МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА
МЕХАНИКО—МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Лёвин Валерий Юрьевич

Развитие методов и средств обеспечения целостности и конфиденциальности регистрируемой информации системы информационной безопасности организации воздушного движения

Специальность: 05.13.19 — методы и системы защиты информации, информационная безопасность

Автореферат

диссертации на соискание ученой степени
кандидата физико—математических наук

Москва 2010

Работа выполнена на кафедре Математической теории интеллектуальных систем Механико—математического факультета Московского государственного университета имени М.В. Ломоносова.

Научный руководитель:	кандидат физико—математических наук *Носов Валентин Александрович*
Официальные оппоненты:	доктор физико-математических наук, профессор *Фомичев Владимир Михайлович*
	кандидат физико-математических наук, доцент *Применко Эдуард Андреевич*
Ведущая организация:	ФГУП "НИИ"Квант"

Защита диссертации состоится 29 декабря 2010 г. в 16 час. 45 мин. на заседании диссертационного совета Д 501.002.16 при Московском государственном университете имени М.В. Ломоносова по адресу: Российская Федерация, 119991, Москва, ГСП—1, Ленинские горы, д. 1. Московский государственный университет имени М.В. Ломоносова, Механико—математический факультет, ауд. 14—08.

С диссертацией можно ознакомиться в библиотеке Механико—математического факультета Московского государственного университета имени М.В. Ломоносова (Главное здание МГУ, 14 этаж).

Автореферат разослан 29 ноября 2010 г.

Ученый секретарь
диссертационного совета
Д 501.002.16 при МГУ,
доктор физико—математических наук Корнев А. А.

Общая характеристика работы

Актуальность работы. Стремительное развитие информационных технологий оказывает существенное влияние на все стороны жизни государства и общества. Эпоха массовых коммуникаций, технологии Интернет, информатизация управления технологическими процессами в различных сферах деятельности человека привели к резкому возрастанию потребности в обеспечении информационной безопасности. В Концепции федеральной целевой программы: "Обеспечение безопасности полетов воздушных судов государственной авиации Российской Федерации в 2010—2014 годах", утвержденной Распоряжением Правительства РФ от 22 апреля 2009 года №554—Р особое внимание уделяется развитию инфраструктуры информационной безопасности единой информационно—аналитической системы для обеспечения, обработки, анализа и документирования параметрической, аудио— и видеоинформации в интересах предупреждения и расследования авиационных происшествий. При создании средств объективного контроля подобных информационно—аналитических систем управления, обеспечение целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи, является одной из ключевых задач. Непрерывное совершенствование вычислительной техники постоянно расширяет набор требований, предъявляемых к алгоритмам цифровой подписи и протоколам на их основе, решающим поставленные задачи. Для обеспечения необходимого уровня безопасности протоколов и, соответственно, алгоритмов цифровой подписи, наряду с традиционными подходами на основе сложности решения задач факторизации и дискретного логарифмирования, все чаще рассматривают группу точек эллиптической кривой[1], которая, несмотря на свою сложную структуру, по целому ряду показателей удобна для вычислений. Однако, при решении задач в такой постановке должен применяться системный подход, согласно которому, под методом цифровой подписи понимаются не только асимметричный алгоритм подписи, но и сопутствующие выработке цифровой подписи алгоритмы расчета уникального хеш—значения, организации ключей, подбора необходимых технологических параметров и ряд других факторов. Вместе с тем, исследования показывают, что результатов практического характера, целью которых является использование эллиптической кривой в протоколах цифровой подписи повышенной безопасности и быстродействия, недостаточно. Необходимо отметить, что Постановлением Правительства РФ от 18 июня 1998 года № 605 (ст. 1, п. 4) определено: "Единая система организации воздушного движения Российской Федерации имеет стратегическое значение для безопасности государства". Отмеченные выше обстоятельства определяют актуальность настоящей работы.

[1]N.Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48, 1987.

V.Miller, Uses an elliptic curves in cryptography, Advances in Cryptology: Proceedings of CRYPTO'85, Lecture notes in computer science 218, 1986, Springer—Verlag, 417—426.

Цель диссертационной работы состоит в разработке программных средств на основе совершенствования алгоритмов цифровой подписи на эллиптических кривых, решающих задачу обеспечения целостности и конфиденциальности информации в процессе ее сбора, хранения и передачи в рамках системы информационной безопасности организации воздушного движения.

Для достижения поставленной цели в диссертации сформулированы и решаются следующие задачи.

- Совершенствование стандартов цифровой подписи на основе эллиптических кривых, решающих задачу обеспечения целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи в рамках системы информационной безопасности организации воздушного движения.
- Исследование модели эллиптической кривой с целью получения формулы, позволяющей разработчику повысить точность определения размеров используемых в протоколах цифровой подписи автоматизированной системы управления ключей.
- Построение алгоритмов кодирования данных точками эллиптических кривых, пригодных для применения в системах реального времени.
- Создание математических методов совершенствования и модификации однонаправленных хеш—функций с целью повышения их эффективности при программно—аппаратных реализациях.
- Разработка и тестовые испытания комплекса программно—аппаратных средств, решающих задачу обеспечения целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи, и отвечающих требованиям системы информационной безопасности организации воздушного движения.

Цель настоящей работы и перечисленные задачи соответствуют областям исследований в сфере информационной безопасности, а именно—развитию моделей и методов обеспечения целостности и конфиденциальности цифровой информации для формирования на их основе программных средств противодействия нарушениям конфиденциальности и целостности информации, циркулирующей в автоматизированных системах объективного контроля организации воздушного движения в интересах предотвращения и расследования авиационных происшествий. Эти исследования отражены в п.п. 2,6,13 Паспорта специальности 05.13.19 — "Методы и системы защиты информации, информационная безопасность."

Научная новизна результатов диссертации состоит в развитии методов использования модели эллиптической кривой в протоколах цифровой подписи,

применяющихся для защиты целевой системы, а также в усовершенствовании однонаправленных хеш—функций с целью повышения их устойчивости к различным методам компрометации: генерация коллизий; "нехватка"ключей; разглашение служебных параметров; нарушение целостности и ряд других. Предложено улучшение метода Шнайера борьбы с туннельными коллизиями хеш—функций. Создан мультиключевой алгоритм реализации хеш—функций, при котором ключ может обновляться на каждом раунде, что позволило существенно увеличить порядок ключевого множества. На основе метода Полларда получена формула расчета длин ключей, позволяющая определять уровень безопасности систем на основе эллиптических кривых. Применен системный подход к созданию эффективных средств обеспечения целостности и конфиденциальности информации, объединяющий полученные результаты по однонаправленным хеш—функциям, ключевой подсистеме, по схемам цифровой подписи и выработке технологических параметров.

Практическая значимость диссертационной работы заключается в разработанных автором в интересах системы обеспечения информационной безопасности организации воздушного движения методах построения безопасных протоколов цифровой подписи на основе эллиптических кривых, в создании эффективных, с позиции программно—аппаратных реализаций, алгоритмов построения однонаправленных хеш—функций. По результатам диссертационной работы автором спроектирован и реализован комплекс средств по работе с эллиптическими кривыми, однонаправленными хеш—функциями, протоколами цифровой подписи. При решении задачи обеспечения целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи, удалось конструктивно решить вопрос создания резерва ключей, "отсечении"недоверенной стороны, оперативной модификации и противодействия различным методам компрометации. Результаты диссертации используются при разработке автоматизированной системы управления полетами, навигации, посадки и связи для аэродромов государственной авиации (далее именуемой АСУП НПС или целевой системой).

На защиту выносятся следующие основные результаты.

- Усовершенствованные методы использования модели эллиптической кривой с целью построения схем цифровой подписи, устойчивых к изначальной фальсификации, внедрению скрытых каналов передачи данных и других методов компрометации. Формула расчета, повышающая точность определения размеров применяющихся в протоколах цифровой подписи ключей.

- Алгоритмы кодирования данных точками эллиптических кривых, которые используются для создания на их основе программных средств, реализующих эти алгоритмы в реальном времени и позволяющих применять

в целевой системе протоколы выработки общих ключей и передачи информации на основе эллиптических кривых.

