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

На правах рукописи

УДК 004.056.5: 005.92

ФИСУНОВ
Александр Васильевич

РАЗРАБОТКА МЕТОДИКИ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРЕДПРИЯТИЯ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра технических наук

по специальности 1-38 80 04 «Технология приборостроения»

Минск 2018

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Матюшков Владимир Егорович,** доктор технических наук, профессор, член Академии инженерных наук Российской Федерации, Лауреат государственной премии СССР (1986 год), Лауреат государственной премии Республики Беларусь (2000 год), главный инженер Научно-производственного республиканского унитарного предприятия «КБТЭМ-ОМО»

Рецензент: **Казека Александр Анатольевич,** кандидат технических наук, доцент, старший научный сотрудник ОАО «КБ Радар» – управляющая компания холдинга «Системы радиолокации»

Защита диссертации состоится «26» января 2018 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г.Минск, ул. П. Бровки, 6, 1 уч. корп., ауд. 413, тел.: 293-89-37, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Информационные технологии стремительно меняются и занимают все больше места в нашей жизни, почти вся наша работа сегодня автоматизирована, благодаря им. В современном обществе информационные технологии применяются в управлении организациями всех типов во всех сферах общественного производства, как один из важнейших инструментов современного управления.

Сейчас организации, переходящие на электронный документооборот, в первую очередь думают об эффективности. Повышение эффективности возможно двумя способами – через увеличение результата и уменьшение затрат. Современные системы электронного документооборота используют оба эти способа.

Отдельным вопросом данных систем является информационная безопасность. Угрозой для информационной безопасности является несанкционированный доступ к информации с целью неправомерного использования, модификации или уничтожения, что представляет опасность для экономического и имиджевого благополучия вовлеченных сторон. Для нейтрализации таких угроз используются криптографические методы обеспечения безопасности информации.

Основное внимание в диссертации уделено электронной цифровой подписи, как наиболее распространенному и функциональному методу обеспечения целостности электронного документа.

Электронная цифровая подпись – это реквизит электронного документа, полученный путем криптографического преобразования информации, позволяющий проверить отсутствие искажений в электронном документе с момента его подписания, для установления источника данных, а также защиты от подделывания.

Согласно законодательству Республики Беларусь, документы, созданные организацией или физическим лицом на бумажном носителе и в электронном виде, идентичные по содержанию, имеют одинаковую юридическую силу. Этот факт, а также последние изменения в Законе об электронном документе и электронной цифровой подписи являются причинами актуальности и дальнейшего развития технологий в этой области.

Выражаю благодарность за оказанную помощь в ходе подготовки диссертационной работы своему научному руководителю – доктору технических наук, профессору кафедры ПИКС Матюшкову Владимиру Егоровичу, а также за высококвалифицированные консультации по возникающим вопросам кандидату технических наук, доценту кафедры ПИКС Алексееву Виктору Федоровичу.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время системы электронного документооборота выступают в качестве ключевого фактора автоматической системы управления любого предприятия. Это вызвало необходимость проработки вопросов обеспечения конфиденциальности, целостности, повышения скорости обработки и подписания электронного документа. В современных системах электронного документооборота в качестве основного средства обеспечения информационной безопасности используется электронная цифровая подпись. Современные системы электронного документооборота позволяют обрабатывать и подписывать документ одновременно только одним пользователем, что увеличивает время обработки и подписания документа, если его должны подписать несколько пользователей. Следовательно, размер электронной цифровой подписи увеличивается пропорционально числу пользователей, подписывающих электронный документ, в несколько раз. Кроме того, процедура проверки подлинности подписи подразумевает проверку подписей всех подписавших. Необходимость повышения эффективности и оперативности обработки информации в системах защищенного электронного документооборота предприятия делает представленную тему диссертации актуальной.

Степень разработанности проблемы

В области теории и практики разработки систем защищенного электронного документооборота, основанного на электронной цифровой подписи, как в странах СНГ, так и за рубежом, издано большое количество трудов.

Среди большого числа эмпирических исследований по этой теме необходимо отметить работы Т. Эль-Гамаля, К. Шнорра, М. Рабина, Н. Коблица.

