД (см. рис. 1) может привести к перехвату злоумышленником информационных пакетов.

4. Методы и средства защиты информации в системах электронного документооборота

Существующие методы и средства защиты информации систем электронной документооборота можно подразделить на четыре основные группы:

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

Методы и средства организационно-правовой защиты информации

К методам и средствам организационной защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации СЭД для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться сервер СЭД; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности СЭД.

На этом уровне защиты информации рассматриваются международные договоры, подзаконные акты государства, государственные стандарты и локальные нормативные акты конкретной организации [7].

Методы и средства инженерно-технической защиты

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

- защиту территории и помещений, где стоит СЭД, от проникновения нарушителей;
- защиту аппаратных средств ЭДО и носителей информации от хищения;
- предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств ЭДО;
- предотвращение возможности перехвата ПЭМИН (побочных электромагнитных излучений и наводок), вызванных работающими техническими средствами компьютерной системы и линиями передачи данных;
- контроль над режимом работы персонала, обеспечивающего работу СЭД;

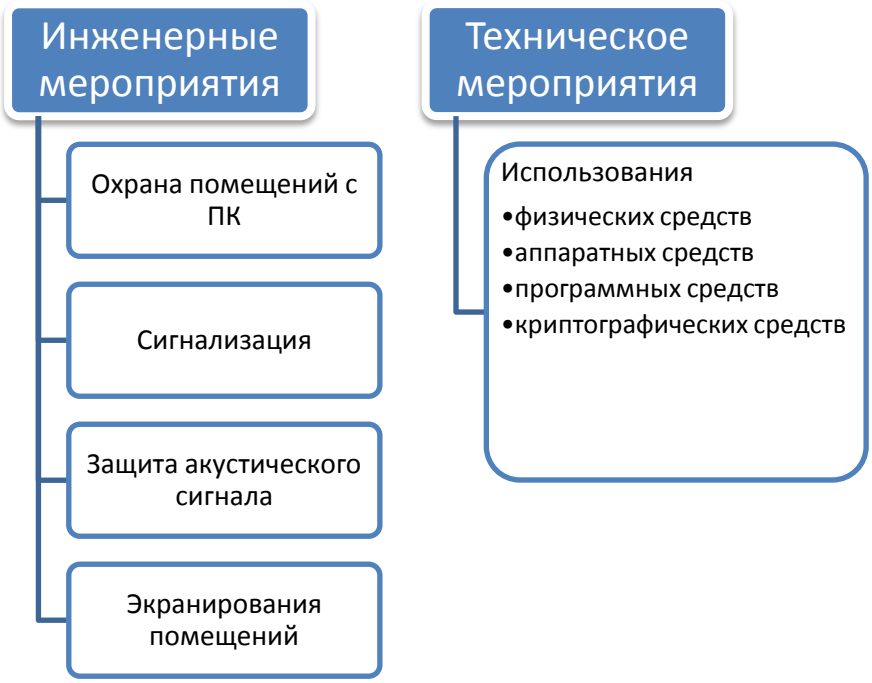

Рис.3 Инженерно-техническая защита

- противопожарную защиту помещений СЭД;
- минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий [15].

Криптографические методы защиты и шифрование

Шифрование является основным средством обеспечения конфиденциальности. Так, в случае обеспечения конфиденциальности данных на локальном компьютере применяют шифрование этих данных, а в случае сетевого взаимодействия - шифрованные каналы передачи данных.

Науку о защите информации с помощью шифрования называют криптографией (криптография в переводе означает загадочное письмо или тайнопись).

Криптография применяется:

- для защиты конфиденциальности информации, передаваемой по открытым каналам связи;
- для аутентификации (подтверждения подлинности) передаваемой информации;
- для защиты конфиденциальной информации при ее хранении на открытых носителях;
- для обеспечения целостности информации (защите информации от внесения несанкционированных изменений) при ее передаче по открытым каналам связи или хранении на открытых носителях;
- для обеспечения неоспоримости передаваемой по сети информации (предотвращения возможного отрицания факта отправки сообщения);
- для защиты программного обеспечения и других информационных ресурсов от несанкционированного использования и копирования [16].

Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств СЭД и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств СЭД.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения СЭД исключительно для выполнения защитных функций. К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей СЭД;
- программы разграничения доступа пользователей к ресурсам СЭД;
- программы шифрования информации;

программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования [17].

Методы идентификации и аутентификации

Под идентификацией, применительно к обеспечению информационной безопасности СЭД, понимают однозначное распознавание уникального имени субъекта СЭД. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

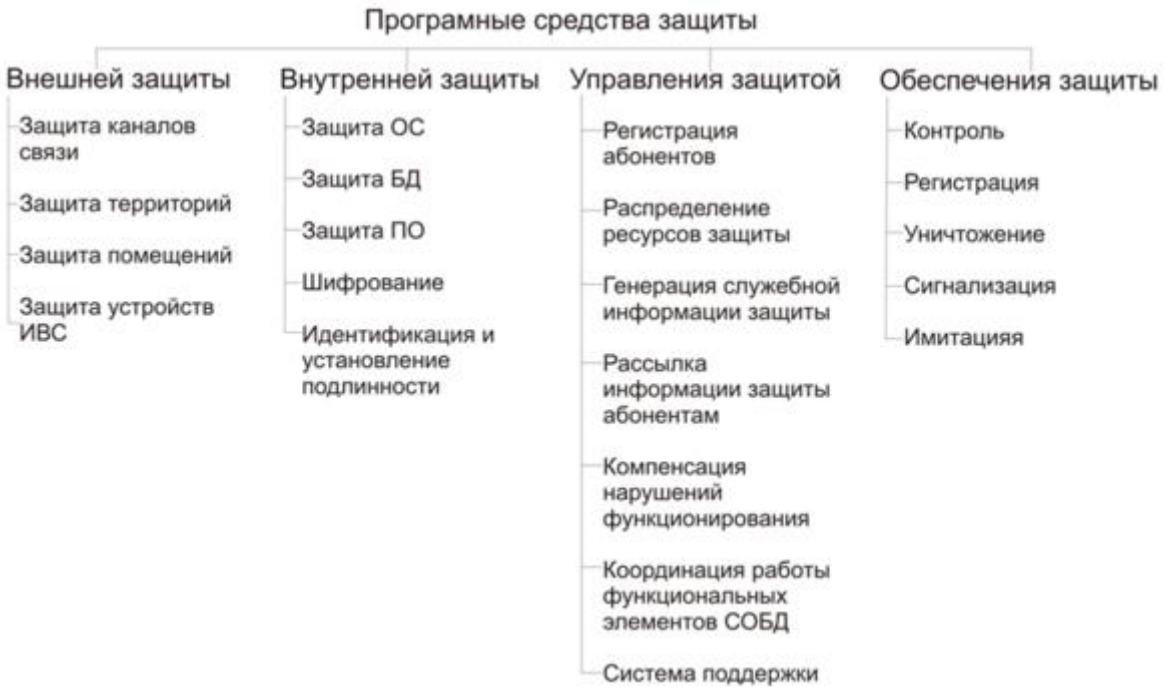

Рис.4 Программные средства защиты

Системы идентификации и аутентификации можно разделить следующим образом:

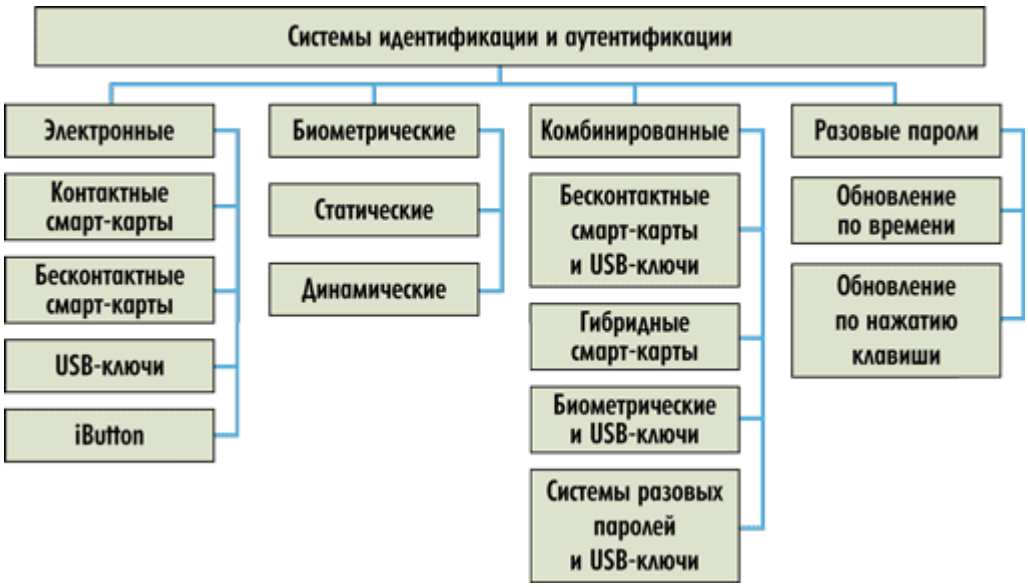

Рис. 5 Системы идентификации и аутентификации

Парольная аутентификация

Самый распространённый способ аутентификации – парольный. Однако слабая парольная защита не удовлетворяет современному уровню требований информационной безопасности. Надежность этого способа

аутентификации в значительной степени зависит от человеческого фактора, то есть от того, насколько качественные ключевые слова будут выбирать пользователи и насколько серьезно они будут относиться к их хранению. Часто сотрудники стараются упростить свою жизнь, нарушая при этом правила безопасности, и фактически, подчас сами того не сознавая, открывают злоумышленникам дорогу к коммерческой информации компании.

Аутентификация на основе ключей ЭЦП

Аутентификация пользователя должна производиться при его доступе в СЭД на основе его логина и пароля, а также секретного ключа ЭЦП пользователя.

При проверке ЭЦП пользователя СЭД, предъявляемой для его аутентификации, должны проверяться:

- соответствие открытого ключа закрытому ключу ЭЦП пользователя;
- действительность сертификата открытого ключа ЭЦП на момент аутентификации;
- проверка статуса сертификата открытого ключа ЭЦП в Центре регистрации ключей ЭЦП.

В случае истечения срока действия сертификата открытого ключа ЭЦП, приостановления его действия или аннулирования в Центре регистрации ключей ЭЦП, доступ к системе пользователя должен автоматически становиться невозможным.

Усиленная аутентификация

Усиленная аутентификация представляет собой аутентификацию с использованием дополнительных аппаратных средств - USB-устройств и смарт-карт. Они представляют собой средства усиленной двухфакторной аутентификации на основе цифровых сертификатов стандарта X.509.

Данные средства обеспечивают единую регистрацию пользователя и устраняют необходимость дополнительной регистрации в каждом из используемых приложений [11].

Выводы по главе I

В результате исследования рассмотрено нормативное-правовое основание ведения делопроизводства и электронного документооборота в Республике Узбекистан. В ходе исследования определилось, что нормативно-правовое база по данной отрасли развивается поэтапно. Были проанализированы достоинства и недостатки систем электронного документооборота. Изучены угрозы информации в системах электронного документооборота. Поставлены задачи: исследование путей оптимизации защиты систем электронного документооборота и изучение международного опыта по усовершенствованию информационной защищённости систем электронного документооборота.

Глава 2. Исследование возможных путей оптимизации защиты систем электронного документооборота

1. Общие требования к безопасности систем электронного документооборота

Требование к безопасности систем электронного документооборота ставятся с точки зрения, что он тоже является одним из типов информационной системы. Но отличительными из этих требований является, такие как:

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

Работа в системе начинается с аутентификации пользователя. Этот этап является одним из самой защищаемой операцией в системе. Механизмов аутентификаций можно условно разделит на три нижеследующие большие группы[18]:

- Знание – то, что знает пользователь;
- Владение – то, что владет пользователь;
- Биометрика – то, что он есть.

Аутентификация знанием — это самый обычный механизм аутентификации, к таким относится авторизация с помощью логином и паролем.