- Мультиключевой алгоритм построения хеш—функций, при котором ключ может обновляться на каждом раунде, методы построения эффективных программно—аппаратных реализаций однонаправленных хеш—функций, решающие задачи отсечения "недоверенной"стороны, "нехватки"и создания резерва ключей, а также задачи защиты от коллизий и долговременного поддержания высокого уровня безопасности информационной системы.

- Комплекс программно—аппаратных средств, обеспечивающий целостность и конфиденциальность цифровой информации в процессе ее сбора, хранения и передачи в рамках системы информационной безопасности организации воздушного движения, прошедший тестовые испытания и отвечающий предъявляемым к нему требованиям.

Основные методы исследований. В диссертации использованы методы информационной безопасности, теории чисел, комбинаторики, компьютерной алгебры, теории эллиптических кривых, теории конечных полей, теории блочных шифров, теории однонаправленных хеш—функций, теории протоколов цифровой подписи, теории сложности алгоритмов, а также методы программной инженерии.

Внедрение результатов работы. Результаты диссертации нашли свое применение при разработке "Автоматизированной системы управления полетами, навигации, посадки и связи аэродромов государственной авиации"(ОКР шифр—"Рейс—2000"). Получен Акт от одного из ведущих предприятий по созданию программно—аппаратных комплексов управления воздушным движением — ОАО НПО "Лианозовский Электромеханический Завод"Концерна ПВО "Алмаз—Антей"об использовании результатов разработки методов и средств обеспечения целостности и конфиденциальности регистрируемой информации.

Апробация работы. Результаты работы неоднократно докладывались на семинарах механико—математического факультета МГУ им. М.В. Ломоносова "Теория автоматов"(2007-2010 гг.) под руководством профессора В.Б. Кудрявцева и на семинарах ВМиК (2010), совместно с Институтом проблем информационной безопасности МГУ им. М.В.Ломоносова под руководством доцента Э.А. Применко, а также на следующих научных конференциях: научная конференция "Ломоносовские чтения"(Москва, МГУ им. Ломоносова, апрель 2007); IX международный семинар "Дискретная математика и её приложения", посвященный 75-летию со дня рождения академика О.Б.Лупанова (2007); третья научная конференция студентов и аспирантов кафедры МаТИС механико-математического факультета МГУ (Москва, МГУ им. Ломоносова, май 2007); научная конференция "Ломоносовские чтения"(Москва, МГУ им. Ломоносова,

апрель 2008); Международная научная конференция "Современные проблемы математики, механики и их приложений"посвященная 70—летию ректора МГУ академика В.А.Садовничего (март 2009).

Публикации. По теме диссертации опубликовано 4 работы, из которых 3 [1,2,4]—в журналах из перечня ведущих рецензируемых изданий, рекомендованных ВАК РФ.

Структура и объем работы. Работа состоит из введения, пяти глав, заключения, списка литературы и приложения. Общий объем диссертации составляет 116 страниц (вместе с приложениями—132 страницы). Список литературы включает 109 наименований.

Краткое содержание работы

Во введении описываются цели работы, обосновывается ее актуальность и практическая значимость, перечисляются основные результаты исследований.

Первая глава является вводной и содержит описание некоторых важных в контексте целей диссертационной работы методов обеспечения целостности и конфиденциальности цифровой информации в рамках построения автоматизированной системы управления полетами, навигации, посадки и связи для аэродромов государственной авиации.

В первом разделе главы с высокой степенью детализации формулируется постановка задачи, определяются требования к ее решению. Особое внимание уделяется обеспечению целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи, как одному из важнейших аспектов системы управления объектом, который в контексте данной работы является целевым. Решения поставленной задачи должны соответствовать требованиям, изложенным в РД ФСТЭК России "Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации"и "Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей", тактико—техническому заданию на составную часть опытно—конструкторской работы "Автоматизированная система управления полетами, навигации, посадки и связи для аэродромов государственной авиации"(шифр ОКР "Рейс—2000"), а также требованиям нормативной и методологической документации Министерства обороны Российской Федерации в области создания средств защиты информации. Вводится понятие надежности схем цифровой подписи и использующих их протоколов, под которой, в контексте данной диссертационной

работы, понимается их устойчивость: к изначальной фальсификации информации; внедрению скрытых каналов передачи данных; к "нехватке"ключей; к проведению внедренными программными агентами вредоносного мониторинга системы АСУП НПС; к последствиям разглашения оперативных параметров "недоверенной"стороне и к имеющийся тенденции снижения уровня информационной безопасности целевой системы.

Во втором разделе первой главы проведено исследование применяющихся на практике методов решения задачи обеспечения целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи. Вводятся определение и основные требования, которым должна удовлетворять цифровая подпись. Для исследования указанных способов решения задачи в работе применяется системный подход, вследствии чего под методом цифровой подписи понимается не только асимметричный алгоритм, но и весь комплекс алгоритмов, сопутствующих составлению уникальной цифровой подписи. Производится детальное формальное описание применяющихся на практике методов цифровой подписи, как суперпозиции нескольких отображений $\mathfrak{S}ig\left(h\left(\mathfrak{M}\right)\right)$, где $\mathfrak{M} \in \{0,1\}^*$ и $h : \{0,1\}^* \to \{0,1\}^\delta, \delta \in \mathbb{N}$, $\mathfrak{S}ig : \{0,1\}^\delta \to \mathfrak{S}$, $\mathfrak{V}er : \{0,1\}^\delta \times \mathfrak{S} \to \{0,1\}$ Функция h, является однонаправленной хеш—функцией порядка $\delta, \delta \in \mathbb{N}$, а $\mathfrak{S}ig\ \mathfrak{V}er$—схематичное представление алгоритмов верификации и генерации цифровой подписи. Подобные функции широко применяются в цифровых устройствах регистрации информации с целью составления уникального идентификационного кода цифрового сообщения и по построению должны обладать некоторыми важными свойствами такими, как однонаправленность, устойчивость к коллизиям, устойчивость к нахождению второго прообраза. С целью обеспечения целостности и конфиденциальности данных управляющей системы в процессе хранения, передачи, пакетного обмена, а также для принятия важных распоряжений и контроля правильности отдачи команд, проведено исследование применяющихся на практике способов построения однонаправленных бесключевых хеш—функций $h(\mathfrak{M}) : \{0,1\}^* \to \{0,1\}^\delta$ *manipulation detection code (MDC)* и ключевых хеш—функций $h(\mathfrak{M}) : \{0,1\}^* \times \{0,1\}^k \to \{0,1\}^\delta$ *message authentication code (MAC)* порядка $\delta \in \mathbb{N}$. Отмечено, что расчет значения подобных функций является первым, ключевых этапом составления цифровой подписи сообщения $\mathfrak{M} \in \{0,1\}^*$. Проведен всесторонний анализ MDC, MAC хеш—функции, применяющихся в системе управления с целью "отсечения"недоверенной стороны, выявления изменения и умышленной фальсификации данных. Установлено, что данные хеш—функции надежны, только когда в протоколе участвуют доверяющие друг другу стороны. Приводятся анализ и описание основных недостатков, использования однонаправленных хеш—функций в рамках единого метода цифровой подписи. Исследован процесс построения однонаправленных хеш—функций.