Авторами российских работ, посвященных изучению вопросов формирования электронной цифровой подписи, алгоритмов, используемых для ее получения, а также криптографической стойкости являются Н.А Молдовян, Е.Б. Маховенко, А.Г. Ростовцев, М.А. Еремеева, А.В. Черемушкин.

Одним из недостатков систем электронного документооборота, представленных в современных автоматических системах управления предприятием, является возможность работы и подписи электронного документа только одним пользователем, что увеличивает время обработки и размер электронной цифровой подписи. Предложенное исследование направлено на устранение этого недостатка при использовании электронной цифровой подписи на основе открытого коллективного ключа.

Цель и задачи исследования

Целью диссертации является разработка методики организации защищенного электронного документооборота предприятия.

Для выполнения поставленной цели в работе были сформулированы **следующие задачи**:

− обзор современных систем электронного документооборота, выявление достоинств и недостатков обеспечения информационной безопасности, анализ методов и средств защиты систем электронного документооборота;

− обосновать организацию защищенного электронного документооборота на основе метода электронной цифровой подписи;

− разработать методику формирования и проверки электронной цифровой подписи;

− разработать методику организации защищенного электронного документооборота предприятия.

Область исследования. Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-38 80 04 «Технология приборостроения».

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследований российских и зарубежных ученых по математике, криптографии, а также разработчиков алгоритмов и программного обеспечения, применяемого для обеспечения криптостойкости информации, разработки систем электронного документооборота, а также анализ технических нормативных правовых актов Республики Беларусь в области криптографической защиты информации.

Информационная база исследования сформирована на основе литературы, открытой информации, предоставляемой разработчиками систем электронного документооборота, сведений из ресурсов Интернет, а также материалов научных изданий, конференций и семинаров.

Научная новизна диссертационной работы заключается в разработке методики организации защищенного электронного документооборота предприятия.

Основные положения, выносимые на защиту

1. Систематизация информации о системах электронного документооборота, применяемых методов и средств обеспечения информационной безопасности.

2. Алгоритм выбора параметров электронной цифровой подписи на основе открытого коллективного ключа, позволяющий повысить оперативность обработки информации.

3. Анализ результатов полученной методики организации защищенного электронного документооборота предприятия.

Теоретическая значимость диссертации заключается в обосновании и разработке формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа и криптографических конструкций с использованием эллиптических кривых, позволяющего повысить оперативность совместной обработки электронных документов при сохранении требуемого

уровня защищённости. Представлена методика организации защищенного электронного документооборота предприятия.

Практическая значимость диссертации состоит в разработке методологии организации защищенного документооборота предприятия, возможности его реализации в новых и уже существующих системах документооборота. На основе предложенной методики организации защищенного документооборота предприятия возможно делегирование полномочий на других работников, увеличение эффективности и скорости взаимодействия структурных подразделений.

Апробация и внедрение результатов исследования

Результаты исследования были неоднократно представлены на III Международной научно-практической конференции «Информационные технологии и инновации в образовании и общественных науках – 2017» (ИТИС – 2017, г. Таганрог, Российская Федерация, 2017 г.), XXX Международная научно-практическая конференция «Вектор развития современной науки» (г. Москва, Российская Федерация, 2018 г.), XVI Международной научно-практической конференции «Вопросы современных научных исследований» (г. Омск, Российская Федерация, 2018 г.), VII международной научно-практической конференции «Технические науки: проблемы и решения.» (г. Москва, Российская Федерация, 2018 г.), V международной научно-практической конференции «Проблемы эффективности функционирования технических и информационных систем.» (г. Санкт-Петербург, Российская Федерация, 16 января 2018 г.), LXI международной научно-практической конференции «Научное сообщество студентов XXI столетия. Технические науки». (г. Новосибирск, Российская Федерация, 15 января 2018 г.).

Отдельные положения диссертации могут быть использованы при преподавании дисциплин «Методы и средства защиты информации», «Программные средства защиты информации и защита информации в автоматизированных офисных и банковских системах», «Основы программирования информационных систем», «Технологии программирования».