Владение — уже более продвинутый уровень безопасности, так как пользователь уже имеет физические возможности, чтобы следит за своим владением. Секретным владением может быт ключи электронные, так и физические. Обычно для быстрой взаимодействий с системы в качестве

владение бывает ключи электронной цифровой подписи (ЭЦП). Место хранение ключей могут быт файловой системой пользователя, или ещё безопаснее специальные устройства для хранения ключей ЭЦП (Э-калит, eToken, РуТокен) [19].

Использование ЭЦП в СЭД не только решает вопрос аутентификации, но и решает другие вопросы, которые связано с авторством и целостностью электронного документа, юридическую значимость документа, а также обеспечит безопасное хранение в случае шифрования с использованием криптографических алгоритмов.

Вышеуказанные требований должны быть обеспечены в каждой системе, которые претендуют на звание СЭД. Но также существуют дополнительные требования, которые после выполнения всех нижеследующих требований СЭД, имеет дополнительные преимущества защищённости по сравнение другими. Для организации защищенной СЭД необходимо использовать механизмы, обеспечивающие[28]:

- контроль целостности используемого программного обеспечения;
- регистрацию событий в информационных системах;
- криптографическую защиту;
- межсетевая экранирования;
- виртуальные частные сети;
- антивирусную защиту;
- аудит информационной безопасности,

которые хорошо известны специалистам по защите информации.

Контроль целостности используемого программного обеспечения

Контроль целостности используемого программного обеспечения проверяется с помощью сравнивание параметров рабочих файлов программы с ранее указанными параметрами. В качестве параметров

берутся хеш-функция от исполняемых файлов. Выбор хеш-функции зависит от того, что насколько быстро и безопасно надо вычислит значение этой функции.

Регистрацию событий в системе

Протоколирование действий пользователя обеспечит своевременное определение действий выполняемые внутри системы. Реализация такой функции повышает ответственность пользователей и помогает быстро найти «зло умышленно» действующего пользователя.

Криптографическая защита

Криптографическая защита информации одно из задач которое решается с помощью ключей ЭЦП. Но стоит учитывать, что инфраструктура электронной подписи состоит из массы компонентов. Даже если брать в расчет только техническую сторону, это и средства криптографической защиты информации (СКЗИ), включая аппаратные средства, крипто-провайдеры, протоколы.

Межсетевое экранирование

Межсетевое экранирование помогает в ограничении доступа к СЭД. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации[20].

2. Зарубежный опыт защиты систем электронного документооборота

Широкомасштабное использование информационных технологий в делопроизводстве привел разработку соответствующих стандартов на международном уровне. Требовании к систем управления электронными документами разрабатывается в основном в интересах государственных органов, чтобы определить единый подход к обмену документами в межведомственным уровне. Но в тоже время этими требованиями пользуется другие организации, для проведения своих закупок, выбирая из них нужные им положения.

Можно сказать, что в 2007–2008 гг. стали появляться требования к СЭД третьего поколения начиная с третьей редакции известного американского стандарта DoD 5015.2. Наиболее заметным событием стал выход в свет в феврале 2008 года европейских требований MoReq2, разработанных по заказу Еврокомиссии (правительства Евросоюза).

Таблица 1 - Основные национальные стандарты СЭД[21]

Стандарт	Страна	Сфера регуляции
DoD 5015.2-STD версия 3	США	Стандарт требований к разработке программных приложений для управления электронными документами; необходимость закупки только сертифицированных продуктов; распределение полномочий и ответственности в СЭД
MoReq2	страны ЕС	Типовые требования к автоматизированным системам электронного документооборота
NoARK-5	Норвегия	Национальные требования Норвегии к управлению электронными документами и их архивации
PROS 99/007 версия 2 (VERS)	Австралия	Управление электронными документами; содержит требования к хранилищам документов
концепция DOMEA	Германия	Управление документами и электронная архивация в ИТ-системах; речь идет об обеспечении максимальной степени юзабилити/эргономики, "прописаны" механизмы ввода документов на бумажных носителях в систему электронного документооборота
концепция ELAK	Австрия	"Электронное дело"; содержит полномасштабный набор требований к электронному управлению документами (более 800 требований, которые охватывают сферы управления информацией и документами, управление рабочими процессами – workflow, а также архивирование)

Новой тенденцией стало появление требований к минимальному набору функциональных возможностей для управления документами, необходимому для деловых систем (учетных, управления ресурсами и бизнес-процессами и т.п.) – в отличие от требований к полномасштабным специализированным системам для управления документами.

Стандарт DoD 5015.2-STD появился в Министерстве обороны США еще в 1996 году и был первым в этой группе стандартов. Его успех стал серьезным стимулом для разработки аналогичных норм в других странах мира, особенно в Европе.

В 2007 г. появилась третья версия стандарта. Стандарт дополнен двумя разделами, посвященными требованиям к тем функциональным возможностям систем управления документами, которые необходимы для исполнения государственными органами положений законов о защите персональных данных и доступе к государственной информации. Это, в первую очередь, дало следующее возможности:

- выделять документы, содержащие персональные данные и/или подлежащие раскрытию по закону о свободе доступа к государственной информации;
- регистрировать запросы граждан относительно своих персональных данных, а также запросы граждан и организаций о доступе к государственной информации; формировать соответствующие электронные досье, содержащие документы, создаваемые в ходе отработки этих запросов;
- управлять документацией по вопросам раскрытия персональной и государственной информации;
- собирать необходимые статистические данные и формировать соответствующие отчеты;
- поддерживать создание цензурированных версий раскрываемых документов и их хранение в связке с оригинальными документами.

Стандарт, кроме того, включает теперь раздел с требованиями по обеспечению взаимодействия между СЭД при передаче электронных документов из одной системы в другую. Существенно доработан и дополнен раздел об управлении электронными секретными документами, а также информацией, содержащей сведения, отнесенные к государственной тайне.

Спецификации MoReq2.

MoReq2 – это вторая версия Типовых требований (Model Requirements, MoReq), которая является новым европейским «де-факто» стандартом для систем, управляющих электронными документами.

MoReq2 уже сейчас весьма влиятелен в области управления электронными документами, и это влияние, как ожидается, в будущем будет только возрастать. Причины этого кроются в следующем:

- он предназначен для всех секторов, а не только для государственных органов;
- это международный стандарт, используемый во всей Европе, а также в Азии, Северной и Южной Америке;
- он описывает функциональные возможности, выходящие далеко за пределы собственно управления документами;
- в ходе его разработки было организовано огромное по масштабам международное обсуждение проекта специалистами из многих стран мира.

В стандарте переработаны и дополнены те разделы, которые в последнее время приобрели наибольшее значение. Добавлены четко сформулированные требования в отношении новых важных аспектов разработки и применения СЭД. Требования разделены на модули, с тем, чтобы облегчить использование стандартов. Обеспечена проверяемость требований, разработаны необходимые документы и материалы, позволяющие проводить тестирование систем управления документами на соответствие требованиям MoReq2.

NOARK-5

Национальные требования Норвегии к управлению электронными документами и их архивации NOARK-5. Несмотря на успех европейского стандарта MoReq/MoReq2 ряд европейских стран разрабатывает свои национальные требования к СЭД и регулярно их обновляет. Чаще всего это связано с тем, что в данных странах есть особенности в области управления документами, которые необходимо учесть при разработке СЭД. Примером является Норвегия, продолжающая развивать собственный стандарт NOARK.

В 2008 г. Национальные Архивы Норвегии опубликовали новую редакцию требований к управлению и архивации электронных документов NOARK-5, которая заменит применявшийся ранее стандарт NOARK-4.

NOARK-5 должен использоваться во всех архивных органах, независимо от их типа и используемого технологического решения. Решение, обеспечивающее формирование архивов, должно охватывать все виды деятельности, в ходе которых создаются документы, которые необходимо сохранить в аутентичном виде. Требования NOARK-5 не зависят от того, относится организация к государственному или частному сектору, обрабатываются ли документы традиционным образом, каков их срок хранения и будут ли они передаваться на архивное хранение.

Комплект документов (в норвежской версии) включает[21]:

- Собственно требования NOARK-5: Стандарт электронной архивации, версия 1.2 от 17 октября 2008 г. (Standard for elektronisk arkiv);
- Приложение 1: Каталог метаданных;
- Приложение 2: Метаданные, сгруппированные по их назначению;
- Приложение 3: XML-схема для использования при передаче документов.

Стандарт разработан с позиций целостного подхода к архивному хранению документов в электронной среде. Основное внимание было уделено разработке требований, нацеленных на то, чтобы создаваемые решения обеспечивали должное управление электронными документами и архивами.

В NOARK-5 предусмотрены три уровня требований: ключевые требования («ядро»), расширения «ядра» и требования к полномасштабным реализациям NOARK-5. Решения, основанные на «ядре» NOARK-5, используются для обеспечения надлежащей регистрации документов, и они могут также использоваться для управления электронными документами в организациях частного сектора Норвегии. NOARK-5 заменяет NOARK-4, при этом предусмотрена «обратная совместимость» с NOARK-4, т.е. будет возможна миграция документов из систем, основанных на ранее действовавшем стандарте, в новые системы. Это учтено при разработке как структуры электронного архива, так и метаданных. Системы, используемые для приема государственных документов в электронном виде, должны отвечать соответствующим требованиям NOARK-5 и должны быть одобрены для этой цели руководителем архивной службы страны. Они публикуются на сайте Национальных Архивов (первая версия NOARK-5 была опубликована 4 июля 2008 г.).

Интересен норвежский стандарт тем, что он учитывает особенности норвежской регистрационной системы делопроизводства, напоминающей российскую, но только еще более сложную, и особенности делопроизводства коллегиальных органов.

3. Проблемы распределения и хранения цифровых ключей

Согласно статье номер 11 по закону «Об электронной цифровой подписи», владелец закрытого ключа электронной цифровой подписи

несет ответственность перед пользователем соответствующего открытого ключа электронной цифровой подписи за убытки, причиненные несанкционированным использованием закрытого ключа электронной цифровой подписи[2].

Одной из проблем при использовании электронной подписи является возможность ее подделки. В своей работе Гольдвассер, Микали и Ривест описывают следующие модели фальсификации электронной подписи, которые актуальны и в настоящее время[22]:

- атака с использованием открытого ключа. Криптоаналитик обладает только открытым ключом;
- атака на основе известных сообщений. Противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им;
- адаптивная атака на основе выбранных сообщений.

Задача защиты ключей от подмены решается с помощью сертификатов. В соответствии со статьей 13 закона «Об электронной цифровой подписи» сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица.

Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями.

Согласно статье 6 закона «Об электронной цифровой подписи» Центр регистрации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзыв истекших и компрометированных сертификатов и ведет базы выданных и

отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

Закрытый ключ является наиболее уязвимым компонентом всей криптосистемы цифровой подписи. Злоумышленник, укравший закрытый ключ пользователя, может создать действительную цифровую подпись любого электронного документа от лица этого пользователя. Поэтому особое внимание нужно уделять способу хранения закрытого ключа.

Пользователь может хранить закрытый ключ на своем персональном компьютере, защитив его с помощью пароля. Однако такой способ хранения имеет ряд недостатков, в частности, защищенность ключа полностью зависит от защищенности компьютера, и пользователь может подписывать документы только на этом компьютере.

В настоящее время существуют следующие устройства хранения закрытого ключа:

- флеш-накопитель;
- смарт-карты;
- usb-брелоки,
- таблетки Touch-Memory.

Самый обычный вариант хранение закрытого ключа, является храние на переносном носителе информации. В этом случаи самая больщая вероятность использования носителя информации в других целях, и это может привести к возможной порчи или кражи кляча.

Смарт-карты (англ. smart card) — пластиковые карты со встроенной микросхемой (англ. integrated circuit card, ICC — карта с интегрированными электронными цепями). В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления. Назначение смарт-карт — одно- и

двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.

USB-брелок — это миниатюрное USB-устройство, зачастую выполненное в виде брелока (за что и получило своё название), которое может применяться для различных целей. К USB-брелокам можно отнести, и средства аутентификации, таких как eToken, iKey, RuToken, «Шипка», Kaztoken и ещё национальный продукт от ГУП UNICON.UZ - «Э-калит».