Пусть $\mathfrak{M} \in \{0,1\}^*$—сообщение, для получения хеш—значения $h\left(\mathfrak{M}\right)$ оно специальным образом разбивается на блоки фиксированной длины m. Обозна-

чим через $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3, \ldots, \mathfrak{M}_N, N \in \mathbb{N}$ разбиение первоначального сообщения $\mathfrak{M}$ на указанные блоки, а через $f()$—сжимающую функцию. В данном случае стандартный алгоритм построения хеш—функции $h(\mathfrak{M})$ может быть записан в виде итерационного процесса:

$$\begin{array}{l} H_0 = \nu; \\ H_i = f(\mathfrak{M}_i, H_{i-1}),\ i = 1, \ldots, N; \\ h(\mathfrak{M}) = H_N; \end{array} \qquad (1)$$

в котором ν—некоторый фиксированный начальный вектор. Если функция $f()$ зависит от ключа, то ν можно положить равным нулевому вектору. В противном случае, для исключения возможности перебора коротких сообщений (при попытках обращения хеш—функции), ν составляется из фрагментов, указывающих дату, время, номер сообщения и другие уникальные признаки. Положив в (1) $f(\mathfrak{M}_i, H_{i-1}) = E_K(\mathfrak{M}_i \oplus H_{i-1}),\ i = 1, \ldots, N,$, где E_K—алгоритм блочного шифрования с ключом K, получим известную схему шифрования со сцеплением блоков, где в качестве результата берется не весь текст $H_1, H_2, H_3, \ldots, H_N$, а только последний блок H_N. Такой режим в ГОСТе 28147-89 назван режимом выработки имитовставки. На основе проделанного исследования установлено отсутствие методов построения эффективных программно—аппаратных реализаций хеш—функций, с целью использования их в целевой системе АСУП НПС. По мере накопления статистического материала об использовании хеш—функций, например, MD4, MD5, SHA-1, RIPEMD-160, HAVAL и других, с применением злоумышленником линейного и дифференциального анализа, атак на основе туннельного эффекта, парадокса дней рождений, грубой силы, встреч посередине уровень информационной безопасности данной системы снижается. Возможность применения на практике методов, успешно компрометирующих распространенные хеш—функции, делает ненадежным использование их в подобной системе. Однако большинство хеш—функций хранится и используется в виде служебных библиотек, уникальных аппаратных реализаций, и, как следствие, пользователю не представляется возможность изменять их уникальную архитектуру. Следовательно хеш—функции, предполагаемые для использования в рамках инфраструктуры системы управления, которая рассматривается в качестве целевой, нуждаются в совершенствовании и модификации с целью построения эффективных программно—аппаратных реализаций (в указанном выше смысле). Установлено, что использование модифицированных блочных шифров в схеме (1) ($f(\mathfrak{M}_i, H_{i-1}) = E_{K_1,K_2}(\mathfrak{M}_i \oplus H_{i-1})$), позволяет решить, возникающую при работе системы, задачу "нехватки"ключей и создать их резерв. Необходимо обратить внимание на то обстоятельство, что имеющиеся на настоящее время результаты на этом направлении носят разрозненный характер и не позволяют строить сложные системы управления критически важными объектами.

В третьем и четвертом разделах проведено исследование имеющихся протоколов и стандартов цифровой подписи DSA, DSS, El—Gamal, ГОСТ Р 34.10—

94, ECDSA, ECEl—Gamal, ГОСТ Р 34.10—01. Приведена аргументация необходимости обоснования использования эллиптической кривой, как оптимальной основы для построения безопасных протоколов цифровой подписи целевой системы. Установлено, что перечисленные стандарты являются модификацией схемы Эль—Гамаля (ECELDSA) цифровой подписи, обладающей определенными недостатками. Показана уязвимость указанной схемы к изначальной фальсификации сообщений и внедрению скрытых каналов передачи информации. Выявленные недостатки не позволяют использовать указанные стандарты цифровой подписи в системе управления объектом защиты и снижают общий уровень информационной безопасности. Отмечается отсутствие должной строгости метода определения размеров ключей в схемах цифровой подписи на основе эллиптических кривых, удовлетворяющий требованиям предъявляемым к ним целевой системой. Показана важность обеспечения анонимности подписывающей стороны и минимизации разглашения служебных параметров. Решение поставленных вопросов затрудняет использование перехвата и навязывания ложной информации, а также усложняет ведение злоумышленником мониторинга в инфраструктуре АСУП НПС, что должно быть учтено при построении системы в интересах предупреждения и расследования авиационных происшествий.

В пятом разделе приведены выводы и основные этапы решения поставленных задач, а также схема типов информационных потоков АСУП НПС. Подчеркнута важность и актуальность решения каждой из вспомогательных задач, определены их роли в системе управления.

Представленные в первой главе результаты исследований свидетельствуют об актуальности рассматриваемых в диссертационной работе задач.

Во второй главе рассматривается построение алгоритмов кодирования данных точками эллиптических кривых. Для применения систем передачи информации и выработки общих ключей на основе эллиптических кривых в АСУП НПС в полном объеме, необходимо создать алгоритмы представления данных (цифровая информация, ключи и других) в виде набора точек. Однако эффективных на практике, способных работать в реальном масштабе времени, алгоритмов представления не разработано, несмотря на то, что впервые о необходимости такого представления было заявлено еще в 1985 Н. Коблицом и В. Миллером. Обозначим через F конечное поле $\mathbb{F}_q = GF(q)$, где $q = p^n, n \in \mathbb{N}$, p—простое число.

Определение 1. *Пусть $x^3 + a_2x^2 + a_4x + a_6$—многочлен без кратных корней. Эллиптической кривой $E(F)$ над полем F называется множество точек $(x, y) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in F$, $i = 1, 2, 3, 4, 6$, вместе с единственным бесконечно удаленным элементом.*

В зависимости от значения характеристики конечного поля F, уравнение эллиптической кривой может приобретать различные виды, приведенные в таб-

лице 1. Если $\mathrm{char}F > 3$, то кривую принято называть эллиптической кривой в

Значение характеристики поля	Вид уравнения эллиптической кривой
$\mathrm{char}F = 2$	$y^2 + cy = x^3 + ax + b$ $y^2 + xy = x^3 + ax^2 + b$
$\mathrm{char}F = 3$	$y^2 = x^3 + ax^2 + bx + c$
$\mathrm{char}F > 3$	$y^2 = x^3 + bx + c$

Таблица 1. Уравнения всевозможных видов эллиптических кривых.

форме Вейерштрасса [2].

Определение 2. *Пусть над полем $\mathbb{F}_p$ заданы две эллиптические кривые: E_{ab} : $y^2 = x^3 + ax + b$ и $E_{a'b'} : y^2 = x^3 + a'x + b'$, $a, b, a', b' \in \mathbb{F}_p$,$a' = v^2a$, $b' = v^3b$, где $v \in \mathbb{F}_p$—квадратичный невычет по модулю p. Тогда такие кривые назовем дуальными.*

Дуальные кривые обладают некоторыми свойствами, позволяющими автору решить поставленную задачу представления. Например, пусть E_{ab}, и $E_{a'b'}$— две дуальные эллиптические кривые над полем $\mathbb{F}_p$. Известно, что тогда справедливо соотношение $\#E_{ab} + \#E_{a'b'} = 2p + 2$. Для построения эффективных алгоритмов кодирования, введем следующее вспомогательное определение.

Определение 3. *Дискретным спектром поля $\mathbb{F}_p$ назовем числовой отрезок вида $]p + 1 - 2\sqrt{p}[, \ldots, p + 1, \ldots, [p + 1 + 2\sqrt{p}]$ с приписанным каждой точке N этого отрезка количеством эллиптических кривых, на которых N точек.*

Установлена, симметрия дискретного спектра конечного поля относительно его центра (числа $p + 1$ указанного в определении 3 отрезка). На основании представленных в диссертационной работе математических рассуждений, автором разработаны детерминированные и вероятностные алгоритмы кодирования, решающие представленную выше задачу представления.

Рассмотрим простое поле $F = \mathbb{F}_p$, эллиптическую в форме Вейерштрасса над этим полем и конечный алфавит $A = \{a_0, a_2, \ldots, a_{M-1}\}$. Закодируем произвольный номер m точкой $P_m(x, y)$, переводя, тем самым, буквы алфавита A в набор точек на эллиптической кривой. Отображение, которое будет построено, является *инъективным*, однако оно обладает тем свойством, что по координатам точки $P_m(x, y)$ однозначно восстанавливается число m, которому она соответствует. Следовательно, корректно определен процесс декодирования.

Построим вероятностный алгоритм кодирования числа $m \in [0, \ldots, M - 1]$ точкой $P_m(x, y)$ эллиптической кривой $y^2 = f(x) = x^3 + ax + b, a, b \in \mathbb{F}_p$ и

[2] J.Silverman, The arithmetic of elliptic curves, Springer—Verlag, 1986.