Публикации

Основные положение работы и результаты диссертации изложены в восьми опубликованных работах общим объемом 30 п.л. (авторский объем 30 п.л.), в том числе две в журналах, входящих в перечень ведущих периодических изданий ВАК, авторским объемом 10 п.л.

Структура и объем работы.

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений. Общий объем диссертации − 130 страниц. Работа содержит 3 таблицы, 4 рисунка. Библиографический список включает 80 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы организации 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 научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В первой главе приведен обзор современных систем электронного документооборота, применяемых на территории Республики Беларусь, проанализированы достоинства и недостатки с точки зрения обеспечения информационной безопасности, показано, что наиболее распространённые системы электронного документооборота реализуют полный набор необходимых функций и предоставляют дополнительные сервисы, расширяющие функциональность, повышающие масштабируемость, надёжность и безопасность.

Функции СЭД в организации показаны на рисунке 1.

Рисунок 1 – Функции СЭД в организации

Рассмотрены методы организации защищенного документооборота, а также особенности организации электронного документооборота на предприятии.

Показано, что внедрение систем электронного документооборота требует подготовленной особым образом инфраструктуры автоматизированной системы управления предприятием и требует значительных затрат на развёртывание и последующее сопровождение.

Отмечается значимость внедрения защищенного электронного документооборота в структуру автоматизированных систем управления предприятием.

Во второй главе при разработке метода формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа предложено использовать групповой закон сложения точек эллиптической кривой.

Структурная схема алгоритма формирования ЭЦП представлена на рисунке 2.

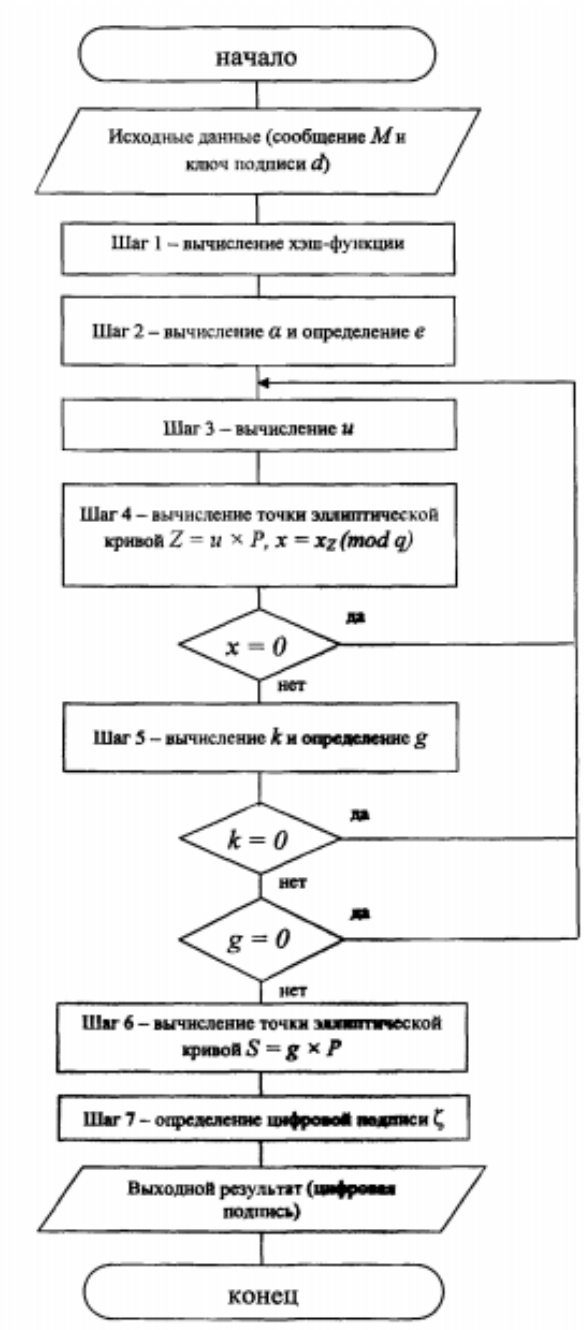

Рисунок 2 – Схема алгоритма формирования подписи

Схема алгоритма проверки ЭЦП приведена на рисунке 3.

