Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 519.72

ЦЕБРУК
Елена Васильевна

Проблема аутентификации информации в локальных сетях

АВТОРЕФЕРАТ
на соискание степени магистра информатики и вычислительной техники

по специальности 1-40 81 01 «Информатика и технологии разработки программного обеспечения»

Научный руководитель
Липницкий Валерий Антонович
доктор техн. наук, профессор

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

Проблемы защиты информации в системах электронной обработки данных (СОД) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под системами электронной обработки данных понимаются системы любой архитектуры и любого функционального назначения, в которых для обработки информации используются средства электронно-вычислительной техники, а под защитой информации – использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в СОД. Широкое распространение и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой с СОД информации.

Четко обозначилось три аспекта уязвимости информации.

1. Подверженность физическому уничтожению или искажению.
2. Возможность несанкционированной (случайной или злоумышленной) модификации.
3. Опасность несанкционированного получения информации лицами, для которых она не предназначена.

В функционирующих компьютерных локальных сетях как никогда *актуальна проблема защиты информации* от несанкционированного использования или искажения. Прямое применение криптографических систем защиты информации резко замедляет ее передвижение. Практическим средством устранения этой проблемы является применение цифровой подписи.

Цифровая подпись электронных документов является эффективным практическим средством защиты этих документов от искажений, исправлений, а также для однозначного определения авторства данных документов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью работы является изучение аспекта формирования цифровой подписи, методики определения авторства и целостности передаваемой информации.

Объектом исследования является информация, передаваемая по локальной сети.

Предмет исследования – цифровая подпись блоков передаваемой информации.

Передача информации по сети значительно увеличивает скорость обмена данными, возникает проблема установления подлинности автора и отсутствия изменений в полученном документе. Поэтому *задачей* работы является разработка системы, предоставляющей защиту передаваемых сообщений от возможных видов злоумышленных действий.

В диссертационной работе рассмотрены алгоритмы шифрования данных RSA и Эль-Гамаля, рассмотрены алгоритмы хэширования информации такие как отечественный стандарт хэширования ГОСТ Р 34.11-94 и функция хэширования MD5, изучены алгоритмы формирования электронной цифровой подписи: алгоритм цифровой подписи DSA; алгоритм цифровой подписи RSA; алгоритм цифровой подписи Эль-Гамаля; алгоритм цифровой подписи ГОСТ Р 34.10-94.

В работе обоснована целесообразность применения электронной цифровой подписи на основе открытого коллективного ключа в системах защищенного электронного документооборота.

В среде MS Visual Studio на языке C# разработан клиент-серверный программный продукт, позволяющий передавать данные по локальной сети, также учитывающий нюансы работы с криптографической системой RSA и электронной цифровой подписью на ее основе.

Научная новизна работы состоит в обосновании и разработке метода формирования и проверки электронной цифровой подписи на основе открытого ключа и криптографических конструкций, позволяющего повысить оперативность совместной обработки электронных документов при сохранении требуемого уровня защищённости.

Практическая значимость работы состоит в разработке программного комплекса ЭЦП и возможности его реализации в существующих локальных сетях, что позволит повысить оперативность обработки электронных документов.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационной работы, приведены цель и задачи работы, указываются методы исследования.

В первой главе «Методы защиты информации в частных криптосистемах» дается понятие криптографической защиты информации, выделены три основные функции для обеспечения безопасности данных, которые необходимо поддерживать:

– защиту конфиденциальности передаваемых или хранимых в памяти данных;

– подтверждение целостности и подлинности данных;

– аутентификацию абонентов при входе в систему и при установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Сделан вывод о том, что целостность и подлинность передаваемых данных достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Так же подробно рассматриваются ассиметричные криптосистемы шифрования.

Во второй главе «Методы и алгоритмы хэширования информации» подробно рассматриваются такие криптографические методы защиты компьютерной информации, как функции хэширования.

Определены следующие основные требования, предъявляемые к криптографической хэш-функции $h(x)$:

– результат действия хэш-функции должен зависеть от всех двоичных символов исходного сообщения, а также от их взаимного расположения;

– $h(x)$ должна быть чувствительна к любым изменениям входной информационной последовательности, при любых изменениях на входе результат действия хэш-функции должен быть непредсказуем – в среднем должна измениться половина бит хэш-образа.

Подробно изучены однонаправленные хэш-функции.

Третья глава диссертационной работы «Алгоритмы формирования электронной цифровой подписи» посвящена изучению алгоритмов формирования ЭЦП.

Описана система ЭЦП, которая включает две основные процедуры:

– формирования цифровой подписи;

– проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи — открытый ключ отправителя.

На рисунке 1 показана схема формирования ЭЦП.

Рисунок 1 — Схема формирования электронной цифровой подписи

На подготовительном этапе этой процедуры абонент А — отправитель сообщения — генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель А прежде всего вычисляет значение хэш-функции $h(M)$ подписываемого текста M.

Абоненты сети могут проверить цифровую подпись полученного сообщения M с помощью открытого ключа K_A отправителя этого сообщения (рисунок 2).

Рисунок 2 — Схема проверки электронной цифровой подписи

При проверке ЭЦП абонент В — получатель сообщения M — расшифровывает принятый дайджест m открытым ключом K_A отправителя А. Кроме того, получатель сам вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если m и m' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Важно отметить, что с точки зрения конечного пользователя процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используются закрытый ключ отправителя, тогда как при зашифровывании используется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровывании — закрытый ключ получателя.