Контактная память (от англ. touch memory иногда встречается англ. contact memory или англ. iButton) — класс электронных устройств, имеющих однопроводный протокол обмена информацией между ними (1-Wire), и помещённых в стандартный металлический корпус (обычно имеющий вид «таблетки»). Металлический корпус служит для защиты находящихся внутри микросхем. Внутри может использоваться достаточно разнообразная электроника от однократно-записываемой и флэш-памяти, до всевозможных контроллеров, таймеров, датчиков температуры и т.п. Устройство активизируется в момент контакта со считывателем. Операции чтения и записи осуществляются практически мгновенно во время контакта. В простейшем случае это просто энергонезависимая память, размещаемая в металлическом корпусе. Небольшой размер позволяет прикреплять контактную память практически на любом носителе — изделии, карточке, брелоке.

Кража или потеря одного из таких устройств может быть легко замечена пользователем, после чего соответствующий сертификат может быть немедленно отозван.

Для повышения защищенности хранения закрытого ключа реализуется двухфакторная авторизация. То есть, до считывания устройства вводится пароль доступа. Но также имеется опасность программного перехвата вводимого пароля и по этой причине

рекомендуется дополнительного включения аппаратных кнопок для ввода пароля.

Электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью право имеющегося лица и скрепленного печатью.

Таким образом, электронная подпись - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Использование ЭЦП позволит:

значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;

усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;

гарантировать достоверность документации;

минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

построить корпоративную систему обмена документами.

4. Криптографические методы обеспечения защиты при сетевом обмене данными

Для эффективной передачи данных по глобальным широкополосным сетям или непосредственно от локальной сети (LAN) превосходно подходит технология Ethernet. В ней данные передаются данные от LAN по оптоволоконным сетям (MAN) в глобальные сети (WAN) без смены протокола - и расстояния практически не играют уже никакой роли.

Ethernet в состоянии передавать все распространенные приложения вперемешку и одновременно. Внедренный каскад расширения позволяет достигать трафика в 10 Гб/сек. Поэтому Ethernet вызывает оправданный интерес также для передачи данных в режиме реального времени у пользователей оборонного сектора (сети C4ISTAR с широким резервированием), министерств (множество приложений вперемешку) или банков (постоянная готовность). Однако заботиться о защите данных во время передачи должны сами пользователи. Высокоскоростная сеть правительства, министерства или оборонной организации в любое время располагает ныне достаточной пропускной способностью, чтобы обеспечить пользователям бесперебойную работу на компьютерах и периферийных устройствах. Для преодоления расстояний в пределах стран и континентов сегодня и в глобальной сети (WAN) зачастую используются стекловолоконные технологии. Способность протокола Ethernet к одновременной передаче любых приложений независимо от размера сети и расстояний, при этом с почти неограниченной пропускной способностью, делает Ethernet еще более привлекательным для правительственных и оборонных организаций, равно как и для финансового сектора. Подкупает также возможность создавать не только соединения «от точки к точке», но и настоящие многоузловые конфигурации. Оптоволоконная технология эффективно использует по несколько длин волн на волокно (WDM). Если в кабеле имеется несколько коммутируемых стекловолокон, можно устраивать кольцевые сети с резервированием. Ethernet может обеспечить также высокую готовность и качество сервиса класс обслуживания.

Правительственные и оборонные организации, как и предприятия финансового сектора, ежедневно имеют дело с предельно «закрытыми» данными. В нарастающих объемах они пересылают по одним и тем же каналам смесь самых различных приложений - речь, сообщения, изображения, данные измерении, видеоконференции. Происходит это очень эффективно и экономно, но получается, что большие объемы

«закрытых» сведений оказываются сосредоточенными на немногих линиях передачи данных. Чтобы не снизить пропускную способность сети и сохранить полностью скорость передачи данных по кабелю, нужна отдельная, независимая от сети система шифрования с собственными аппаратно-программными средствами.

Задача остается актуальным с 1990-х годов. Многие компании предлагает свои решении задачи в виде отдельных аппаратных, программных или аппаратно-программных систем.

Один из аппаратных решений является Ethernet Encryption HC-8555 10G от Crypto AG. Она обеспечит защиту передаваемых данных/сведений из любого приложения по Ethernet-сетям LAN/MAN/WAN с наиболее высшей степенью защищенности. Пропускной способность аппарата 10 гигабит/сек на линиях «от точки-к точке», система не забирает дополнительных ресурсов. Время задержки информации системой мало. Периодическая смена ключей для соединений производится автоматически, в заданное время и без прерывания связи. Присутствия персонала при этом не требуется. Шифрование происходит „на заднем плане" - никому из пользователей тех или иных приложений не нужно особо заботиться.

Недостатки данного подхода: невозможно обслуживать только отдельных частей сетевых запросов, обязательное прямое подключение к другому типу устройств шифрования. Такая схема безопасности требует много аппаратных устройств и соответственно требует дополнительных затрат.

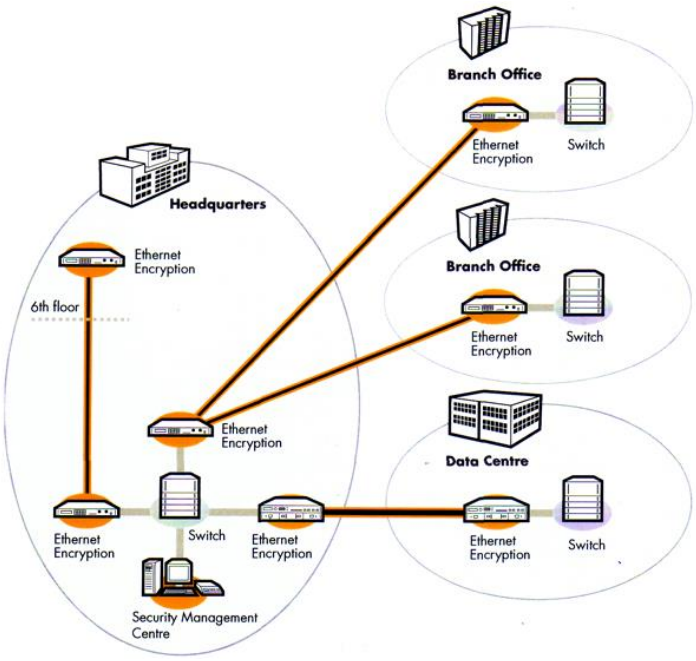

Рис 6. Решения обеспечения защиты Network Security для Ethernet

Рассмотрим программную реализацию обеспечения безопасности в сети. В этом сфере с 1994 года преимущественно используется открытый протокол HTTPS (HyperText Transfer Protocol Secured). Данный протокол был разработан компанией Netscape Communications для браузера Netscape Navigator. HTTPS широко используется в мире веб и поддерживается всеми популярными браузерами. Он не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы SSL и TLS. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от снифферских атак и атак типа man-in-the-middle при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют. Сертификат сервера стоит от 20 до 1000 долларов США. Клиенты для такого типа соединения ничего не платит. Так как браузеры на сегодняшний день распространяется бесплатно.

Последний тип обеспечения безопасности это аппаратно-программные комплексы. Рассмотрим в примере протокола openSAFETY от объединения Ethernet POWERLINK Standardization Group (EPSG).

Основные характеристики протокола openSAFETY включают гибкий телеграммный формат и инкапсуляцию данных, относящихся к безопасности. Узлы безопасности сети автоматически распознают содержание пакета данных, т. е. тип фрейма и длина не требуют конфигурирования. Протокол объединяет все функции безопасности на уровне openSAFETY. Его функции и сервисы включают программу-конфигуратор, управление сетью, словарь объектов, управление объектами, а также синхронизацию по времени. Так как openSAFETY использует только уровни модели OSI, ориентированные на приложения, он не зависит от используемого типа промышленной шины. Для получения всех преимуществ пользователь должен использовать только устройства безопасности, совместимые с openSAFETY. Такие устройства обычно стоит дороже чем другие аппараты такого типа. Поэтому реализация данного подхода может не являться экономически эффективным.

5. Анализ возможностей национальных криптографических алгоритмов, для создания защищенных систем электронного документооборота.

Для эффективного обеспечения защиты информации в системах электронного документооборота необходимо использовать соответствующее нормативное обеспечение. В этом направлении в рамках работы ГУП «UNICON.UZ» разработаны следующие нормативные документы:

1. O‘zDSt 2295:2011 «Электронный документ. Требования к формированию, применению и хранению»

2. O‘zDSt 2298:2011 «Информационная технология. Электронный документооборот. Типовые требования»

3. O‘zDSt 1108:2011 «Информационная технология. Взаимосвязь открытых систем. Структура сертификата открытого ключа ЭЦП и сертификата атрибута»

В Республике Узбекистан также разработаны алгоритмы криптографической защиты информации:

1. Алгоритм шифрования и имитозащиты - O'zDSt 1105:2009 "Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных".

2. Алгоритм хеширования - O'zDSt 1106:2009 "Информационная технология. Криптографическая защита информации. Функции хэширования".

3. Алгоритм электронной цифровой подписи - O'zDSt 1092:2009 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

Стандарт O‘zDSt 2295:2011 устанавливает общие требования к формату, составу и содержанию электронного документа, распространяется на электронные документы органов государственной власти и управления, хозяйствующих субъектов, функционирующих в Республике Узбекистан. Согласно данному стандарту подтверждение подлинности электронного документа есть процедура проверки целостности документа, действительности ЭЦП, а также соответствия ЭЦП владельца документа предъявленному имени.

Электронный документ является подлинным, если он:

a) подписан лицом, уполномоченным подписывать собственноручной подписью подобный документ на бумажном носителе;

b) подписан подлинной электронной цифровой подписью автора, указанного в документе;

c) подписанные документы должны подтверждаться печатью или штампом организаций.

Так как еще на законодательном уровне не имеется аналог печатей или штампов, в данной работе не рассмотрено и не исследовано в этом направлений.

Проверка подлинности электронного документа осуществляется согласно O‘zDSt 1092:2009 путем проверки подлинности цифровой подписи автора средствами в рамках алгоритма ЭЦП.

Защита электронных документов при электронном документообороте согласно O‘zDSt 2295:2011 осуществляется в целях предотвращения нанесения ущерба участникам электронного документооборота или иным лицам. Для предотвращения несанкционированных действий по отношению к электронным документам собственники, владельцы и пользователи электронного документа должны осуществлять организационные и технические мероприятия по защите электронного документа, а также защищать документ на программном уровне.

Электронный документ пользуется юридической защитой, равной защите аналогичного документа на бумажном носителе.

В O‘zDSt 2298 определены требования к построению, функционированию и обеспечению информационной безопасности системы электронного документооборота.

Стандарт O‘zDSt 1108 определяет основные требования к сертификату ключа ЭЦП [9-10].

Конфиденциальность данных при их обработке и передаче по каналам связи должна обеспечиваться путем шифрования данных с использованием СКЗИ. Шифрование данных на прикладном уровне должно обеспечивать защиту информации при ее хранении в базе данных, на клиентской части, а также при передаче по каналам связи [11].

На основе этих требований и стандартов разработано несколько криптографические модули. На сегодняшний день они используется для подписи и отправки налоговых и статических электронных отчетов

бухгалтерами различных организаций, а также большинством случаи, для систем документооборота, чтобы обеспечить защищённого хранение документов. Рассмотрим и анализируем нескольких криптографических модулей применяемых в системах электронного документооборота.

Для примера можно взят модуль ISCSP. ISCSP – это криптографический модуль, внедренный на веб-сервер Apache Server версии 2.0 или 2.2. Модуль обрабатывает HTTP запросы по специально заданному пути. Для генерации и проверки ЭЦП сгенерируется специальный запрос на заданный путь. Модуль, принимая запрос, сравнивает открытый ключ к своему списку открытых ключей (база в СУБД MySQL), и в случаи, если находиться операция генерации ЭЦП, проверка ЭЦП, или генерация хеш-значения продолжится. Тот же функции реализован на стороне клиента в виде ActiveX расширения. ActiveX плотно интегрировано браузеру Internet Explorer. Достоинство этого модуля кроссплатформенность серверной решении. Но клиентская часть программного модуля привязывает пользователя к браузеру Internet Explorer и операционных систем семейства Windows.