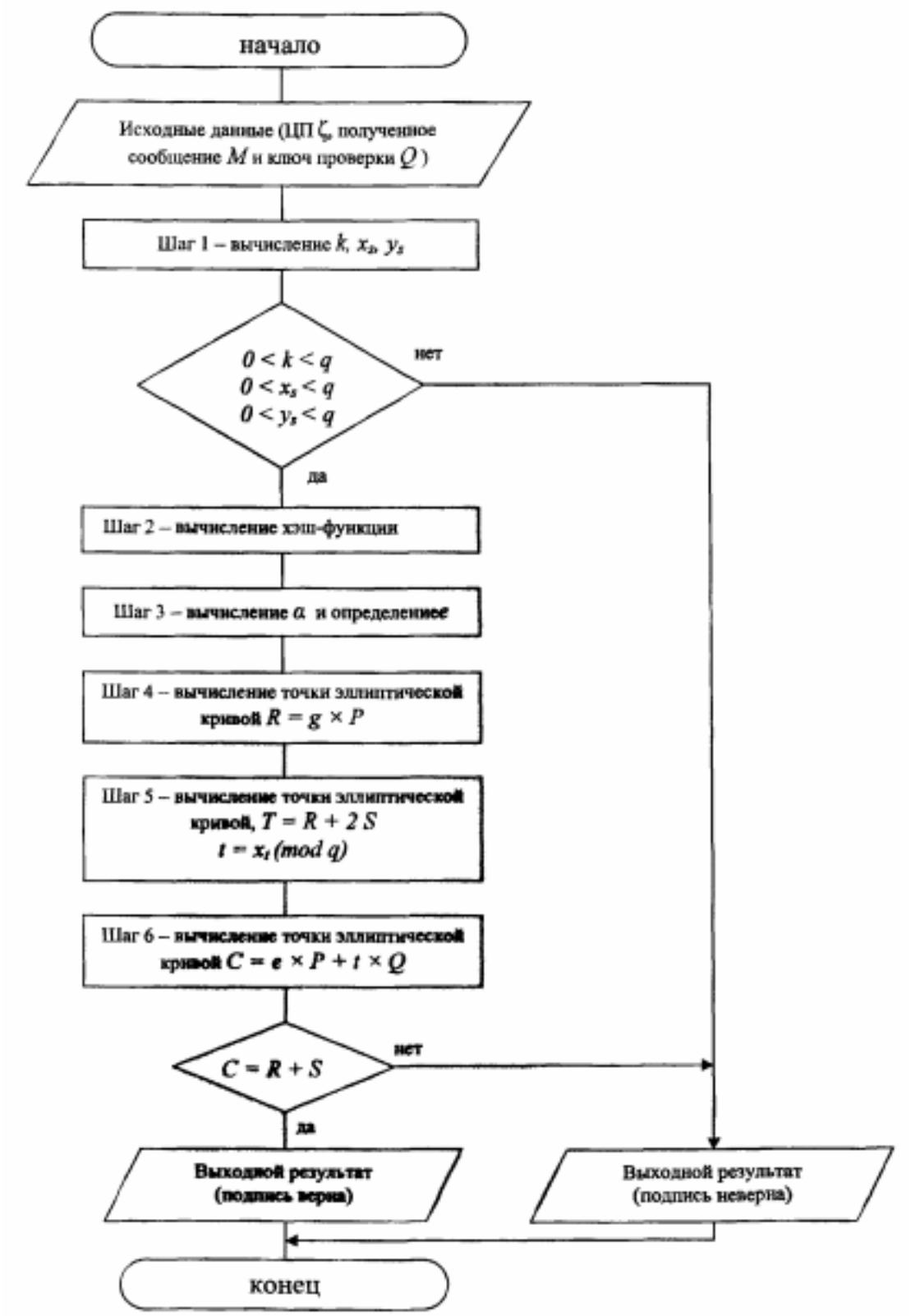

Рисунок 3 – Схема алгоритма проверки подписи

Разработан обобщенный метод формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа, который состоит из трёх этапов: формирования электронной цифровой подписи на основе открытого коллективного ключа на основе генерации индивидуальных параметров подписи и применения функции, отображающих их в коллективный параметр подписи; собственно создание электронной цифровой подписи на основе открытого коллективного ключа и отправка её вместе с электронным документом соответствующим пользователям системы документооборота предприятия; проверка электронной цифровой подписи с использованием открытого коллективного ключа.