соответствующий процесс декодирования. Положим $p > M\kappa$, где κ - достаточно большое целое число[3]. Записываем числа от 1 до $M\kappa$ в виде $m\kappa + j, 1 \leq j \leq \kappa$, после чего вычисляем символ Лежандра $\left(\frac{f(m\kappa+j)}{p}\right)$, если при этом он равен 1, то этот факт означает, что найдена соответствующая точка $P_m(m\kappa + j, \bar{y})$. В этом случае, $\bar{y}$—такое число, что $\bar{y}^2 \equiv f(m\kappa+j)(\mod p)$. Если при вычислении символ Лежандра равен -1, то увеличиваем j на единицу и повторяем процесс. С вероятностью $1 - \frac{1}{2^\kappa}$ такое представление будет найдено. Восстановление m производится по формуле: $m = \begin{cases} \frac{x - x(\mod \kappa)}{\kappa} & \text{если } j \neq \kappa; \\ \frac{x-\kappa}{\kappa} & \text{если } j = \kappa. \end{cases}$

Построим детерминированный алгоритм кодирования конечных алфавитов точками эллиптических кривых. Пусть v—квадратичный невычет, две дуальные кривые E_{ab} и $E_{a'b'}$, $m \in [0, \ldots, M-1]$—число которое мы хотим закодировать. Рассмотрим удвоенный отрезок: $[0, \ldots, 2M-2]$. Введем вспомогательные обозначения $g(x) = x^3 + ax + b$, $g_v(x) = x^3 + a'x + b'$. Последовательно, начиная с 0 до $2M-2$, вычисляем символ Лежандра $\left(\frac{g(m)}{p}\right), m \in [0, \ldots, 2M-2]$, если $\left(\frac{g(m)}{p}\right) = 1$, то данному числу соответствует точка на первой кривой, а если $\left(\frac{g(m)}{p}\right) = -1$, то данному числу соответствует точка на второй кривой, т.к., справедливо соотношение $g_v(x) = v^3 g\left(\frac{x}{v}\right)$. Заметим, что если $\left(\frac{g(m)}{p}\right) = -1$, то $g(m)$—квадратичный невычет по модулю p, но тогда $g_v(mv)$ будет являться квадратичным вычетом, верно и обратное. Свойство быть вычетом или невычетом равносильно существованию на соответствующей эллиптической кривой точки $P_m(x, y)$, в которую переводится число m. Дойдя до $2M-2$, выбираем ту кривую, на которой вычетов больше или равно M. Заметим, что подстановка x в $E_{a'b'}$ равносильна подстановки $\left(\frac{x}{v}\right)$ в E_{ab}. В результате работы этого алгоритма в памяти реализующей его ЭВМ получим вид кривой и соответствующую подстановку. Использование автором перечисленных выше результатов, позволило в АСУП НПС в полной мере применять как перспективные системы выработки общих ключей и передачи цифровых сообщений на основе эллиптических кривых, так и протоколы цифровой подписи.

В третьей главе в интересах целевой системы, проведено исследование возможности использования модели эллиптической кривой для построения надежных (в смысле, введенном в главе 1) схем цифровой подписи. Для поддержа-

[3]Последнее число характеризует вероятность отсутствия представления и равна $\frac{1}{2^\kappa}$. Для практических целей положим $\kappa = 20$ или $\kappa = 50$.

ния комплексов информационной безопасности объекта на должном уровне, во многих странах используют официальные руководства RSA Security. Указанные руководства носят рекомендательный характер и основаны на результатах сравнительного анализа различных стандартов. Основой для составления подобных таблиц служит метод увеличения размеров ключей. Показано, что подобный метод не решает поставленную задачу, а наоборот, из—за использования сложной арифметики делает использование систем затруднительным в АСУП НПС. На основе проведенного исследования возможности применения модели эллиптической кривой, как метода, повышающего уровень безопасности систем, и использующего при этом ключи существенно меньшей длины. Получена формула, позволяющая разработчику выбирать размер ключей целевой системы.

В теории чисел принято представлять сложность алгоритма в виде функции от длины входа, то есть от количества бит n, необходимых для записи входных данных. Если эта функция представляет собой многочлен от n, то алгоритм имеет *полиномиальную* сложность, если эта функция имеет вид $e^{Cn},\ c = const$, то сложность—*экспоненциальна.* Для определения *субъэкспоненциальной* сложности введем функцию:

$$L_p(\mu, c) = \exp\left(c(\ln p)^{\mu}(\ln\ln p)^{1-\mu}\right). \tag{2}$$

При $\mu = 0$, функция (2) полиномиальна по $\ln p$, если $\mu = 1$ — то экспоненциальна. Поведение функции (2) при $0 < \mu < 1$ называется *субъэкспоненциальным* с показателем μ. При рассмотрении подобных алгоритмов, указанная функция дает представление о вычислительной сложности алгоритма. Субъэкспоненциальные по сложности алгоритмы занимают промежуточное положение между полиномиальными и экспоненциальными алгоритмами. Рассмотрим конечное поле $F = GF(q), q = p^n$, p—простое.

Определение 4. *Задачей дискретного логарифмирования (DLP) в конечном поле F с основанием $Q \in F^* : \langle Q\rangle = F^*$ называется задача нахождения для заданного числа $P \in F^*$ такого целого числа x, что $Q^x = P$.*

Определение 5. *Задачей дискретного логарифмирования (ECDLP) на эллиптической кривой $E(F)$ над конечным полем F называется задача нахождения для точки $Q \in E(F)$ и точки $P \in E(F)$ такого целого числа x (если оно существует)*[4]*, что имеет место соотношение $xQ = P$.*

Установлено, что в общем случае наилучший оценкой сложности решения задачи в определении 4 в простом поле считается оценка $L_p\left[\frac{1}{3}; c\right]$, где $c = (92 + 26\sqrt{13})^{1/3} \approx 1,902$, полученная применением метода решета числового поля. Задача в определении 5 в общем случае более сложна для решения, чем задача 4.

[4]Такого числа может и не существовать, ведь группа точек эллиптической кривой не является циклической.

Это отчетливо проявляется, если $char(F) = 2$. Заметим, что на настоящее время не существует полиномиальных, детерминированных алгоритмов, эффективно решающих задачу дискретного логарифмирования на эллиптической кривой. Сложность решения этой задачи является в общем случае экспоненциальной, в мультипликативной группе—субъэкспоненциальной. Автором установлено, что наилучший среди известных на настоящий момент алгоритмов по решению ECDLP имеет сложность $O(\sqrt{p})$ операций сложения в группе $\{E(F_p, \oplus)\}$. Для получения этой оценки использовался метод Полларда. С целью проведения расчета, введем в рассмотрение число $n = [\log_2 p]$. Отбросив константы и, введя в рассмотрение функции $C_{ECDLP}(n)$ $(C_{DLP}(l))$—сложности решения ECDLP (DLP) в зависимости от количества бит $n(l)$ на входе, получим формулу $C_{ECDLP}(n) \approx C_{DLP}(l)$, где $n = 2\left(\log_2\left(\exp\left(c_1 l^{1/3}\left(\ln(l\ln 2)\right)^{2/3}\right)\right)\right), c_1 \approx 1,672$. Следовательно, $C_{ECDLP}(n) \approx C_{DLP}(s)$, $s = O\left(n^3\right)$. Здесь ECDLP рассматривается над полем F_p, а DLP над полем F_{p^s}. Только за счет перехода на модель эллиптической кривой произошло увеличение сложности на нелинейный множитель s.