А также существует модули iSigner и iCrypter. Если их рассмотреть шире, iSigner – это серверная решения, привязанная языку программирования PHP. Такой подход сильно уменьшает расход времени, от программиста для интегрирования криптографического модуля не требуется профессиональных навыков. Клиентская часть тоже существенно улучшен за счет использования технологии NPAPI. NPAPI – это программный интерфейс подключаемых модулей Netscape (англ. Netscape Plugin Application Programming Interface, NPAPI - кроссплатформенная архитектура разработки плагинов, поддерживаемая многими браузерами. Интерфейс был разработан для семейства браузеров Netscape Navigator, начиная с Netscape Navigator 2.0 и в дальнейшим был реализован многими другими браузерами, включая все популярные на сегодняшний день. Достоинством криптографического модуля является

полное кроссплатформенность. Недостатком является привязанность серверной решении на языку программирования.

В свою очередь iCrypter представляет собой новый уровень криптографических модулей. Помимо стандартных функций с ЭЦП в этом модуле реализовано криптографические функции шифровании. Имеет тот же достоинства и недостатки как iSigner.

Выводы по главе II

В данной главе описаны требования к безопасности систем электронного документооборота, а также дополнительные требования к защищенным системам такого типа. Изучены зарубежные стандарты по организации электронного документооборота. Рассмотрены возможности обеспечения информационной безопасности в сети. Определены существующие проблемы безопасности организации безопасного соединения. Сделан вывод, что оптимальный вариант для создания собственной реализации безопасного соединения является программный метод обеспечения безопасности.

Глава 3. Разработка программного модуля для оптимизации защиты информации в системах электронного документооборота

1. Алгоритм программного модуля для защиты информации

Как было изучено сейчас наиболее уязвимая часть СЭД является обмен информаций в незащищенных сетях. Современные сети обмена данными состоят из многочисленных административных организаций и их аппаратными и программными обеспечениями, которые соединены между собой. Каждый элемент, подключенный к сети, свободно управляет данными, которые проходят через него. Он может прослушать, записать, изменить, или полностью блокировать соединения[23].

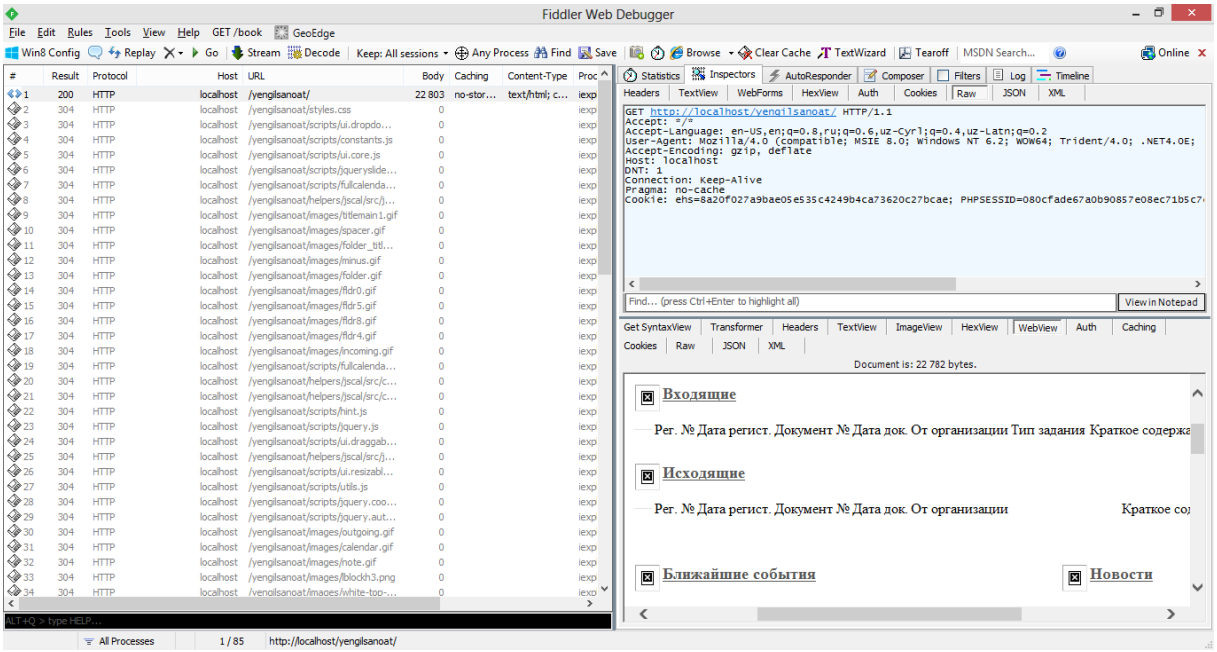

Рис 7. Пример прослушивания данных с помощью веб-сниффера

Учитывая, что обмениваемые данные могут быть частными, конфиденциальными или имеющими большую ценность, возникает вопрос: - как можно обеспечить конфиденциальность и целостность данных и как избежать утечки информации?

Рис 8. Стандартное открытое подключение.

В данной диссертационной работе предлагается использовать шифрующие и дешифрующие прокси-сервера для обеспечения безопасности обмена данными. Современный HTTP протокол настолько гибок, что теоретически можно бесконечно устанавливать промежуточные сервера и менять структуру данных, предварительно зафиксировав все на своих местах. Используя эту функцию, не трогая ни программу пользователя, ни сервера программы можно обеспечить пользователей шифрованным трафиком. Для обеспечения такого рода связи требуется шифратор-дешифратор прокси (ШДП) на стороне клиента и дешифратор-шифратор прокси (ДШП) на стороне сервера. Такая структура обеспечения информационной безопасности будет работать только в одностороннем порядке. Для двусторонней шифрования-дешифрования клиент прокси должен шифровать запрос и дешифровать ответ сервера, а сервер прокси должен дешифровать запрос и шифровать ответ сервера.

Рис 9. Защищенное подключение с помощью шифрующих прокси-серверов.

Шифруется вес запрос выходящей информаций от клиента и указывается метки о том, что трафик шифрован, далее трафик направляется к дешифратору, который расположен на стороне сервера.

Дешифратор определяет шифрованный траффик по указанным меткам, дешифруя траффик, направляет к реальному серверу. Далее происходить обратное шифрование в сервере и дешифрование в стороне клиента. Таким алгоритмом обмена информаций в сеть попадает только шифрованные данные. В качестве стандарта шифрования можно выбрать практический любой алгоритм симметричного шифрования, заранее определяя, какое шифрования будет использован. В текущей диссертационной работе было выбрано алгоритм симметричного шифрования AES (Rijndeal-128).

Advanced Encryption Standard (AES), также известный как Rijndael) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. Национальный институт стандартов и технологий США (англ. National Institute of Standards and Technology, NIST) опубликовал спецификацию AES 26 ноября 2001 года после пятилетнего периода, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования. По состоянию на 2009 год AES является одним из самых распространённых алгоритмов симметричного шифрования [24].

По сколку для уменьшения затраты времени было выбрано симметричный алгоритм шифрования, поднимается проблема обмена секретными ключами. Для обмена секретными ключами с популярности используется алгоритм Диффи — Хеллмана. Алгоритм Диффи — Хеллмана (англ. Diffie-Hellman, DH) позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищённый от подмены, канал связи.

Схема обмена ключами Диффи — Хеллмана, изобретённая в 1976 году при сотрудничестве Уитфилда Диффи и Мартина Хеллмана, под сильным влиянием работы Ральфа Меркля (Ralph Merkle) о системе

распространения публичных ключей, стала первым практическим методом для получения общего секретного ключа при общении через незащищенный канал связи.

Описание алгоритма Диффи — Хеллмана

Обоим абонентам известны некоторые два числа g и p (например, они могут быть «зашиты» в программное обеспечение), которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того чтобы создать, неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: первый абонент — число a, второй абонент — число b. Затем первый абонент вычисляет значение

$$A = g^a mod\ p$$

и пересылает его второму, а второй вычисляет

$$B = g^b mod\ p$$

и передаёт первому. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи). На втором этапе первый абонент на основе имеющегося у него $\boldsymbol{a}$ и полученного по сети $\boldsymbol{B}$ вычисляет значение:

$$B^a mod\ p = g^{ab} mod\ p,$$

а второй абонент на основе имеющегося у него b и полученного по сети $\boldsymbol{A}$ вычисляет значение:

$$A^b mod\ p = g^{ab} mod\ p.$$

Как нетрудно видеть, у обоих абонентов получилось одно и то же число:

$$K = g^{ab} mod\ p.$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой

(за разумное время) проблемой вычисления $g^{ab} mod\ p$ по перехваченным $g^{a} mod\ p$ и $g^{b} mod\ p$, если числа p,a,b выбраны достаточно большими.

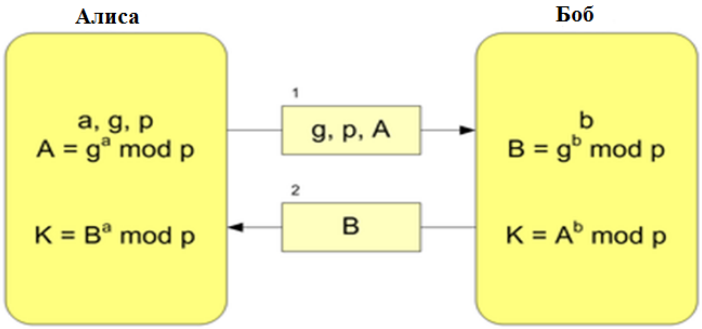

Рис 10. Пример использования алгоритма Диффи — Хеллмана, где K — итоговый общий секретный ключ.

В практических реализациях, для a и b используются числа порядка 10^{100} и p порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

Криптографическая стойкость алгоритма Диффи — Хеллмана (то есть, сложность вычисления $K = g^{ab} mod\ p$ по известным $p, g, A = g^{a} mod\ p$ и $B=g^{b} mod\ p$), основана на предполагаемой сложности проблемы дискретного логарифмирования. Однако, хотя умение решать проблему дискретного логарифмирования позволит взломать алгоритм Диффи — Хеллмана, обратное утверждение до сих является открытым вопросом (другими словами, эквивалентность этих проблем не доказана). Сложность данной задачи очень высока, но мощность компьютеров повышается очень быстро и возможность вычисления секретного ключа соответственно растет.

По этому, предлагается усовершенствованный алгоритм для обмена ключей, используя элементы параметрической алгебры[26]. Стандартное умножение и возведение в степень заменяется на параметрическое умножение и параметрическое возведение в степень соответственно.

Ниже приведены основные операции алгебры с параметром[25]:

1) Умножение с параметром **R**

a ® b (mod p) ≡ a+b*(1+R*a) (mod p);

2) Возведение в степень с параметром **R**

$a^{\backslash 37} \equiv a^{\backslash(32+4+1)}$ (mod p) ≡ (((((a\2)\2)\2)\2)®(a\2)\2) ® a (mod p),

где: **$a^{\backslash 2}$ (mod p) ≡ a*(2+R*a) (mod p) ;**

Здесь:

® - символ операции умножения с параметром **R,**

\ - символ операции возведения в степень с параметром **R,**

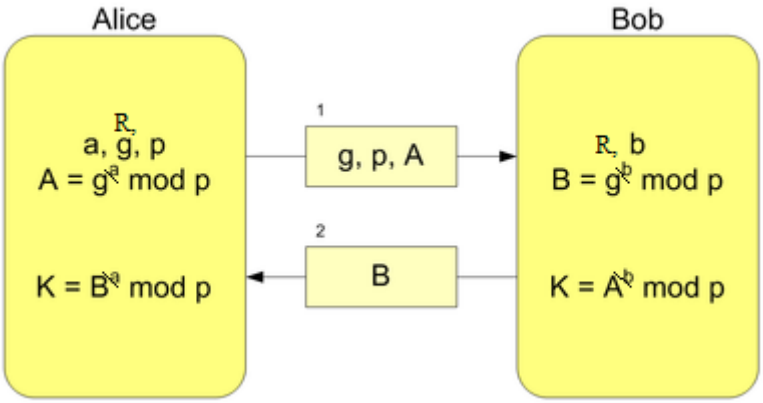

Рис 11. Улучшенный алгоритм Диффи-Хелмана

Использования параметрического возведения по степени, даже с ранее известным параметром намного уменьшает возможность нахождение секретного ключа с помощью современных алгоритмов криптоанализа. Например, для метода дискретного логарифмирования постановка задачи имеет особую сложность.

