На правах рукописи 

Березин Андрей Николаевич

МЕТОДЫ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ ЗАЩИТНЫХ ПРЕОБРАЗОВАНИЙ ИНФОРМАЦИИ

Специальность 05.13.19 –
«Методы и системы защиты информации, информационная безопасность»

Автореферат
диссертации на соискание учёной степени
кандидата технических наук

Санкт-Петербург – 2016

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)» (СПбГЭТУ «ЛЭТИ»).

Научный руководитель: доктор технических наук, профессор
Молдовян Николай Андреевич

Официальные оппоненты: **Коржик Валерий Иванович,**
доктор технических наук, профессор, ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича», почётный профессор СПбГУТ

Левина Алла Борисовна,
кандидат физико-математических наук, доцент, ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», доцент кафедры «Безопасные информационные технологи»

Ведущая организация: Открытое акционерное общество «Научно-исследовательский институт «ВЕКТОР» (ОАО «НИИ «Вектор»), г. Санкт-Петербург

Защита состоится 9 февраля 2017 г. в 15-30 на заседании диссертационного совета Д 002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук (СПИИРАН) по адресу: 199178, Санкт-Петербург, В. О., 14 линия, 39.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) по адресу: 199178, Санкт-Петербург, В. О., 14 линия, 39 и на сайте www.spiiras.nw.ru.

Автореферат разослан «___» _____ 2016 года.

Ученый секретарь
диссертационного совета Д 002.199.01
кандидат технических наук Фаткиева Роза Равильевна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Для защиты информации в информационно-телекоммуникационных технологиях широко используются алгоритмические средства, стойкость которых базируется на вычислительной сложности некоторых задач, в частности задач факторизации и дискретного логарифмирования по простому модулю. Безопасность таких алгоритмов определяется с точки зрения теории сложности и оценивается количеством операций (стойкостью), необходимых для решения вычислительно трудной задачи. При определении требуемого уровня стойкости дополнительно учитывают стоимость оборудования, которое может быть использовано на текущий момент времени, и научные достижения в области новой вычислительной техники. Однако при таком подходе к оцениванию безопасности алгоритмов остаётся неучтённой вероятность появления прорывных методов решения используемой вычислительно трудной задачи.

В последнее время предлагается понятие интегрального показателя безопасности. Данный показатель учитывает стойкость используемых вычислительно трудных задач и вероятность того, что будут найдены прорывные алгоритмы решения в области вычислительно сложных задач, используемых в алгоритмических средствах защиты информации. Существенное повышение указанного показателя может быть достигнуто путём разработки алгоритмов защиты информации, для взлома которых потребуется решать две независимые вычислительно сложные задачи.

Вопросы безопасности информации, обрабатываемой в электронной форме, приобретают ключевое значение в современных информационно-телекоммуникационных технологиях, в связи с этим тема диссертационной работы представляется своевременной и актуальной.

Степень разработанности темы. Исследования посвящённые вопросам разработки алгоритмов защиты информации, основанных на двух трудных задачах приведены в работах следующих авторов: Brickell E.F., Girault M., Harn L., He J., Ismail E.S., Kiesler T., Kuo W.C., Laih C.S., McCurley K.S., Pointcheval D., Shao Z., Shmuely Z., Васильев И.Н., Головачёв Д.А., Гортинская Л.В., Дернова Е.С., Костина А.А., Латышев Д.М., Молдовян А.А., Молдовян Д.Н., Молдовян Н.А., Нгуен Л.М., Рыжков А.В., Сухов Д.К., Щербаков В.А. и др. В подавляющем большинстве работ указанных авторов для повышения уровня безопасности, оцениваемому по интегральному критерию, предложены только единичные алгоритмы аутентификации, электронной цифровой подписи, обмена секретом, в основном использующие модуль $p = 2n + 1$, где n - трудно факторизуемое число, для взлома которых требуется решить две вычислительно сложные задачи, однако известные методы их построения не позволяют реализовать алгоритмы защиты информации других типов, что сдерживает их применение на практике.