Основываясь на сделанных расчетах, представленных на рисунке 1, отражено соотношение длин ключей в системах над конечными полями (горизонтальная ось) и системами на основе эллиптических кривых (вертикальная ось), имеющих одинаковый уровень информационной безопасности. Изменение параметра s показано на рисунке 2. Доказательно обоснованные расчеты, позволяют разработчику выбирать размер ключей систем на основе эллиптических кривых в рамках целевой системы. Принимая во внимание стандарт на цифровую подпись (имеющиеся таблицы RSA) и используя полученные оценки, приведем соотношение бит систем DSA (DSS),(ECDSA, ГОСТ Р 34.10-01) в виде таблицы 2. Исходя из представленных в ней данных, 1024—битная схема цифровой подписи DSA может быть заменена на 160—битную схему ECDSA электронной цифровой подписи на эллиптических кривых. На основе проведенного анализа обоснованы хорошие перспективы и целесообразность использования модели эллиптический кривой в задаче разработки безопасных, обладающих достаточным быстродействием протоколов цифровой подписи системы АСУП НПС на основе эллиптических кривых. Указанная особенность не только позволяет успешно использовать подобные системы в различных программно—аппаратных решениях, но и существенно ускоряют процесс вычислений, что, в

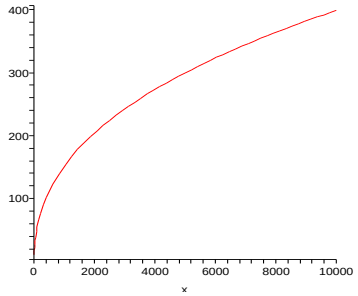

Рис. 1. Соотношение длин ключей.

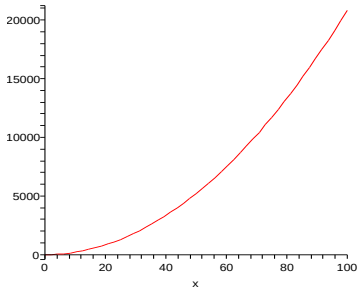

Рис. 2. Коэффициент расширения поля.

свою очередь, приводит к повышению производительности используемых вычислителей системы. Данное свойство является ключевым при разработки современных мобильных цифровых устройств, участвующих а информационном обмене целевой системы. Практическая ценность расчета состоит в том, что, используя полученные результаты, разработчик в состоянии контролировать уровень информационной безопасности систем на основе сложности решения задач, представленных в определениях 4, 5, для долговременного поддержания рекомендованного уровня информационной безопасности подконтрольного объекта.

ECDSA:	DSA:
106	512
132	768
160	1024
224	2048

Таблица 2. Размеры ключей.

Четвертая глава посвящена исследованию и совершенствованию применяющихся на практике однонаправленных хеш—функций с целью повышения эффективности их программно—аппаратных реализаций в целевой системе. В первом разделе главы проведен анализ основных атак на однонаправленные хеш—функции. Обозначим, через $P_1(k,n)$ вероятность того, что для фиксированных $\mathfrak{M} \in 0,1^*$ и $\mathfrak{N}_1,\ldots,\mathfrak{N}_k \in \{0,1\}^*$ существует номер $i=1,..,k$ такой, что $h(\mathfrak{M}) = h(\mathfrak{N}_i)$, где n—порядок хеш–функции $h()$. Через $P_2(n,k)$ обозначим вероятность того, что на множестве из k элементов, каждый из которых может принимать 2^n значений, существуют хотя бы два с одинаковыми значениями. На основе математических расчетов получено, $P_1(k,n) = 1-(1-2^{-n})^k$, $P_2(n,k) > 1-e^{\frac{-(k(k-1))}{2^n}}$. Используя полученные оценки для атак методом "грубой"силы и атак, основанных на парадоксе дней рождений, рассчитаны таблицы практически важных значений указанных вероятностей. Основываясь на значениях вероятности $P_2(k,n)$, сделан вывод о том, что задача предварительной заготовки коллизии (например, методом дней рождений), приводит к успеху при переборе уже $k = 2^{n/2}$ текстов, и является более легкой вычислительной задачей. Проведено исследование атак, основанных на специфике построения хеш—функций. Анализируя унифицированный алгоритм подобного построения 1, замечено, что текст $\mathfrak{M}$ разбивается на блоки $\mathfrak{M}_i$ (в большинстве случаев размером в 512 бит) и включается итерационный процесс подсчета хеш—значения $h_i = f(h_{i-1}, \mathfrak{M}_i)$. Длина раунда небольшая, поэтому при определенных условиях, применяя дифференциальный анализ, можно найти текст $\triangle C$ такой, что $h(\mathfrak{M}_i + \triangle C) = h(\mathfrak{M}_i)$. Подобные атаки, названные автором атаками на основе туннельного эффекта $\triangle C$, позволяют вскрывать некоторые распространенные хеш—функции с линейной трудоемкостью. Установлено, что используя туннели вида: $C = \left(0, 2^{31}, 2^{31}-2^{28}, 0,0,0,0,0,0,0,0,0,-2^{16},0,0,0\right)$, $C = \left(0,0,0,2^{20},0,0,0,0,0,0,0,2^{18}+2^{31},0,0,0,0,2^{31}\right)$ успешно компрометируются хеш—функции MD4, RIPEMD128. Атака на основе туннельного эффекта при определенных условиях, является самой быстрой, ее трудоемкость минимальна и сводится к простым вычислениям. Данные обстоятельства позволяют сделать

вывод о том, что использования в рамках целевой системы хеш—функций небезопасно и требует разработки методов устойчивости к коллизии и нахождению второго прообраза. Установлено, что рекомендованный для предотвращения указанных недостатков метод Шнайера не способен устранить туннельный эффект. Для решения задач в такой постановке однонаправленные хеш—функции рассматривались как черные ящики, уровень доверия к которым необходимо повысить, применяя математические методы. В результате, в работе построены методы, позволяющие не только вновь использовать на практике некоторые хеш—функции, но и конструировать надежные хеш—функции для применения в АСУП НПС. Практическая ценность представленного решения обусловлена тем обстоятельством, что большинство хеш—функций, обладают уникальной архитектурой, стандартизованы и организованы в служебные библиотеки (например, PGP), работающие под ОС MS Windows, Linux. Пусть $\mathfrak{M} \in \{0,1\}^*$ произвольный текст. Разработаны и протестированы следующие методы:

SS—суффиксной суперпозиции	$\hat{h}(\mathfrak{M}) = \ldots \parallel h(\mathfrak{M} \parallel h(\mathfrak{M} \parallel h(\mathfrak{M})))\ldots;$
PC—префиксной конкантенации	$\hat{h}(\mathfrak{M}) = \ldots \parallel h(h(h(\mathfrak{M}) \parallel \mathfrak{M}) \parallel \mathfrak{M}) \parallel \mathfrak{M}\ldots;$
C—конкантенации	$\hat{h}(\mathfrak{M}) = h_1(\mathfrak{M}) \parallel h_2(\mathfrak{M}) \parallel \ldots \parallel h_k(\mathfrak{M});$
S—суперпозиции	$\hat{h}(\mathfrak{M}) = h_1(h_2(\ldots h_k(\mathfrak{M})));$
SUB—перестановок	$\hat{h}(\mathfrak{M}) = h(\mathfrak{M}) \parallel h(\pi_1(\mathfrak{M})) \parallel \ldots \parallel h(\pi_k(\mathfrak{M}));$
SSUB—усиленных перестановок	$\hat{h}(\mathfrak{M}) = \ldots h(\pi_2(h(\pi_1(h(\mathfrak{M}) \parallel \mathfrak{M})) \parallel \mathfrak{M}))\ldots.$

Здесь π_i, $i = 1, \ldots, k$— произвольные перестановки исходного текста $\mathfrak{M}$, h_i однонаправленные хеш—функции, $\parallel$—конкантенация. Исследована на примерах устойчивость к коллизиям полученных хеш—функций и приведены способы их избежания. Используя понятие ключевых однонаправленных хеш—функций (MAC), ключи могут быть внедрены как в перестановку, так и непосредственно в саму однонаправленную хеш—функцию, что решает вопросы нехватки ключей и отсечения "недовереной"стороны. Среди полученных методик выбраны оптимальные с позиции безопасности и скорости работы реализующих их программных механизмов. Предложены эффективные схемы $E_{k_1}(\mathfrak{M}, h_{k_2}(\mathfrak{M}))$, $(E_{k_1}(\mathfrak{M}), h_{k_2}(\mathfrak{M}))$, $(E_{k_1}(\mathfrak{M}), h_{k_2}(E_{k_1}(\mathfrak{M})))$ совместного использования ключевой хеш—функции и симметричного шифрования для решения задач аутентификации источника данных и распознавания информационных потоков различных типов данных АСУП НПС, соответствующих требованиям технического задания на эту работу. Даны рекомендации по оптимальному использованию схем и способов организации ключей. Получена схема (3) алгоритмизации итерационного процесса (1).