Произведено сравнение характеристик обычной и проверки электронной цифровой подписи на основе открытого коллективного ключа для n пользователей, которое показало, что сложность генерации подписи является одинаковой, а сложность проверки электронной цифровой подписи на основе открытого коллективного ключа в n раз меньше.

Исследована реализуемость электронной цифровой подписи с использованием открытого коллективного ключа на основе известных алгоритмов электронной цифровой подписи и показана возможность разработки электронной цифровой подписи на основе открытого коллективного ключа с использованием отечественных стандартов цифровой подписи и схемы Шнорра.

На основе стандарта электронной цифровой подписи СТБ 34.101.45-2013 разработана схема формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа, которая соответствует обобщенному методу электронной цифровой подписи на основе открытого коллективного ключа.

В **третьей главе** диссертационной работы производится разработка алгоритма выбора параметров электронной цифровой подписи на основе открытого коллективного ключа. Выявлен ряд свойств эллиптических кривых, при которых существенно уменьшается стойкость. Результатом выбора параметров электронной цифровой подписи на основе открытого коллективного ключа является уравнение эллиптической кривой с порядком группы, удовлетворяющим требуемой стойкости и скорости преобразования.

Применение данного алгоритма позволяет осуществлять поиск уравнения эллиптической кривой для создания электронной цифровой подписи на основе открытого коллективного ключа с требуемым уровнем стойкости за конечное число шагов с невысокой временной сложностью. Произведена разработка методики организации защищенного электронного документооборота предприятия.

Все разработанные алгоритмы и программы соответствуют государственным стандартам и требованиям безопасности, позволяют строить ЭК, удовлетворяющие криптографическим требованиям, обеспечивают быструю генерацию и проверку цифровой подписи.

Были получены зависимости скорости выполнения различных операций от длины (разрядности) обрабатываемых чисел, скорости генерации параметров КГС от типа кривой, а также зависимости времени поиска секретного

ключа от длины ключа. На основе полученных зависимостей, задавая возможности системы можно определить время, за которое можно осуществить взлом.

Зависимость скорости криптографических преобразований от длины ключа изображена на рисунке 4.