После решения проблемы обмена секретными ключами, можно рисовать всю схему обмена информации.

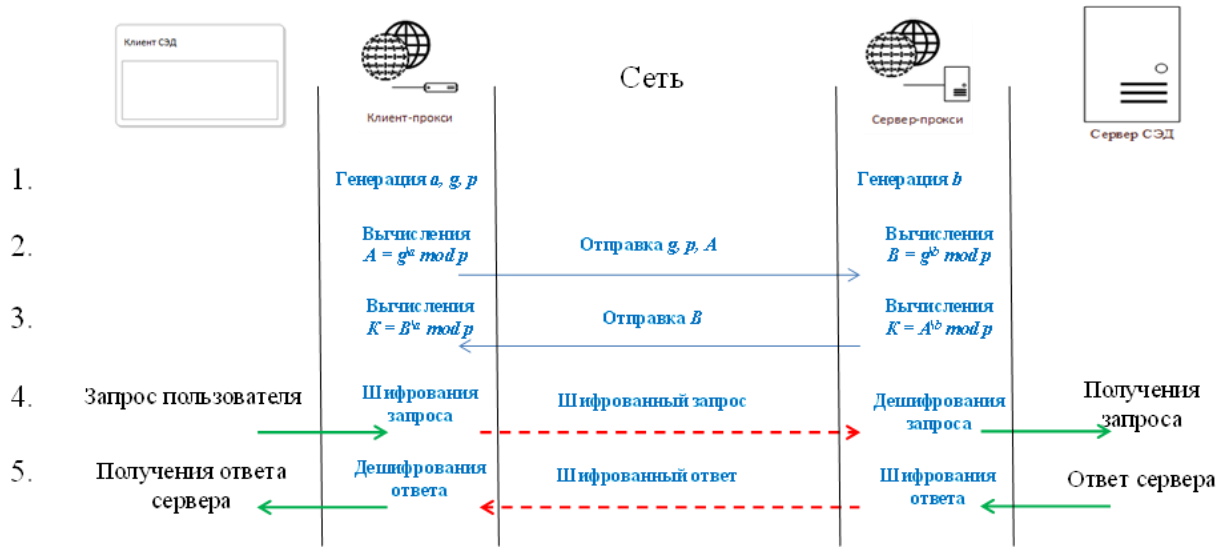

Рис 12. Алгоритм работы шифрованного соединения с помощью прокси-серверов

2. Средства создания программного модуля

До выбора средства разработки надо учесть, что большинство часть пользователей СЭД используют семейства операционных систем Windows. Но в том же времени сервера СЭД все больше специализируется на операционных систем с ядром Linux. Поэтому средства создания программного модуля должно быт кроссплатформенным. Кроссплатформенность позволит нам обеспечить возможность работы системы со всеми операционными системами.

В качестве средства создания было выбрано язык программирования Java.

Java — объектно-ориентированный язык программирования, разработанный компанией Sun Microsystems (в последующем приобретённой компанией Oracle). Приложения Java обычно транслируется в специальный байт-код, поэтому они могут работать на любой виртуальной Java-машине вне зависимости от компьютерной архитектуры. Дата официального выпуска — 23 мая 1995 года.

Программы на Java транслируются в байт-код, выполняемый виртуальной машиной Java (JVM) — программой, обрабатывающей байтовый код и передающей инструкции оборудованию как интерпретатор.

Достоинством подобного способа выполнения программ является полная независимость байт-кода от операционной системы и оборудования, что позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина. Другой важной особенностью технологии Java является гибкая система безопасности благодаря тому, что исполнение программы полностью контролируется виртуальной машиной. Любые операции, которые превышают установленные полномочия программы (например, попытка несанкционированного доступа к данным или соединения с другим компьютером) вызывают немедленное прерывание.

Часто к недостаткам концепции виртуальной машины относят то, что исполнение байт-кода виртуальной машиной может снижать производительность программ и алгоритмов, реализованных на языке Java. В последнее время был внесен ряд усовершенствований, которые несколько увеличили скорость выполнения программ на Java:

- применение технологии трансляции байт-кода в машинный код непосредственно во время работы программы (JIT-технология) с возможностью сохранения версий класса в машинном коде,
- широкое использование платформенно-ориентированного кода (native-код) в стандартных библиотеках,
- аппаратные средства, обеспечивающие ускоренную обработку байт-кода (например, технология Jazelle, поддерживаемая некоторыми процессорами фирмы ARM).

Чтобы не разбираться всеми спецификациями HTTP (RFC 1945, RFC 2616), нужен прокси-сервер с открытым исходным кодом. Было выбрано прокси-сервер jHttp2 от Benjamin Kohl (http://jhttp2.sourceforge.net/). Этот

проект отличается тем, что очень функционален и не сложно структурирован.

jHTTPp2 небольшой HTTP прокси-сервер на основе Java. Она была разработана с несколькими преимуществами:

- имеет поддержку HTTP 1.1;
- позволяет работать с безопасными соединениями (называемые SSL туннелирования);
- встроенный веб сервер для настройки программы;
- настраиваемый контроль сессионными файлами;
- небольшой размер и поддержка кроссплатформенности.

После внесения изменений на jHTTPp2, он будет работать в трех режимах:

- обычный прокси;
- клиент прокси;
- сервер прокси.

3. Анализ эффективности использования программного модуля

При использовании программного модуля, в сети появляется две новые элементы для обработки данных. Так как шифрующие прокси-сервера активно преобразует данных, требуется дополнительные мощности вычислительной техники и соответственно дополнительное время.

Время установления соединения и обмена данных более заметно, когда обменивается очень маленький размер данных. Но, после увеличения обмениваемых данных отличие времени уменьшится.

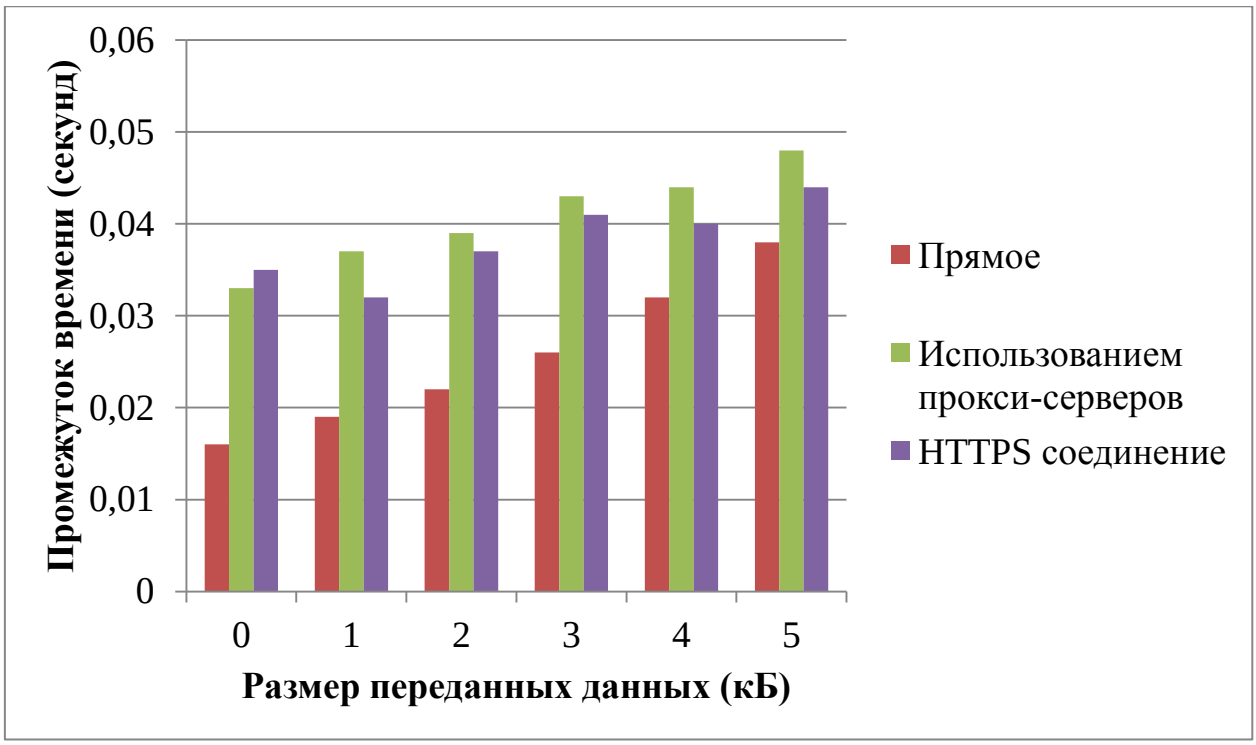

Рис 13. Диаграмма для показа затраты времени

С точки зрения информационной безопасности шифрования данных при сетевом обмене информации – это очень хорошо. Но при таком структуре обмена данными есть вероятность, что третья сторона ведет себя как участник обмена. То есть при обмене данными между точками A и B, некий C точка может выдать себя как B для A точки, точно так же как A для B точки. В этом случаи C получает один ключ общий с A (которая считает, что это B) и один ключ общий с B (который считает, что это A). Следовательно, C может получать от A любое сообщение для B, расшифровать его ключом, прочитать, зашифровать ключом и передать B. Таким образом, фальсификация может оставаться незамеченным. По этому, в программе использован модифицированный метод обмена общих секретных ключей. Стандартное умножение и возведение в степень заменяется на параметрическое умножение и параметрическое возведение в степень соответственно. Но попадание настоящего алгоритма работы или программного обеспечение в руки третей стороны предоставляет возможность атаки в вышеуказанной форме. Чтобы предотвратит такого

типа угрозы, предлагается использовать инфраструктуру открытых ключей (Public Key Infrastructure - PKI).

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- закрытый ключ известен только его владельцу;
- удостоверяющий центр создает сертификат открытого ключа, таким образом, удостоверяя этот ключ;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Фактически, PKI представляет собой систему, основным компонентом, которым является удостоверяющий центр и пользователи, взаимодействующие между собой посредством удостоверяющего центра.

Используя PKI структуру, появляется возможность удостоверить точку, которая устанавливается соединение. Но чтобы сохранить секретность параметра параметрических функций советуется сохранить секретность исходного кода программы и распространять программы в бинарном формате.

4. Рекомендации по применению программного модуля

Архитектура построения СЭД может быть, как толстым клиентом, так и тонким клиентом. Чтобы построит систему в архитектуре «толстый клиент», обычно разработают клиент-приложение. Клиент будет скачивать часть базы системы и будет обработать требование пользователя. Такая архитектура сейчас используется в СЭД «ELMA». Во время подключения к серверу и скачивания базы данных можно использовать ранее предложенные шифрующие прокси-сервера.