$$\begin{array}{l} H_i = E_{A,B}(C) \oplus D; \\ A, C, D \in \{\mathfrak{M}_i, H_{i-1}, \mathfrak{M}_i \oplus H_{i-1}, X, const\}; \\ X = g(\mathfrak{M}_i, H_{i-1}, const), B = f(\mathfrak{M}_i, H_{i-1}, const). \end{array} \qquad (3)$$

В схеме (3) функции $g(\cdot), f(\cdot)$ являются функциями сжатия блока до определенной фиксированной длины, равной длине ключа К шифрования в алгорит-

ме блочного шифрования E. В результате проведенных исследований полученной схемы, удалось выделить надежные схемы хеширования на основе блочных шифров и структурировать имеющиеся на практике схемы построения однонаправленных хеш—функций из алгоритмов блочного шифрования. Схема (3) усилена за счет разработанного *мультиключевого алгоритма расчета хеш—значения*, основанного на модифицированных стандартах блочного шифрования (ГОСТ 28147-89, DES), являющихся сетями Фейстеля. Введение параметрического семейства латинских квадратов, позволило ввести в S—блоки зависимость от дополнительного ключа. В результате, без потери быстродействия, число ключей соответствующей MAC—функции, основанной на сети Фейстеля, увеличено в несколько раз. Отмеченное обстоятельство позволило разработать мультиключевой алгоритм построения однонаправленных хеш—функций, в котором ключ может обновляться на каждом раунде, что позволило существенно увеличить порядок ключевого множества. Формально, вместо статической системы $h = E_k(\mathrm{C})$, k—первоначальный ключ, рассматривалась динамическая система (конечный автомат) вида: $h_t = E_{k,k_t}(\mathrm{C}), k_t = f(k, k_{t-1}), t = 1, 2, \ldots$. При таком подходе на каждом этапе итерационного процесса 3 происходит смена блоков перестановок (S—блоков), зависящих от ключа k_t. Используя в мультиключевом алгоритме переменные S—блоки, удалось многократно снизить эффективность использования линейного и дифференциального анализа для компрометации системы. Действительно, основываясь на исследовании трудов Шамира и Мацуми, установлено, что если S—блоки не являются фиксированными, то соответствующие виды анализов малоэффективны. Разработанные схемы применены для введения дополнительных ключей в предложенные алгоритмы подсчета хеш—значения, которые позволяют разработчику создать их иерархию при использовании в различных аппаратных решениях. Отмечается то обстоятельство, что применение переменных блоков (мультиключевого подхода) с целью шифрования требует детального изучения вопросов, связанных с наличием слабых ключей и оптимальностью выбора блоков замены. В противном случае схема будет иметь существенные недостатки. Мультиключевой способ построения хеш—функций используется в высокоскоростных аппаратных реализациях целевой системы. Представленные результаты позволяют успешно решать поставленные выше задачи в рамках единого метода цифровой подписи на эллиптических кривых, существенно повышая защиту от заранее выработанных коллизий и позволяя создать иерархию и резерв ключей.

Пятая глава посвящена совершенствованию и созданию программных реализаций схем цифровой подписи на основе эллиптических кривых, решающих задачу обеспечения целостности и конфиденциальности цифровой информации в процессе ее сбора, хранения и передачи в рамках целевой системы, а также описанию реализованного программно—аппаратного комплекса. Показано, что протоколы цифровой подписи DSA, ECDSA, ГОСТ Р 34.10—94, ГОСТ Р 34.10—01 неустойчивы к изначальной фальсификации информации. В работе рассмотрен наиболее перспективный алгоритм цифровой подписи на эллипти-

ческих кривых ECDSA, принятый стандартами: ISO(1998); ANSI X9.62(1999); IEEE(2000); NIST(2000). Алгоритмы генерации и верификации цифровой подписи данного стандарта связаны с сообщением $\mathfrak{M}$ только через хеш—функцию $h(\cdot)$. В FIPS рекомендуется использовать ECDSA с хеш—функцией SHA-1 порядка 160 бит, однако в ECELGSA, ГОСТ Р 34.10—01 применяют другие хеш—функции. Учитывая счетность множества всех текстов над алфавитом $0, 1$, для любой хеш—функции существуют два различных сообщения $\mathfrak{M}_1, \mathfrak{M}_2 \in \{0,1\}^*$ таких, что $h(\mathfrak{M}_1) = h(\mathfrak{M}_2)$. Вопрос нахождения коллизий в хеш—функциях является открытым и, по сути, ответ на него — дело времени. В работе приводились методы оперативного вычисления коллизий, например, основываясь на туннельном эффекте. Следовательно, злоумышленник в состоянии заранее заготовить сообщения $\mathfrak{M}_1, \mathfrak{M}_2$. При этом, отдав на подпись сообщение $\mathfrak{M}_1$ и заменив его после процедуры подписывания, своим сообщением $\mathfrak{M}_2$, злоумышленник, успешно проходит процедуру верификации ложного сообщения. Автором установлено, что ECDSA, ГОСТ Р 34.10—94, ГОСТ Р 34.10—01 являются частными случаями схемы цифровой подписи ECELGSA. Действительно, после несложных преобразований, уравнение генерации цифровой подписи ECDSA представляется в виде $u \equiv k_1 v + k_2 w \mod (p-1)$, где k_1, k_2—долгосрочный и сеансовый ключи. Рассмотрев в качестве троек (u, v, w) всевозможные перестановки чисел $h(\mathfrak{M}), \pm r, \pm s$ при некотором выборе знаков, получим новые схемы цифровой подписи, приведенные в таблице 3. Заметим, что схемы 1,2,3,4

Номер	u	v	ω	Уравнение генерации	Уравнение проверки
1	$h(\mathfrak{M})$	r	s	$h(\mathfrak{M}) = k_1 r + k_2 s$	$h(\mathfrak{M})P = rQ_1 \oplus sQ_2$
2	$h(\mathfrak{M})$	$-r$	s	$h(\mathfrak{M}) = -rk_1 + k_2 s$	$h(\mathfrak{M})P = -rQ_1 \oplus sQ_2$
3	$-h(\mathfrak{M})$	s	r	$-h(\mathfrak{M}) = k_1 s + k_2 r$	$-h(\mathfrak{M})P = sQ_1 \oplus rQ_2$
4	s	r	$h(\mathfrak{M})$	$s = k_1 r + k_2 h(\mathfrak{M})$	$sP = rQ_1 \oplus h(\mathfrak{M})Q_2$

Таблица 3. Простейшие полученные модификации схемы ECELDSA.

являются соответствуют схемам цифровой ECELGSA, ECDSA, ГОСТ Р 34.10-94, ГОСТ Р 34.10-01. Как уже отмечалось в первой главе, указанные схемы являются частными случаями схемы Эль—Гамаля, и, как следствие, обладают отмеченными выше недостатками. Для устранения недостатков перечисленных схем и других частных случаев схемы Эль—Гамаля, вводится зависимость между текстом $h(\mathfrak{M})$ и сеансовым ключом k_2. В качестве слабой зависимости рассматривается замена в алгоритме генерации цифровой подписи $h(\mathfrak{M})$ на $h(\mathfrak{M} \parallel r)$. С целью усложнения зависимости применяются способы модификации хеш—функций (описанные в главе 4) и введение уникальных идентификационных меток (время, размер, число 0, и другие). Внедрение нетривиальной зависимости хеш—значения от случайного сеансового ключа и терминальных параметров усиливает схему цифровой подписи. Однако, для проверки подписи необходимо знать алгоритм выработки хеш—значения, что в некоторых случаях существенно снижает безопасность подобных схем.