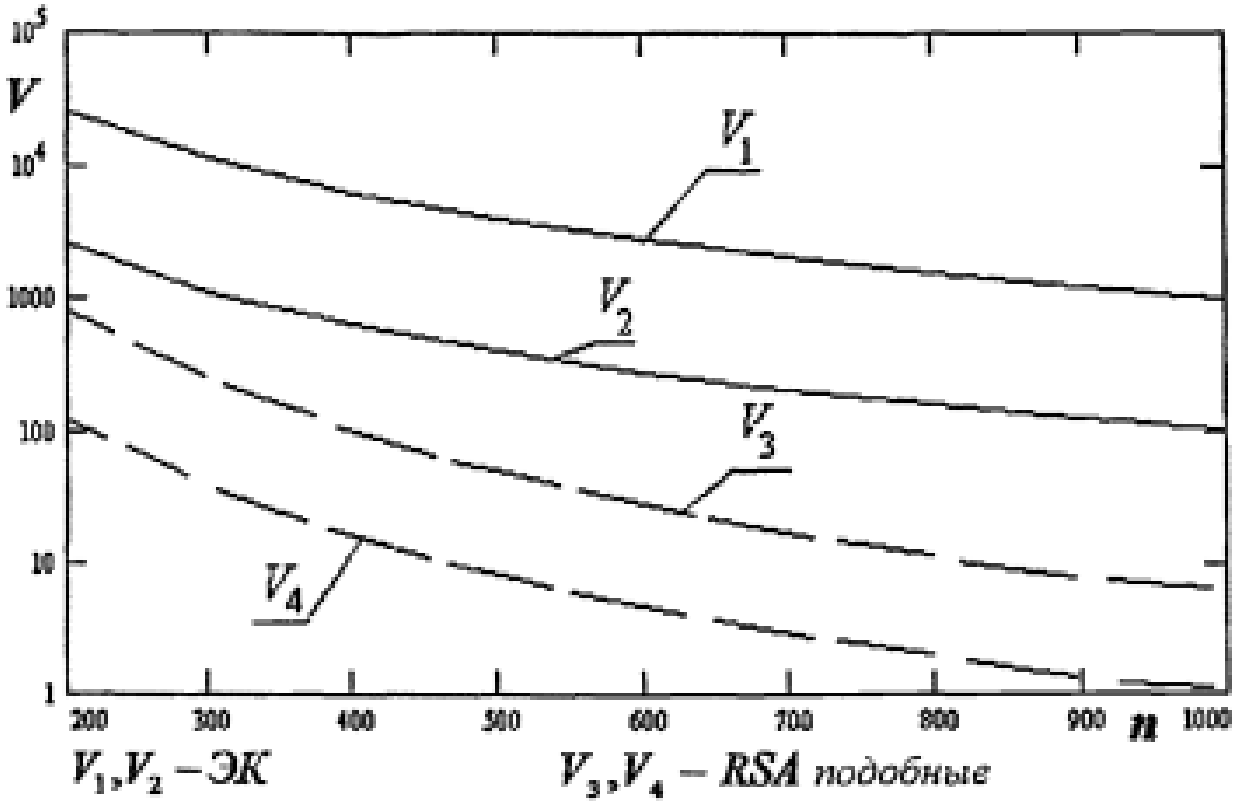

Рисунок 4 – Зависимость скорости криптографических преобразований от длины ключа для различных задач

Преимущество использования ЭК при создании ЭЦП ОКК подтверждается результатами исследования скорости криптографического преобразования V [бит/с] в зависимости от длины ключа n [бит].

В **приложениях** приведен программный код методики формирования и проверки ЭЦП, хеш-функция belt.

ЗАКЛЮЧЕНИЕ

1.Проведен анализ существующих систем электронного документооборота выявлены их основные недостатки и предложены способы их устранения, обоснована целесообразность применения электронной цифровой подписи на основе открытого коллективного ключа в системах защищённого электронного документооборота предприятия.

2. Разработан метод формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа, использующий эллиптическую криптографию. Метод формирования и проверки электронной цифро-

вой подписи на основе открытого коллективного ключа даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер электронной цифровой подписи не увеличивается. Время на подписание документа остается прежним, как и при стандартной процедуре подписи, а время проверки подлинности электронной цифровой подписи уменьшается в *n*- раз пропорционально количеству пользователей, участвующих в создании и подписании документа.

3. Разработан алгоритм выбора параметров электронной цифровой подписи на основе открытого коллективного ключа, основанный на выборе эллиптических кривых, эффективных как по показателю криптостойкости, так и по показателю скорости выполнения криптографического преобразования. Применение данного алгоритма позволит повысить оперативность обработки информации при формировании и проверке электронной цифровой подписи.

4. Разработанный подход к созданию электронной цифровой подписи на основе открытого коллективного ключа не только обеспечивает значительное упрощение процесса аутентификации коллективных документов и повышает оперативность процедуры проверки электронной цифровой подписи, но и придает внутреннюю целостность аутентифицирующей информации.

Предполагаемые области дальнейшего применения электронной цифровой подписи на основе открытого коллективного ключа: разработка крупных проектов, системы коллективного управления, системы управления государственными и силовыми структурами, финансы и бизнес.

Таким образом, в ходе диссертации была разработана методика организации защищенного электронного документооборота предприятия, поставленная научная задача решена, цель диссертационной работы достигнута.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Фисунов, А.В. Обзор мер безопасности в системах электронного документооборота / А.В. Фисунов, М.П. Богатко, В.В. Щеголев // Вопросы современных научных исследований. Сборник материалов XVI международной научно-практической конференции (г. Омск, Российская Федерация, 19 января, 2018 г.).

[2] Богатко, М.П. Анализ комплексных систем защиты информации от несанкционированного доступа / М.П. Богатко, А.В. Фисунов, В.В. Щеголев // Вопросы современных научных исследований. Сборник материалов XVI международной научно-практической конференции (г. Омск, Российская Федерация, 19 января, 2018 г.).