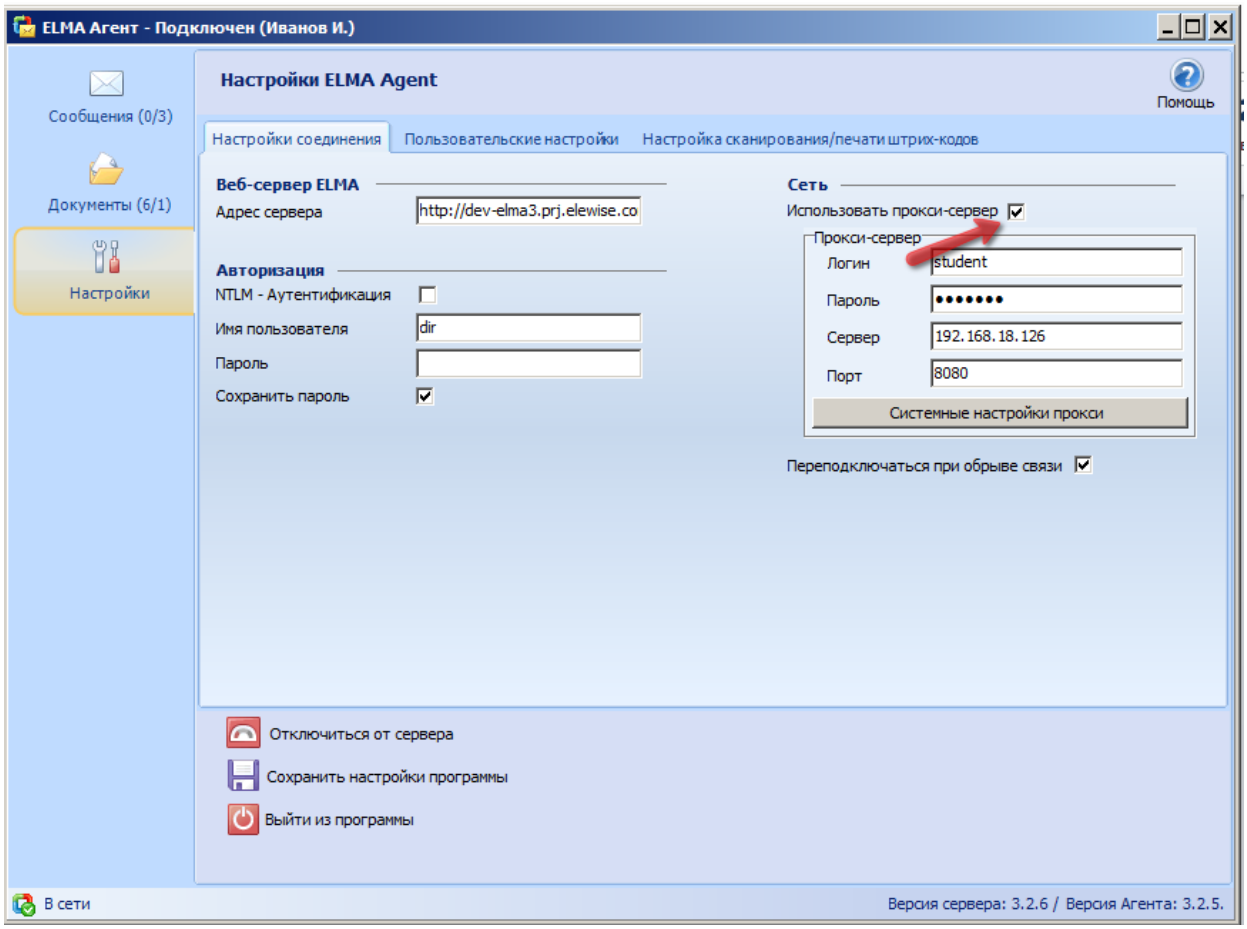

Рис 14. Настройка прокси-сервера в архитектуре «толстый клиент».

Тонкий клиент для СЭД, обычно, предоставляется в виде веб приложения. Например, СЭД «E-hujjat» и СЭД «Гермес» использует данную технологию. Веб технологий предоставляет широкие возможности при построении тонких клиентов. Клиент-приложением веб технологий является браузер, и все браузеры имеет возможность работы с прокси-серверами.

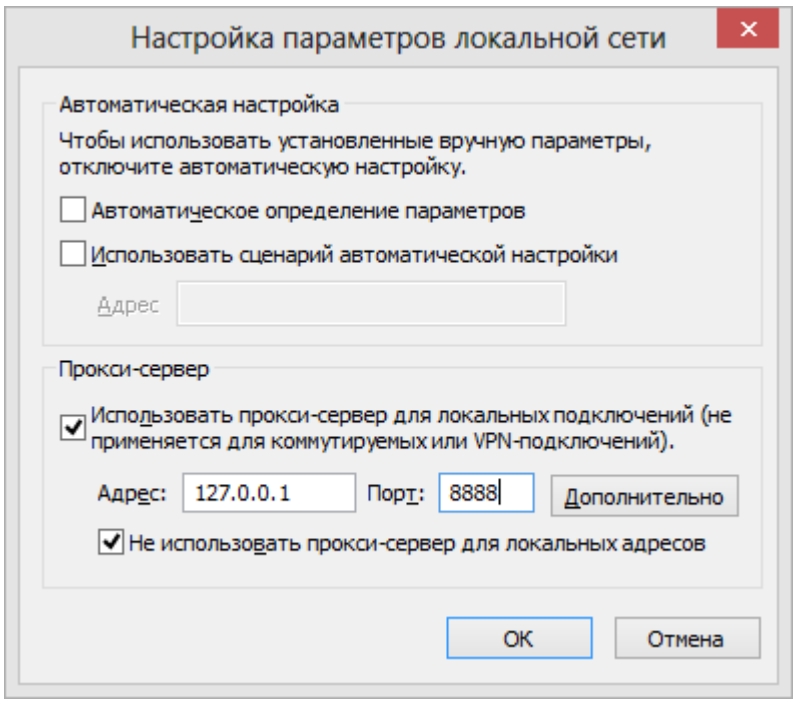

Рис 15. Настройка прокси-сервера в браузере Internet Explorer.

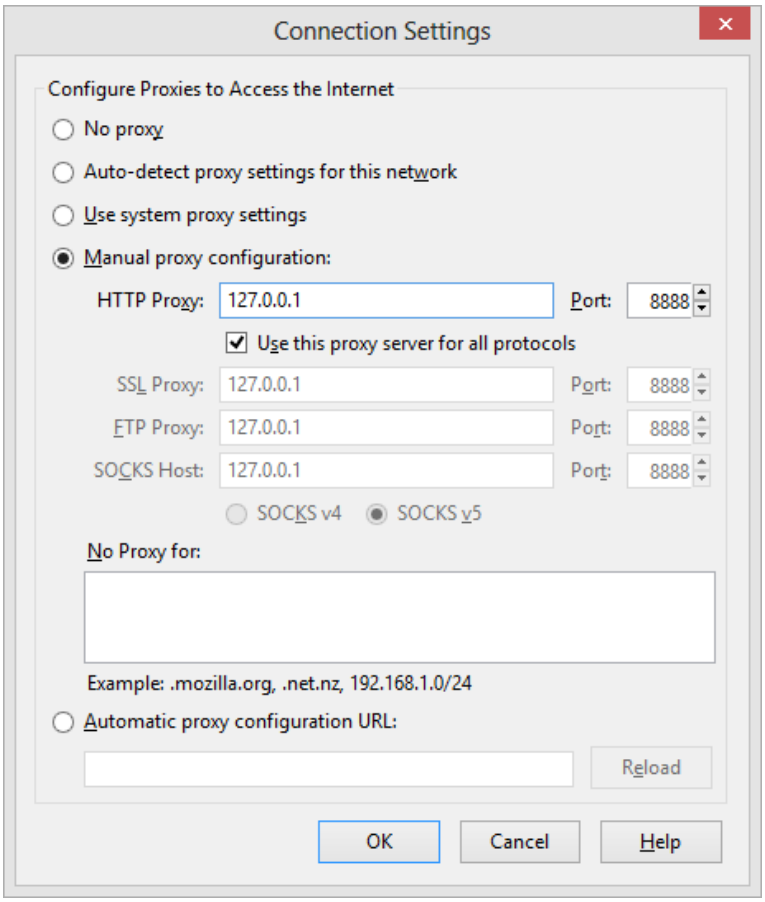

Рис 16. Настройка прокси-сервера в браузере Mozilla Firefox.

После настройки программы пользователя сам пользователь не будет чувствовать никаких изменений.

Программу можно запустит в трёх режимах:

- Обычный прокси – не шифрует, только перенаправляет запрос;

- Шифрующий клиент прокси – будет запущен в стороне клиента и шифрует запрос, дешифрует ответ;

- Шифрующий сервер прокси - будет запущен в стороне сервера и дешифрует запрос, шифрует ответ.

Программа запускается с помощью соответствующих .bat файлов.

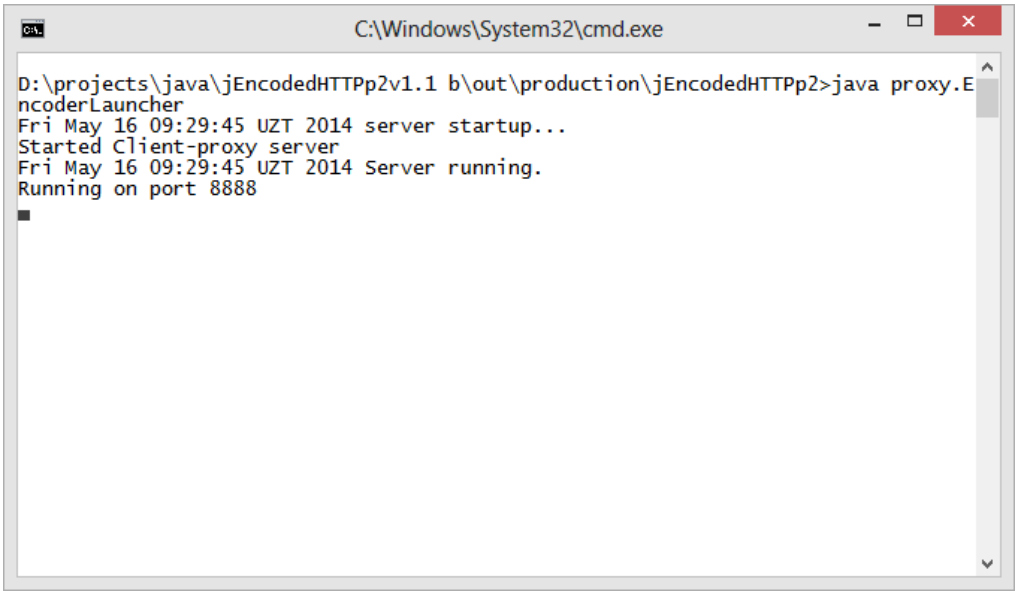

Рис 17. Запуск клиент-прокси программы.

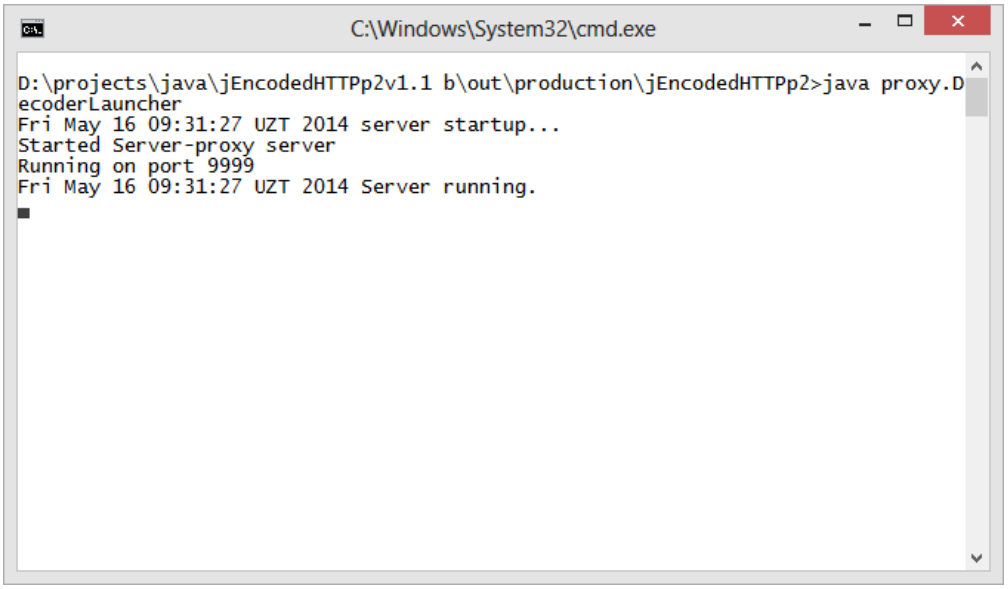

Рис 18. Запуск сервер-прокси программы.