Для решения задачи минимизации разглашения служебных параметров системы управления разработаны схемы с восстановлением на основе эллиптических кривых, где совместно с подписью передается хеш—значение $h(\mathfrak{M})$. Сторона—верификатор в состоянии извлечь из подписи (r, s) сообщения $\mathfrak{M}$ восстановленное хеш—значение $h(\mathfrak{M})'$ без знания алгоритма вычисления хеш—значения $h(\cdot)$. Для проверки правильности подписи остается проверить справедливость соотношения $h(\mathfrak{M})' = h(\mathfrak{M}')$, где $\mathfrak{M}'$—сообщение, подпись под которым проверяется, а $h(\mathfrak{M})'$—хеш—значение приписываемого сообщения $\mathfrak{M}$, извлеченное из цифровой подписи (r, s). Данная схема реализована в виде модуля ECNRDSA, который решает поставленную задачу.

С целью предотвращения изначальной фальсификации в подобных схемах, получена схема ECSDSA, не являющаяся схемой с восстановлением. При построении единого контура информационно—аналитической системы АСУП НПС, кроме задач, связанных с аутентификацией информации, рассмотрены не менее важные *задачи обеспечения анонимности*. Более формально, злоумышленник имеет возможность, осуществляя мониторинг пакетов данных, устанавливать их тип или идентифицировать посылающую сторону (так как долгосрочные ключи изменяются не так оперативно как сеансовые и являются жестко привязанными к стороне инициирующей протокол "слепой"подписи). Применение схем слепой подписи в сетях АСУП НПС, позволяет избежать воздействия вредоносного мониторинга за типами информационных потоков. При этом предоставляется возможность повысить время жизни ключей данной системы. Автору удалось разработать схемы ECBDSA слепой подписи на основе эллиптических кривых. В их основе лежит модификация схемы ECSDSA за счет введения сглаживающих слагаемых. При равновероятностном выборе указанных слагаемых по соответствующей подписи корректно идентифицировать пользователя не представляется возможным, поэтому, все требования протокола "слепой"подписи удовлетворены.

Представленные выше схемы цифровой подписи могут быть использованы для организации скрытых каналов передачи данных со сравнительно большой пропускной способностью. Действительно, случайный характер выбора сеансового ключа k_2, по которому в стандартах формируется элемент подписи r, позволяет передавать в подписи необходимую информацию (результаты мониторинга системы, команды, сигналы и другие). Указанный недостаток в классических схемах цифровой подписи не удовлетворяет требованиям нормативной документации. При длине модуля $N = 1024$ бит в одной подписи можно передать около 1000 бит информации. Изложенные соображения свидетельствуют о том, что построенный таким образом канал передачи данных является обладает высокой пропускной способностью. Для предотвращения внедрения подобных каналов представим оба элемента подписи (r, s) в одинаковом виде: $k_1 P = (x_1, y_1), r = x_1 \mod N; k_2 P = (x_2, y_2), s = x_2 \mod N$. Числа k_1, k_2 вычисляются одновременно путем анализа двух сравнений, которые записываются

в зависимости от вида проверочного соотношения. Ключевая идея указанного механизма состоит в том, чтобы сделать вычислительно невозможным расчет одного из параметров r, s при наперед заданном значении другого. Параметры r, s используются как аргументы двух различных функций $f_1(r, s)$, $f_2(r, s)$. При определенных ограничениях на значения аргументов их можно изменять таким образом, что значения одной функции, например $f_2(r, s)$, будет оставаться неизменным. Значение оставшейся функции $f_1(r, s)$ при этом будет изменяться таким образом, что можно подобрать пару значений r и s, при которых будет выполняться некоторое проверочное соотношение. Следовательно, в определенной области пар значений (r, s) $f_2(r, s) = const = \omega$, поэтому проверочное соотношение удалось упростить, что при определенном его виде позволит вычислить подпись $(r(\omega), s(\omega))$, зависящую от параметра ω. В работе приведены виды проверочных уравнений, условия постоянства, непосредственные схемы подобных подписей.

Приводится описание разработанного автором модуля **ECDSM (Elliptic Curve Digital Signature Module)** и его роль в аппаратных комплексах системы АСУП НПС, обеспечивающих целостность и конфиденциальность цифровой информации в процессе сбора, хранения и передачи между ключевыми объектами целевой системы. С целью структуризации процесса обработки большого количества информационных потоков рассматривался единый протокол взаимодействия систем АСУП НПС. Согласно единому протоколу, данные, подлежащие объективному контролю, организованы в виде цифровых пакетов разных типов и размеров. Каждый цифровой пакет данных содержит рассчитанную с использованием разработанных методов уникальную цифровую подпись. Представим содержимое пакета в виде таблицы 4.

Код информационного источника	Размер данных	Данные	Цифровая подпись 1	...	Цифровая подпись n

Таблица 4. Схема цифрового пакета.

Количество цифровых подписей выбирается, исходя из числа информационных типов потоков и числа упомянутых выше ключевых объектов (источников). По этой причине каждый подконтрольный источник данных обладает уникальными ключами, необходимыми для выработки и проверки подписи. Модуль **ECDSM** реализован автором, как виртуальный C++ класс, основные функции которого приведены на нижеследующей схеме.

```
public class ECDSM   {   public: ECDSM(void);
                         virtual bool SetDigitalSignature(Adata *data, BYTE *buf);
                         virtual bool VerDigitalSignature(Adata *data, BYTE *buf);
                         virtual bool InitAdata(Adata *data);
                         ~ECDSM(void);
                     };
```

Структура Adata представляет собой некоторое количество терминальных

параметров, таких как долгосрочные(сеансовые) ключи, код источника, тип и размер данных, необходимых для выработки (проверки) цифровой подписи на эллиптической кривой.

Функция virtual bool InitAdata(Adata *data) производит начальную инициализацию структуры Adata. На этапе инициализации происходит заполнение всех необходимых полей Adata, включая эллиптическую кривую, точку основания, ключи, параметры MAC(MDC)—хеш—функций.

Функция virtual bool SetDigitalSignature(Adata *data, BYTE *buf) вычисляет цифровую подпись для параметров data и пакета данных buf. При этом вычисленная подпись встраивается в пакет данных buf. В случае успеха функция возвращает значение true, иначе—значение false.

Функция virtual bool VerDigitalSignature(Adata *data, BYTE *buf) проверяет цифровую подпись для параметров data и пакета данных buf. В случае успеха функция возвращает значение true, иначе—значение false.

Представлены описания технологических особенностей, разработанных автором программ. Модуль цифровой подписи на основе эллиптических кривых ECDSM реализован, как отмечалось выше, как виртуальный C++ класс. Целесообразность подобного технологического решения обусловлена гибкостью и простотой поддержания большого числа описанных подклассов, так как набор необходимых функций подобных классов единообразен. Модуль ECDSM интегрирован в МЦМ (многоканальный цифровой магнитофон) и в соответствующие системные библиотеки (ecdsm.dll). Тестовая реализация программы, написана с использованием графической библиотеки framework 2.5 на платформе ОС Windows Professional.

Далее перечислены поддерживаемые модулем **ECDSM** виды схем цифровой подписи. Виртуальный класс ECDSM приводится к одному из перечисленных ниже классов.

- **ECDSA** (Elliptic Curve Digital Signature Algorithm) является реализацией стандарта ECDSA, описанного в главе 1.
- **ECGOST** (Elliptic Curve GOST) является реализацией действующего ГОСТ РФ 34.10-01.
- **SECDSA** (Strong Elliptic Curve Digital Signature Algorithm) соответствует реализации усиленной схемы ECDSA, описание которой приведено в главе 5. Данная схема является устойчивой к изначальной фальсификации сообщений.
- **SECGOST** (Strong Elliptic Curve GOST)—реализация ГОСТ РФ 34.10-01, устойчивого к изначальной фальсификации сообщений (см. главу 5).