Четвертая глава «Реализация компьютерной версии электронной цифровой подписи для применения в локальной сети» посвящена разработке компьютерной версии ЭЦП для применения в локальных сетях.

Описано приложение, которое имеет клиент-серверную архитектуру. Клиент и сервер могут находится как в рамках одной вычислительной системы, так и на различных компьютерах, связанных сетью. Приложение позволяет производить оправку как текстовых сообщений, так и различных видов файлов

по сети. Для установления подлинности автора и отсутствия изменений в полученном документе приложение позволяет сформировать электронную цифровую подпись на базе алгоритма RSA. В качестве подписываемого документа может быть использован любой файл. После получения цифровой подписи файлы (документ, файл открытого ключа с расширением .key и файл цифровой подписи с расширением .eds) могут быть отправлены получателю. В свою очередь получатель имеет возможность проверки подлинности полученного файла.

Диаграмма вариантов использования представлена на рисунке 3.

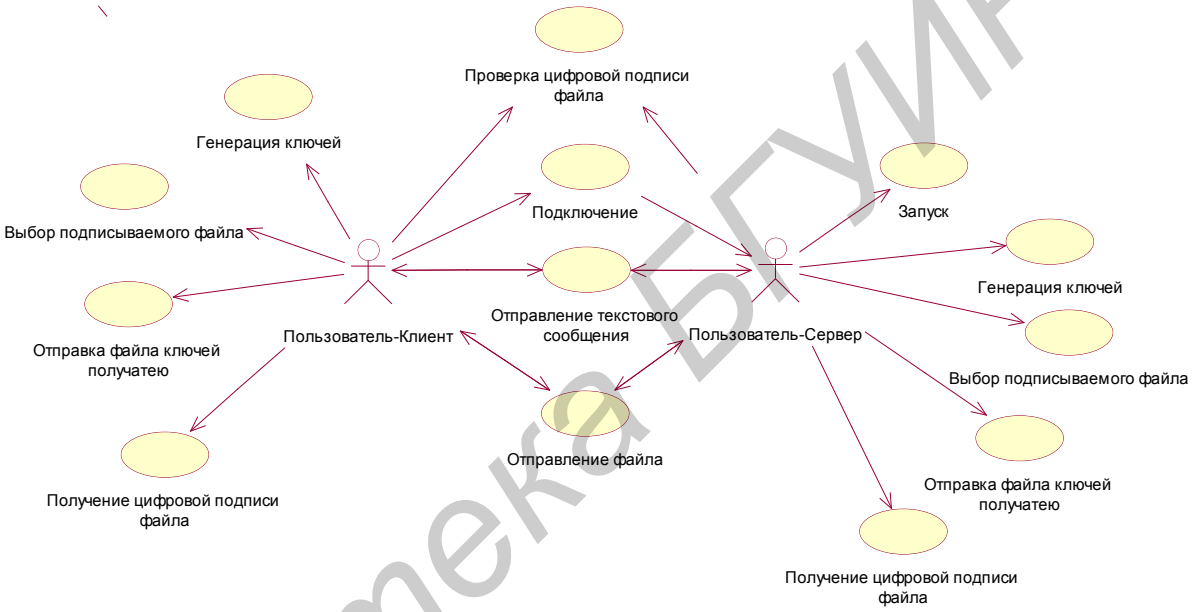

Рисунок 3 – Диаграмма вариантов использования

В заключении сформулированы основные результаты работы, кратко охарактеризована их новизна и практическая ценность. Приведены сведения о публикации результатов работы.

ЗАКЛЮЧЕНИЕ

В диссертационной работе рассмотрены алгоритмы шифрования данных RSA и Эль-Гамаля, рассмотрены алгоритмы хэширования информации такие как отечественный стандарт хэширования ГОСТ Р 34.11-94 и функция хэширования MD5, изучены алгоритмы формирования электронной цифровой подписи:

- алгоритм цифровой подписи DSA;
- алгоритм цифровой подписи RSA;
- алгоритм цифровой подписи Эль-Гамаля;
- алгоритм цифровой подписи ГОСТ Р 34.10-94.

В ходе работы обоснована целесообразность применения электронной цифровой подписи на основе открытого коллективного ключа в системах защищенного электронного документооборота.

В среде Rational Rose построена и описана диаграмма вариантов использования проекта.

Разработана клиент-серверная архитектура приложения, которую просто тестировать и технически сопровождать. Описаны и рассмотрены классы взаимодействия клиента и сервера.

В среде MS Visual Studio на языке C# разработан клиент-серверный программный продукт, позволяющий передавать данные по локальной сети, также учитывающий нюансы работы с криптографической системой RSA и электронной цифровой подписью на ее основе. Разработанная версия ЭЦП пригодна для реализации в локальной сети.

Метод формирования и проверки ЭЦП RSA даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер ЭЦП не увеличивается. Время на подписание документа остается прежним, а время проверки подлинности ЭЦП уменьшается в m-раз пропорционально количеству пользователей, участвующих в создании и подписании документа.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Цебрук Е.В. Проблема аутентификации информации в локальных сетях / Е.В. Цебрук // Материалы VII Международной научно-практической конференции: «Современные тенденции в научной деятельности». – Москва, 2015 – С. 1531 – 1534.