Если запустит программу в режиме отладки, то можно увидеть процесс шифрования и дешифрования.

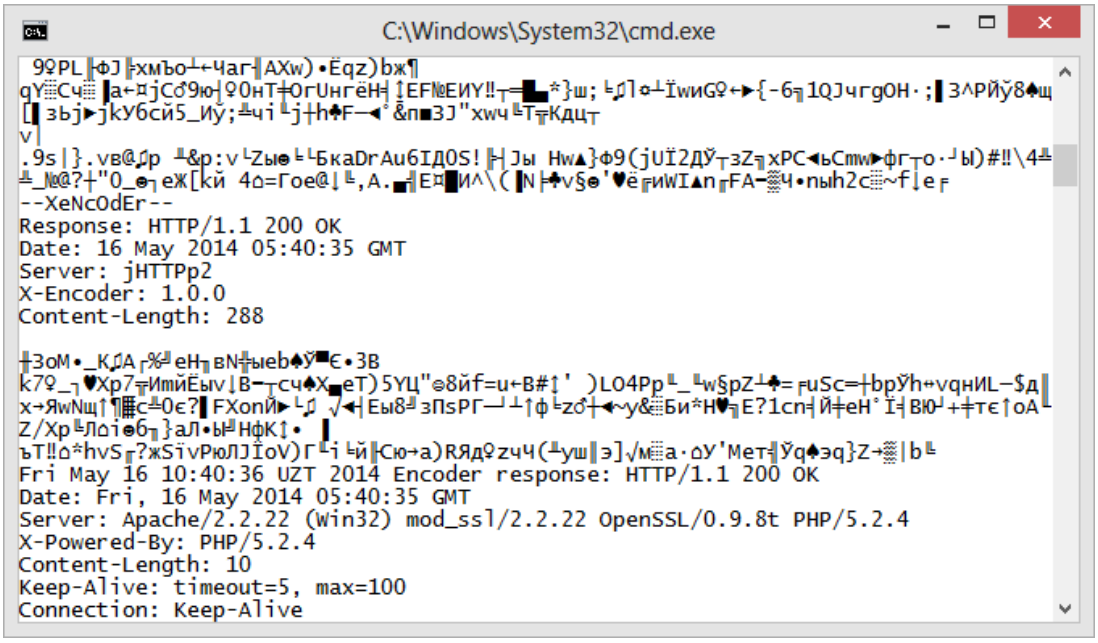

Рис 19. Режим отладки клиент-прокси.

Рис 20. Режим отладки сервер-прокси.

Для конечного пользователя СЭД изменения в сети не отражается.

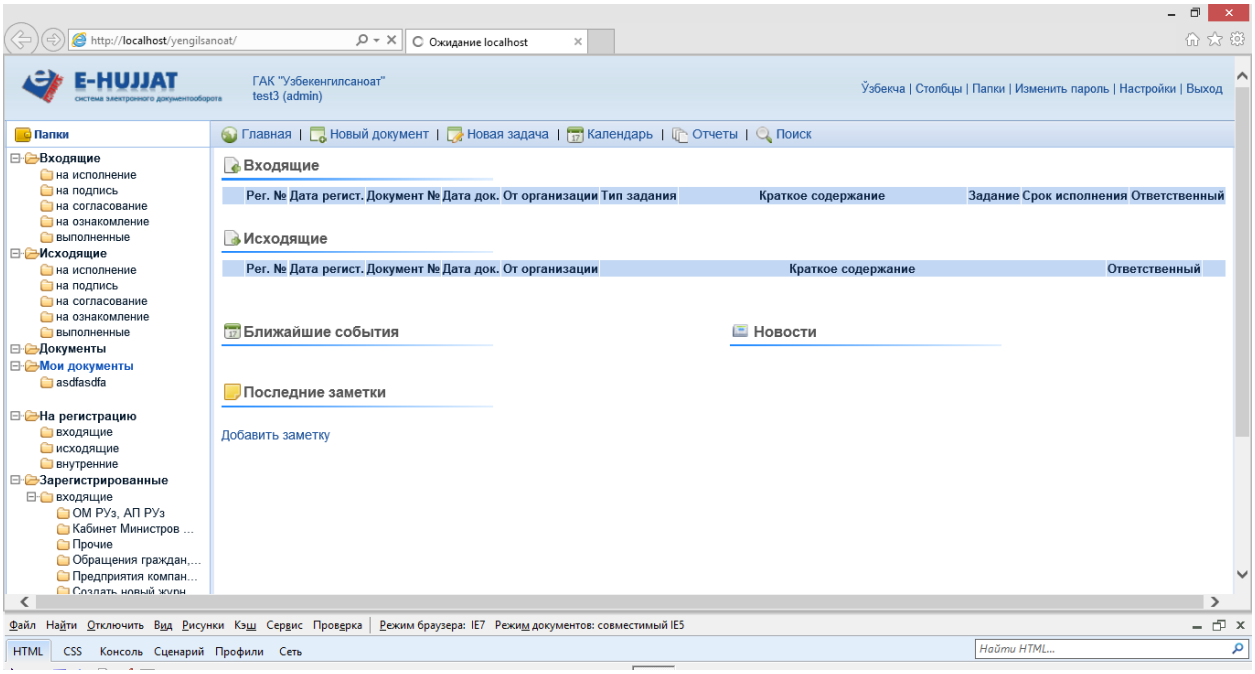

Рис 19. Главная страница СЭД «Э-ҳужжат» с использованием шифрующих прокси-серверов

Через сниффер обмениваемая информация не будет видно.

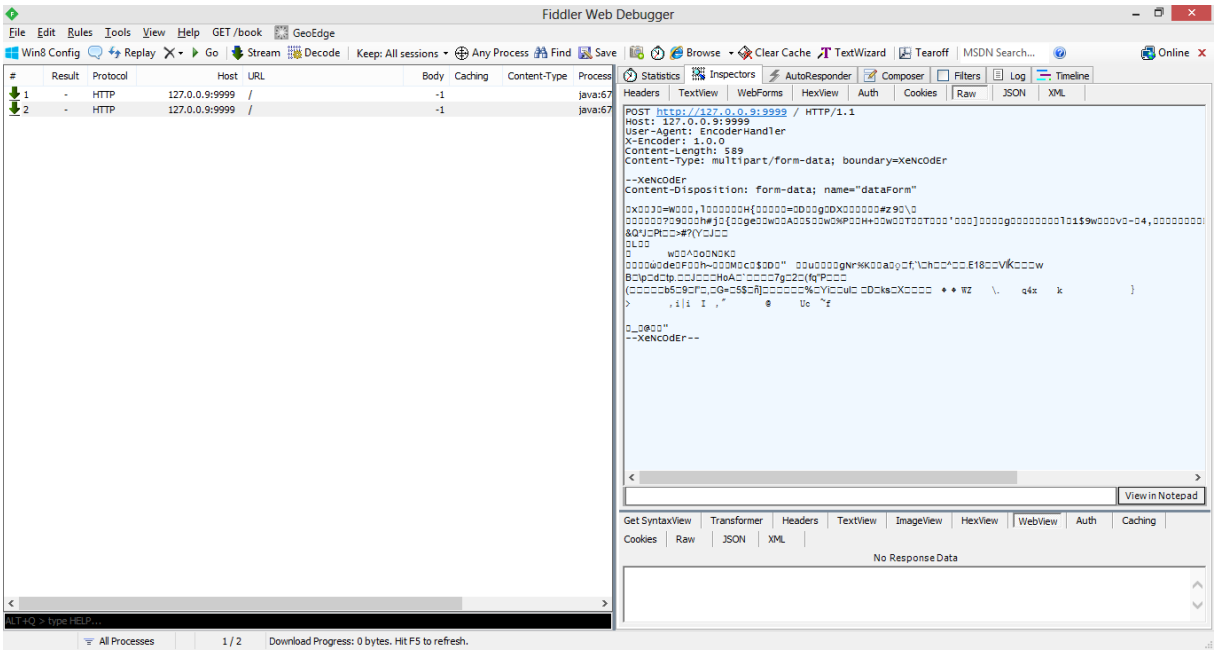

Рис 20. Вид обмениваемой информации с помощью веб-сниффера

Но стоит уделить внимание на то, что после применение предлагаемой технологии обмена информации, веб-сервер в качестве сетевого адреса пользователя будет применять сетевой адрес сервер-

прокси. Поэтому, программисту СЭД стоит не учитывать сетевой адрес прокси как реальный сетевой адрес пользователя. Также в дальнейших исследованиях предлагается добавить к запросу пользователя специальную строку – **X-FORWARDED-FOR**, которая указывает реальный сетевой адрес клиента.

Выводы по главе III

В данной главе предложен метод для безопасного соединения в незащищенных от прослушивания каналах связи, путем применения шифрующих прокси-серверов. Для обеспечения безопасной передачи единого ключа шифрования был усовершенствован алгоритм Диффи-Хеллмана. Разработана программа, реализующая предлагаемый метод и алгоритм. Анализ работы программы показал неплохой результат – увеличилась устойчивость безопасности данных, причем потеря времени при обмене данными не значительна. Предложены рекомендации по применению программы в системах электронного документооборота в качестве отдельного модуля.

Заключение

В ходе выполнения диссертационной работы получены следующие результаты:

1. Изучено нормативно-правовое основание ведения делопроизводства и электронного документооборота в Республике Узбекистан. В ходе исследования определилось, что нормативно-правовая база по данной отрасли развивается поэтапно.
2. Проанализированы достоинства и недостатки систем электронного документооборота, где главным недостатком в таких системах является информационная безопасность.
3. Определены основные группы методов и средств защиты информации в системах электронного документооборота. Был сделан вывод, что при использовании современных систем электронного документооборота следует применять в комплексе вышеописанные группы методов и средств защиты информации.
4. Рассмотрены основные требования для систем электронного документооборота в целом, и определены дополнительные требования для защищенных систем электронного документооборота.
5. Проанализированы возможности национальных криптографических алгоритмов. Выявлены достоинства и недостатки национальных крипто-модулей.
6. Разработан метод обмена информацией для защиты от прослушивания в каналах связи и усовершенствован алгоритм Диффи-Хеллмана для обмена секретным ключом.
7. Создана программа, реализующая вышеуказанный алгоритм и метод.

8. Подготовлены рекомендации по внедрению программы в систему электронного документооборота в качестве отдельного модуля.

Список использованной литературы

Законы Республики Узбекистан:

1. Закон Республики Узбекистан от 6 мая 1994 г. № 1064-XII «Об обращениях граждан».
2. Закон Республики Узбекистан от 11 декабря 2003 г. № 562-II «Об электронной цифровой подписи».
3. Закон Республики Узбекистан от 29 апреля 2004 г. № 611-II «Об электронном документообороте».

Постановления и распоряжения Президента Республики Узбекистан, Кабинета Министров:

4. Постановление Кабинета Министров Республики Узбекистан от 29 марта 1999 г. № 140 «Об утверждении нормативных документов по делопроизводству и организации контроля исполнения в органах государственной власти и управления Республики Узбекистан».
5. Постановления Кабинета Министров Республики Узбекистан от 12 января 1999 г. № 12 «О мерах по укреплению исполнительской дисциплины».
6. Постановления Кабинета Министров Республики Узбекистан от 04 мая 2011 г. № 126 «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате кабинета министров, органах государственного и хозяйственного управления, государственной власти на местах».

Работы Президента Республики Узбекистан И.А. Каримова:

7. Доклад Президента Республики Узбекистан Ислама Каримова на заседании Кабинета Министров, посвященном итогам социально-экономического развития страны в 2012 году и важнейшим приоритетным направлениям экономической программы на 2013 год

Нормативные документы:

8. O’zDSt 2298:2011 Информационная технология. Электронный документооборот. Типовые требования.
9. O'zDSt 1105:2009 Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных.
10. O'zDSt 1106:2009 Информационная технология. Криптографическая защита информации. Функции хэширования.
11. O'zDSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки ЭЦП.