- **ECELDSA** (Elliptic Curve El—Gamal Digital Signature Algorithm) представляет собой реализацию алгоритма цифровой подписи Эль—Гамаля.
- **SECELDSA** (Strong Elliptic Curve El—Gamal Digital Signature Algorithm) представляет собой реализацию усовершенствованной автором схемы цифровой подписи Эль—Гамаля.
- **ECNRDSA** (Elliptic Curve Nyberg—Rueppel Digital Signature Algorithm) является реализацией алгоритма цифровой подписи с восстановлением.
- **ECSDSA** (Elliptic Curve Schorr Digital Signature Algorithm)—реализация аналога схемы Шнорра на основе эллиптической кривой.
- **ECBDSA** (Elliptic Curve Blind Digital Signature Algorithm)—соответствует алгоритму "слепой"подписи на основе эллиптических кривых.
- **ECWHCDSA** (Elliptic Curve Without Hidden Channels Digital Signature Algorithm) представляет собой схему цифровой подписи, устойчивую к внедрению скрытых каналов передачи данных, обладающих высокой пропускной способностью.
- **WDSA** (Weak Digital Signature Algorithm)—является "слабой"симметричной цифровой подписью (см. главу 4 диссертационной работы).

Каждый из перечисленных классов наследует ряд классов полученных применением разработанных автором методов повышения эффективности программно—аппаратных реализаций однонаправленных хеш—функций, представленных в главе 4. Для каждого из введенных классов **SS, PC, C, S, SUB, SSUB**, реализована зависимость от следующих подклассов, представленных на рисунке 3.

Отмечено, что в качестве хеш—функций возможно применять, не только представленные на рисунке 3 функции, но и произвольную однонаправленную хеш—функцию. Данное обстоятельство расширяет список возможных классов, увеличивая время жизни системы информационной безопасности подконтрольного объекта. Список классов расширяется также путем применения различных блочных шифров (класс **MACBC**) и их SB—модификаций (подкласс **UECB**—Universal Electronic Code Book соответствующий разработанной автором в главе 4 универсальной схеме построения однонаправленных хеш—функций на основе блочных шифров). Приведенное обстоятельство свидетельствует о возможности оперативной модификации реализованного модуля **ECDSM**.

Полученные автором в диссертационной работе результаты применяются в информационных системах объективного контроля оперативных и диспетчерских служб в рамках Концепции информационной безопасности организации

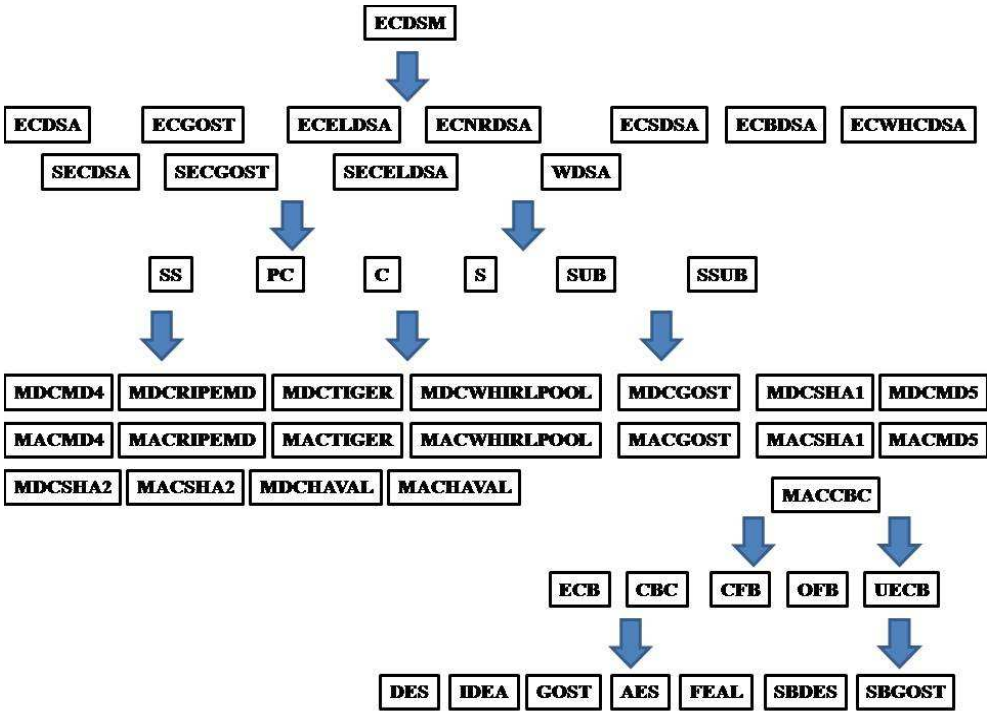

Рис. 3. Схема сопряжения подклассов ECDSM.

воздушного движения РФ. Данные системы разрабатываются ФГУП Научно—технологический центр "Электронтех"РАН с целью реализации автоматической записи, обработки, архивирования и воспроизведения речевой, телеметрической и видеоинформации в реальном масштабе времени, а также для обеспечения многоуровневой защиты информации от несанкционированного доступа. Использование данной аппаратуры позволяет на высоком уровне обеспечивать объективность контролируемой информации автоматизированной системы управления полетами, навигации, посадки и связи аэродромов государственной авиации"(ОКР шифр—"Рейс—2000"). Модуль ECDSM и соответствующие программные комплексы применяются НТЦ "Электронтех"РАН в современных многоканальных цифровых магнитофонах (МЦМ) и станциях воспроизведения регистрируемой информации.

В заключении диссертационной работы перечисляются ее основные результаты.

- Усовершенствованы методы использования модели эллиптической кривой с целью построения схем цифровой подписи, устойчивых к изначальной фальсификации, внедрению скрытых каналов передачи данных и других методов компрометации. Создана схема "слепой"цифровой подписи на основе эллиптических кривых. На основе метода Полларда получена формула расчета длин ключей, позволяющая определять уровень безопасности систем на основе эллиптических кривых.

- Разработаны алгоритмы кодирования данных точками эллиптических

кривых, используемые для создания на их основе программных средств, позволяющих в реальном времени использовать в целевой системе протоколы выработки общих ключей и передачи информации на основе эллиптических кривых.

- Созданы методы построения эффективных программно—аппаратных реализаций однонаправленных хеш—функций, решающие задачи отсечения "недоверенной"стороны, "нехватки"и создании резерва ключей, а также задачи защиты от коллизий и долговременного поддержания высокого уровня безопасности информационной системы. Предложен мультиключевой алгоритм реализации хеш—функций, при котором ключ может обновляться на каждом раунде, что позволило существенно увеличить порядок ключевого множества.

- Реализован и прошел тестовые испытания комплекс программно—аппаратных средств, обеспечивающих целостность и конфиденциальность информации в процессе ее сбора, хранения и передачи в рамках системы информационной безопасности организации воздушного движения.

Благодарности. Автор выражает глубокую признательность своему научному руководителю кандидату физико—математических наук, в.н.с. Носову Валентину Александровичу за постановку задач и осуществление научного руководства, доктору физико—математических наук, профессору Васенину Валерию Александровичу за ценные замечания по тексту диссертации, способствующие ее улучшению.

Публикации по теме диссертации

[1]. Лёвин В.Ю. Кодирование алфавитов точками эллиптических кривых.// Интеллектуальные системы, 2007, т.11, вып. 1—4, стр. 171—183.

[2]. Лёвин В.Ю., Носов В.А. Анализ повышения криптографической сложности систем при переходе на эллиптические кривые.// Интеллектуальные системы, 2008, т.12, вып. 1—4, стр. 253—269. (В.Ю. Лёвину принадлежат результаты по обоснованию целесообразности использования эллиптической кривой в построении стойких протоколов цифровой подписи и проведение соответствующего математического расчета изменения криптостойкости подобных систем).

[3]. Лёвин В.Ю., Носов В.А. Повышение криптостойкости криптосистем при переходе на эллиптические кривые.// Материалы международной конференции "Современные проблемы математики, механики и их приложений"посвященной 70-летию ректора МГУ академика В.А.Садовничего,

2009, стр. 364—365. (В.Ю. Лёвину принадлежат результаты проведенного расчета изменения стойкости систем при переходе на модель эллиптической кривой).

[4]. Лёвин В.Ю. Повышение криптографической стойкости протокола цифровой подписи на эллиптических кривых.// Информационные технологии, 2010, №5, стр. 33—37.