[3] Фисунов, А.В. Алгоритм поиска простых чисел решето Эратосфена / А.В. Фисунов, А.В. Петкун, Е.В. Романов // международный электронный научный журнал Общества Науки и Творчества «Научное знание современности» (ISSN 2541-7827).

[4] Петкун, А.В. Нейронная сеть как средство для распознавания пиксельных изображений цифр банковских карт / А.В. Петкун, Е.В. Романов, А.В.

Фисунов // Технические науки: проблемы и решения. Сборник статей VII международной научно-практической конференции (г. Москва, Российская Федерация, 2018 г.).

[5] Щеголев, В.В. Обзор программных комплексов расчета надежности технических систем / В.В. Щеголев, А.В. Фисунов, М.П. Богатко // Проблемы эффективности функционирования технических и информационных систем. Сборник материалов V международной научно-практической конференции (г. Санкт-Петербург, Российская Федерация, 16 января 2018 г.).

[6] Романов, Е.В. Использование сверточных нейронных сетей для обработки изображений / Е.В. Романов, А.В. Петкун, А.В. Фисунов // LXI международная научно-практическая конференция «Научное сообщество студентов XXI столетия. Технические науки». Сборник статей №1 (г. Новосибирск, Российская Федерация, 15 января 2018 г.), – 2018 г.

[7] Щеголев, В.В. Концепция к постановке задачи принятия решений и выбору альтернатив при создании сложных технических систем / Щеголев В.В., Богатко М.П., Фисунов А.В. // ADVANCED SCIENCE. Сборник материалов II международной научно-практической конференции (Россия, Пенза, 17 января 2018 г.)

[8] Богатко, М. П. Основы оценки соответствия средств защиты информации требованиям, изложенным в технических нормативно-правовых актах / М.П. Богатко, А.В. Фисунов, В.В. Щеголев. // Современные тенденции в науке. Сборник материалов II международной научно-практической конференции (г. Самара, Российская Федерация, 20 января, 2018 г.). – С. 164–168.

РЭЗЮМЭ

Фісуноў Аляксандр Васільевіч

Ключавыя словы: дакументазварот, методыка, электронны лічбавы подпіс, эліптычная крывая.

Мэта работы: распрацоўка методыкі арганізацыі абароненага электроннага дакументазвароту прадпрыемства.

Атрыманыя вынікі і іх навізна: Праведзены аналіз існуючых сістэм электроннага дакументазвароту выяўлены іх асноўныя недахопы і прапанаваны спосабы іх ліквідацыі, абгрунтавана мэтазгоднасць прымянення электроннага лічбавага подпісу на аснове адкрытага калектыўнага ключа ў сістэмах абароненага электроннага дакументазвароту прадпрыемства.

Распрацаваны метад фарміравання і праверкі электроннага лічбавага подпісу на аснове адкрытага калектыўнага ключа, які выкарыстоўвае эліптычную крыптаграфію. Метад фарміравання і праверкі электроннага лічбавага подпісу на аснове адкрытага калектыўнага ключа дае магчымасць апрацоўкі і падпісання дакумента адначасова некалькімі карыстальнікамі. Пры гэтым памер электроннага лічбавага подпісу не павялічваецца. Час на падпісанне дакумента застаецца ранейшым, як і пры стандартнай працэдуры подпісы, а падчас праверкі сапраўднасці электроннай лічбавай подпісы памяншаецца ў *n*- раз прапарцыйна колькасці карыстальнікаў, якія ўдзельнічаюць у стварэнні і падпісанні дакумента.

Распрацаваны алгарытм выбару параметраў электроннага лічбавага подпісу на аснове адкрытага калектыўнага ключа, заснаваны на выбары эліптычных крывых, эфектыўных як па паказчыку крыптаўстойлівасці, так і па паказчыку хуткасці выканання крыптаграфічнага пераўтварэнні. Ужыванне дадзенага алгарытму дасць магчымасць павысіць аператыўнасць апрацоўкі інфармацыі пры фарміраванні і праверцы электроннай лічбавай подпісы.

