Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.942

СЕЛЕНЯ
Ольга Анатольевна

СИСТЕМА ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель
кандидат технических наук, доцент
Саломатин Сергей Борисович

Минск 2017

ВВЕДЕНИЕ

Важнейшее место в системе защиты электронного документооборота играет схема подтверждения подлинности на основе электронной цифровой подписи с различными алгоритмами хэширования, шифрования, и др. способами усиления криптостойкости.

В настоящее время основной проблемой алгоритмов цифровой подписи является постоянное совершенствование вычислительной мощности, что уменьшает время взлома любой криптографической схемы. Это обстоятельство побуждает ученых исследовать все новые способы усиления криптостойкости алгоритмов. Одним из таких способов является применение алгеброгеометрических кодов, которые помимо улучшения показателя криптостойкости позволяет исправлять ошибки в сообщениях, передаваемых в канале связи.

Разработка и исследование новых алгоритмов шифрования, ЭЦП, хэширования с использованием алгеброгеометрических кодов является актуальной задачей специалистов в области криптозащиты.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является разработка системы защиты электронного документооборота используя алгеброгеометрические коды.

Поставленная цель работы определяет следующие основные задачи:

1. Провести обзор и анализ методов защиты электронного документооборота с помощью электронной цифровой подписи, а также возможных путей повышения криптостойкости ЭЦП.

2. Разработать алгоритм использования технологии алгеброгеометрических кодов в составе электронной цифровой подписи .

3. Провести моделирование электронной цифровой подписи с дополнительным элементом защиты, включающим алгеброгеометрические коды.

Апробация результатов диссертации

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на XV Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Беларусь, 2017 г.).

Опубликованность результатов диссертации

Изложенные в диссертации основные положения и выводы опубликованы в 2 печатных работах. В их числе 1 статья в сборниках материалов конференций.

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав и заключения, библиографического списка и приложений. Общий объем диссертации – 82 страницы, работа содержит 25 рисунков, библиографический список включает 30 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено состояние проблемы необходимости совершенствования методов и средств защиты, применяемых в системах электронного документооборота, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с приоритетными направлениями научных исследований, приведена апробация результатов диссертации и их опубликованность.

В первой главе приведен обзор структурных компонентов, возможных угроз и методов защиты электронного документооборота, а также уделено

внимание такому методу защиты, как электронная цифровая подпись, проанализирована текущая нормативная база Республики Беларусь в области криптографической защиты и приведена модель защищенной системы электронного документооборота.

Во второй главе рассмотрены теоретические сведения о алгеброгеометрических кодах, а также теоретико-кодовые схемы, использующие АГ коды, которые существуют на данный момент, сделано сравнение эффективности криптографических методов защиты информации при фиксированном уровне стойкости.

В третей главе представлены результаты моделирования системы защиты информации электронного документооборота, а именно модифицированная схема электронной цифровой подписи на основе стандарта Республики Беларусь СТБ 34.101.45-2013 с встраиванием процедуры разделения секрета, также приведен алгоритм шифрования промежуточных значений подписи на основе алгеброгеометрических кодов

В **приложениях** приведен графический материал для защиты магистерской диссертации а также программная реализация алгоритма шифрования на алгеброгеометрических кривых в пакете Maple.

ЗАКЛЮЧЕНИЕ

1. Проведена систематизация знаний по вопросам защиты электронного документооборота: понятие электронного документооборота и ее основные компоненты, возможные угрозы для системы электронного документооборота, пути их устранения; произведен анализ законодательной базы Республики Беларусь, касательно криптографической защиты информации.

2. Предложена архитектурная схема защиты электронного документооборота, в которую включен компонент электронной цифровой подписи на эллиптических кривых и шифрование на основе алгеброгеометрических кодов

3. Проведено исследование основ теории алгеброгеометрических кодов, систем криптографической защиты на основе кодов исправляющих ошибки: криптосистемы МакЭлиса, Нидеррайтера.

4. Проведено моделирование схем пороговой электронной цифровой подписи на основе СТБ 34.101.45-2013 с разделенным секретом с использованием алгоритмов хэширования SHA-2 и SHA-3, и произведено сравнение результатов подписи с помощью статистических тестов NIST.

5. Разработан алгоритм шифрования промежуточных данных в пороговой схеме электронной цифровой подписи с разделенным секретом на основе СТБ 34.101.45-2013 с использованием алгеброгеометрических кодов.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Селеня, О.А. Реализация пороговой схемы электронной цифровой подписи с разделенным секретом на основе СТБ 34.101.45-2013 / О.А. Селеня // Научные стремления. Молодежный сборник научных статей. – 2016. – №18. – С.11–14.

2. Саломатин, С.Б., Селеня, О.А. Сравнение схем цифровой подписи на основе СТБ 34.101.45-2013 с разделенным секретом при использовании алгоритмов хэширования SHA-2 и SHA-3/ С.Б. Саломатин, О.А. Селеня//Технические средства защиты информации: Тезисы докл. XV Белорусско-российской научно-технической конференции, 6 июня 2017г. – Минск: БГУИР, 2017 – С.68.