Основная литература:

12. «Перспективы электронного правительства», Някина Е.С., Погодина Е.С., Государственное управление. Электронный вестник. Выпуск № 31. Апрель 2012 г.
13. Печникова Т.В., Печникова А.В. Практика работы с документами в организации: Учеб. пособие для вузов. – М.: ЭМОС, 1999. – 208с.
14. Кузнецова Т.В. Делопроизводство (Документационное обеспечение управления). — М.: ЗАО "Бизнес-школа "Интел-Синтез", 2000. - 818 с.
15. Фатьянов А.А. Правовое регулирование электронного документооборота: учебно-практическое пособие. М.: Российская газета, 2005-200 с.
16. Технические методы и средства защиты информации. / Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. СПб.: ООО «Издательство полигон», 2000. -320 с.
17. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: Кудиц-Образ, 2001. - 368 с.
18. Pfeeger C.P., Pfeeger S.L.: Security in Computing. Third edn. Prentice Hall 2003 г.

19. Jonas Birme, Document Management System Security, Umea University, 2005 г.
20. Дэвид В. Чепмен, Энди Фокс Брандмауэры Cisco Secure PIX, Cisco® Secure PIX® Firewalls. — М.: «Вильямс», 2003. — С. 384
21. Журнал «Секретарь-референт» № 6 (78) июнь 2009
22. «A digital signature scheme secure against adaptive chosen-message attacks.», Shafi Goldwasser, Silvio Micali, and Ronald Rivest. SIAM Journal on Computing, 17(2):281—308, 1988.
23. Парпиев Н.Н., Турсунбаев У.Т., Безопасное соединение в незащищенных каналах связи. // ICTNEWS, №4 2014.
24. Biryukov, Alex and Khovratovich, Dmitry Related-key Cryptanalysis of the Full AES-192 and AES-256 (англ.) // Advances in Cryptology – ASIACRYPT 2009. — Springer Berlin / Heidelberg, 2009. — Т. 5912. — С. 1—18. — DOI:10.1007/978-3-642-10366-7_1
25. Хасанов П.Ф., Хасанов Х.П., Стойкость Государственного стандарта ЭЦП Республики Узбекиста, 2010 г.
26. Турсунбаев У.Т., Парпиев Н.Н., Усовершенствованный алгоритм Диффи-Хеллмана для обмена секретными ключами, Сборник научных статей, ТГТУ, 2014 г.

Электронные ресурсы:

27. http://news.excelion.ru, Основные критерии защищенности [Электронный ресурс].
28. http://www.ixbt.com/soft/sed.shtml, Обзор систем электронного документооборота // 20 декабря 2011г. [Электронный ресурс].
29. http://www.citforum.ru/ofis/ofis96/104.shtm, Афанасьев А. Методы управления документооборотом в организации. [Электронный ресурс].
30. http://daily.sec.ru/2012/02/27/print-O-zashite-elektronnogo-dokumentooborota.html, Алексей Сабанов, О защите электронного документооборота. 2012 г. [Электронный ресурс].

31. http://www.cnews.ru/article/2013/06/05/informacionnye_sistemy_pravovoe_pole_531148, Станислав Макаров, Наталья Рудычева, Информационные системы: правовое поле, 2013 [Электронный ресурс].

Приложение

Код программы для запуска клиентского прокси:

```
import java.net.InetAddress;
public class EncoderLauncher {

   static Jhttpp2Server encoderServer;

   public static void main(String[] args) throws Exception{
      encoderServer = new Jhttpp2Server(8888);
      encoderServer.use_proxy = true;
      encoderServer.proxy = InetAddress.getByName("192.168.0.2");
      encoderServer.proxy_port = 7777;
      encoderServer.serverType = Jhttpp2Server.ServerType.ENCODER;
      encoderServer.debug = true;
      encoderServer.init();
      if (encoderServer.error){
         System.out.println("Error: " + encoderServer.error_msg);
      } else {
         new Thread(encoderServer).start();
         System.out.println("Started Client-proxy server");
         System.out.println("Running on port " + encoderServer.port);
      }
   }
}
```

Код программы для запуска серверного прокси:

```
public class DecoderLauncher {

   static Jhttpp2Server decoderServer;

   public static void main(String[] args) throws Exception{
      decoderServer = new Jhttpp2Server(9999);
      decoderServer.serverType = Jhttpp2Server.ServerType.DECODER;
      decoderServer.debug = true;
      decoderServer.init();
      if (decoderServer.error){
         System.out.println("Error: " + decoderServer.error_msg);
      } else {
         new Thread(decoderServer).start();
         System.out.println("Started Server-proxy server");
         System.out.println("Running on port " + decoderServer.port);
      }
   }
}
```

Часть кода программы, отвечающая за обработку запросов:

```
import java.util.Date;

public class Handler {
   public static String pKey;
   public static String boundary = "XeNcOdEr";
   public static boolean isEncoded = true;
```

```
   public static byte[] handleRequest(byte[] request, Jhttpp2Server.ServerType
serverType, Jhttpp2Server server)
   {
      server.writeLog("Request: " + new String(request));
      //serverType = Jhttpp2Server.ServerType.SIMPLE;
      HTTPParser httpParser = new HTTPParser(request);
      switch (serverType){
         case ENCODER:
            //if (httpParser.hostName != server.realServer) { isEncoded = false;
return request; }
            byte[] body = (encode(request, pKey));
            byte[] start = (("--"+boundary+"\r\n" +
                  "Content-Disposition: form-data;
name=\"dataForm\"\r\n\r\n").getBytes());
            byte[] stop = ("\r\n--" + boundary + "--").getBytes();
            byte[] byteBuffer = new byte[start.length + body.length + stop.length];
            System.arraycopy(start, 0, byteBuffer, 0, start.length);
            System.arraycopy(body, 0, byteBuffer, start.length, body.length);
            System.arraycopy(stop, 0, byteBuffer, start.length + body.length,
stop.length);
            server.writeLog("Encoded body Length: " + new
String(body).length());
            server.writeLog("Encoded body: " + new String(body));
            //if (server.proxy.getHostAddress())
               byte[] head = ("POST http://" + server.proxy.getHostAddress() +
":" + server.proxy_port + "/ " + server.getHttpVersion() + "\r\n" +
                  "Host: " + server.proxy.getHostAddress() + ":" +
server.proxy_port + "\r\n" +
                  "User-Agent: EncoderHandler\r\n" +
                  "X-Encoder: 1.0.0\r\n" +
```

```
                    "Content-Length: " + byteBuffer.length + "\r\n" +
                    "Content-Type: multipart/form-data;
boundary="+boundary+"\r\n" +
                    "\r\n").getBytes();
            byte[] headBody = new byte[head.length + byteBuffer.length];
            System.arraycopy(head, 0, headBody, 0, head.length);
            System.arraycopy(byteBuffer, 0, headBody, head.length,
byteBuffer.length);
            isEncoded = true;
            server.writeLog("Encoder request: " + new String(headBody));
            return headBody;
         case DECODER:
            if (httpParser.isEncoded()){
               isEncoded = true;
               server.writeLog("Decoder request: " + new
String(decode((httpParser.getEncodedBody(httpParser.body)), pKey)));
               return decode((httpParser.getEncodedBody(httpParser.body)),
pKey);
            } else {
               //isEncoded = false;
               return request;
            }
         default:
            return request;
      }
   }
   public static byte[] handleResponse(byte[] response,
Jhttpp2Server.ServerType serverType, Jhttpp2Server server)
   {
      System.out.println("Response: " + new String(response));
```

```
        //serverType = Jhttpp2Server.ServerType.SIMPLE;
        HTTPParser httpParser = new HTTPParser(response);
        switch (serverType){
            case ENCODER:
                if (httpParser.isEncoded()){
                    isEncoded = true;
                    server.writeLog("Encoder response: " + new
String(decode((httpParser.body), pKey)));
                    return decode((httpParser.body), pKey);
                } else {
                    //isEncoded = false;
                    return response;
                }
            case DECODER:
                //if (httpParser.getHostName() != server.realServer) { isEncoded =
false; return response; }
                if (httpParser.isEncoded()) return response;
                Date date = new Date();
                byte[] encodedHttp = (encode(response, pKey));
                byte[] head = ("HTTP/1.1 200 OK\r\n" +
                "Date: " + date.toGMTString() + "\r\n" +
                "Server: jHTTPp2\r\n" +
                "X-Encoder: 1.0.0\r\n" +
                "Content-Length: " + encodedHttp.length + "\r\n" +
                        "\r\n").getBytes();
                byte[] headAndBody = new byte[head.length + encodedHttp.length];
                System.arraycopy(head, 0, headAndBody, 0, head.length);
                System.arraycopy(encodedHttp, 0, headAndBody, head.length,
encodedHttp.length);
                isEncoded = true;
```

```
            server.writeLog("Decoder response: " + new String(headAndBody));
            return headAndBody;
        default:
            return response;
    }
}

public static byte[] encode(byte[] pText, String pKey) {
    byte[] res = AES.encrypt(pText, pKey.getBytes());
    return res;
}

public static byte[] decode(byte[] pText, String pKey) {
    byte[] res = AES.decrypt(pText, pKey.getBytes());
    return res;
}

private static byte[][] getTripleSecret(String pKey) {
    byte[] bytes = pKey.getBytes();
    byte[][] tripleKey = new byte[3][8];
    System.arraycopy(bytes, 0, tripleKey[0], 0, 8);
    System.arraycopy(bytes, 8, tripleKey[1], 0, 8);
    System.arraycopy(bytes, 16, tripleKey[2], 0, 8);
    return tripleKey;
}

public static byte[] getRealBytes(byte[] x){
    int len = x.length;
    if (x[x.length-1] == 0x00)
    for(int i = x.length-2; i > 0; i--){
```

```
            if (x[i] == 0x00){
                len = i;
            } else {
                break;
            }
        }
        byte[] real = new byte[len];
        System.arraycopy(x, 0, real, 0, len);
        return real;/*return x;*/
    }
    public static byte[] base64UrlEncode(byte[] input) {
        Base64 decoder = new Base64(true);
        return decoder.encode(input);
    }
    public static byte[] base64UrlDecode(byte[] input) {
        Base64 decoder = new Base64(true);
        return decoder.decode(input);
    }

}
```

Часть кода программы, реализующая криптографический алгоритм шифрования AES(Rijndeal-128):

……

```
public static byte[] encrypt(byte[] in,byte[] key){
    Nb = 4;
    Nk = key.length/4;
    Nr = Nk + 6;
    int lenght=0;
    byte[] padding = new byte[1];
    int i;
    lenght = 16 - in.length % 16;
    padding = new byte[lenght];
    padding[0] = (byte) 0x80;
    for (i = 1; i < lenght; i++)
       padding[i] = 0;
    byte[] tmp = new byte[in.length + lenght];
    byte[] bloc = new byte[16];
    w = generateSubkeys(key);
    int count = 0;
    for (i = 0; i < in.length + lenght; i++) {
       if (i > 0 && i % 16 == 0) {
          bloc = encryptBloc(bloc);
          System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);
       }
       if (i < in.length)
          bloc[i % 16] = in[i];
       else{
          bloc[i % 16] = padding[count % 16];
          count++;
       }
```

```
        }
        if(bloc.length == 16){
            bloc = encryptBloc(bloc);
            System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);
        }
        return tmp;
    }
    public static byte[] decrypt(byte[] in,byte[] key){
        int i;
        byte[] tmp = new byte[in.length];
        byte[] bloc = new byte[16];
        Nb = 4;
        Nk = key.length/4;
        Nr = Nk + 6;
        w = generateSubkeys(key);
        for (i = 0; i < in.length; i++) {
            if (i > 0 && i % 16 == 0) {
                bloc = decryptBloc(bloc);
                System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);
            }
            if (i < in.length)
                bloc[i % 16] = in[i];
        }
        bloc = decryptBloc(bloc);
        System.arraycopy(bloc, 0, tmp, i - 16, bloc.length);
        tmp = deletePadding(tmp);
        return tmp;
    }
```

……