Распрацаваны падыход да стварэння электроннага лічбавага подпісу на аснове адкрытага калектыўнага ключа не толькі забяспечвае значнае спрашчэнне працэсу аўтэнтыфікацыі калектыўных дакументаў і павышае аператыўнасць працэдуры праверкі электроннага лічбавага подпісу, але і надае ўнутраную цэласнасць аутентифицирующей інфармацыі.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс Беларускага дзяржаўнага універсітэта інфарматыкі і радыёэлектронікі ў лекцыйныя курсы «Метады і сродкі абароны інфармацыі», «Праграмныя сродкі абароны інфармацыі і абарона інфармацыі ў аўтаматызаваных офісных і банкаўскіх сістэмах».

Вобласць ужывання: кіраванне прадпрыемствам, інфармацыйная бяспека, крыптаграфія.

РЕЗЮМЕ

Фисунов Александр Васильевич

Ключевые слова: документооборот, методика, электронная цифровая подпись, эллиптические кривые.

Цель работы: разработка методики организации защищенного электронного документооборота предприятия.

Полученные результаты и их новизна: Проведен анализ существующих систем электронного документооборота выявлены их основные недостатки и предложены способы их устранения, обоснована целесообразность применения электронной цифровой подписи на основе открытого коллективного ключа в системах защищённого электронного документооборота предприятия.

Разработан метод формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа, использующий эллиптическую криптографию. Метод формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер электронной цифровой подписи не увеличивается. Время на подписание документа остается прежним, как и при стандартной процедуре подписи, а время проверки подлинности электронной цифровой подписи уменьшается в n- раз пропорционально количеству пользователей, участвующих в создании и подписании документа.

Разработан алгоритм выбора параметров электронной цифровой подписи на основе открытого коллективного ключа, основанный на выборе эллиптических кривых, эффективных как по показателю криптостойкости, так и по показателю скорости выполнения криптографического преобразования. Применение данного алгоритма позволит повысить оперативность обработки информации при формировании и проверке электронной цифровой подписи.

Разработанный подход к созданию электронной цифровой подписи на основе открытого коллективного ключа не только обеспечивает значительное упрощение процесса аутентификации коллективных документов и повышает оперативность процедуры проверки электронной цифровой подписи, но и придает внутреннюю целостность аутентифицирующей информации.

Степень использования: результаты внедрены в учебный процесс Белорусского государственного университета информатики и радиоэлектроники в лекционные курсы «Методы и средства защиты информации», «Программные средства защиты информации и защита информации в автоматизированных офисных и банковских системах».

Область применения: управление предприятием, информационная безопасность, криптография.

ABSTRACT

Fisunov Alexander Vasilyevich

Keywords: document management, methodology, electronic digital signature, elliptical curves.

The object of study: development of methods for organizing secure electronic document management of the enterprise.

The result and novelty: The analysis of the existing electronic document management systems revealed their main shortcomings and suggested ways to eliminate them, justified the advisability of using an electronic digital signature based on an open collective key in the systems of the protected electronic workflow of the enterprise.

A method for generating and verifying an electronic digital signature based on an open collective key using elliptical cryptography is developed. The method of forming and verifying an electronic digital signature based on an open collective key makes it possible to process and sign the document simultaneously by several users. At the same time, the size of the electronic digital signature does not increase. The time for signing the document remains the same as for the standard signature procedure, and the time for authenticating the electronic digital signature is reduced by n times in proportion to the number of users participating in the creation and signing of the document.

An algorithm for selecting parameters of an electronic digital signature based on an open collective key is developed, based on the choice of elliptic curves effective both in terms of the cryptographic stability index and the rate of performance of the cryptographic transformation. The application of this algorithm will improve the efficiency of information processing when creating and verifying an electronic digital signature.

The developed approach to the creation of an electronic digital signature based on an open collective key not only provides a significant simplification of the process of authenticating collective documents and increases the efficiency of the procedure for verifying an electronic digital signature, but also imparts the internal integrity of authenticating information.

Degree of use: results are introduced in the educational process of the Belarussian State University of Informatics and Radio Electronics in the "Methods and means of information protection" and "Software tools for protecting information and protecting information in automated office and banking systems" lecture courses.

Sphere of application: enterprise management, information security, cryptography.