Решаемая научно-техническая задача. Решается задача разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения.

Цель и задачи исследования. Целью диссертационного исследования является повышение уровня информационной безопасности информационно-телекоммуникационных технологий. Решение сформулированной научно-технической задачи предусматривало:

1. Разработку метода построения алгоритмов и протоколов для применения в средствах защиты информации, обладающих повышенным уровнем безопасности, который позволит расширить виды алгоритмов и протоколов указанного типа.
2. Разработку протоколов локальной и удалённой аутентификации пользователей, субъектов и объектов информационных процессов, обладающих повышенным уровнем безопасности.
3. Разработку протоколов обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающих повышенным уровнем безопасности.
4. Разработку протоколов обеспечения анонимности в открытых компьютерных сетях, обладающих повышенным уровнем безопасности.

Научная новизна

1. Впервые предложен метод построения алгоритмов и протоколов, нарушение безопасности которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что, по крайней мере, решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.
2. На основе предложенного метода разработаны новые протоколы аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности: протокол электронной цифровой подписи (ЭЦП), отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол утверждаемой групповой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма маскирования ключей, благодаря чему руководитель и только он может доказывать стороннему проверяющему список лиц, которые подписывали документ, без разглашения секретных ключей подчинённых и своего собственного; протокол интерактивной аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю n специальной структуры; протокол двухшаговой аутентификации субъекта, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и элемента выделенной подгруппы мультипликативной группы кольца вычетов по модулю n в ка-

честве запроса, благодаря чему достигнута возможность безопасной аутентификации субъекта за два шага.

3. На основе предложенного метода разработаны новые протоколы защиты информации, обладающие повышенным уровнем безопасности: протоколы обмена ключами, отличающиеся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и рандомизирующего параметра, благодаря чему обеспечивается случайность значения ключа, формируемого в ходе протокола; протокол защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры; протокол коммутативного защитного преобразования информации, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и механизма расщепления сообщений, благодаря чему обеспечивается возможность выполнения защитных преобразований для произвольных сообщений; протокол стойкого защитного преобразования информации с использованием ключа малого размера, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры и процедуры бесключевого защитного преобразования совместно с аутентификацией по коротким ключам, благодаря чему возможно задать стойкость протокола, для малых длин ключа.
4. На основе предложенного метода разработаны новые протоколы обеспечения анонимности, обладающие повышенным уровнем безопасности: протокол слепой ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП; протокол слепой коллективной ЭЦП, отличающийся использованием ЗДЛ по трудно факторизуемому модулю специальной структуры, благодаря чему достигнуто снижение размера, вычислительной сложности процедур генерации и проверки ЭЦП.

Теоретическая и практическая значимость работы определяется тем, что предложен метод построения алгоритмов и протоколов, имеющих повышенный уровень безопасности, свободный от недостатков существующих аналогов, а разработанные протоколы аутентификации, обеспечения конфиденциальности и анонимности, имеют широкое применение в информационно-телекоммуникационных технологиях.

Методология и методы исследования. При выполнении диссертационного исследования были использованы аппарат и методы алгебры, теории вероятности, дискретной математики, теории чисел, теории сложности и информационной безопасности.

Положения, выносимые на защиту:

1. Метод построения алгоритмов и протоколов, повышенный уровень безопасности которых обеспечивается тем, что для их взлома требуется одновременно решить задачи дискретного логарифмирования и факторизации.

2. Протоколы локальной и удалённой аутентификации пользователей, объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности.
3. Протоколы обеспечения конфиденциальности информации, передаваемой по открытым каналам связи, обладающие повышенным уровнем безопасности.
4. Протоколы обеспечения анонимности в открытых компьютерных сетях, обладающие повышенным уровнем безопасности.

Достоверность и апробация результатов. Достоверность подтверждается строгими математическими доказательствами, обеспечивается анализом состояния исследований в этой области на сегодняшний день и апробацией основных результатов на 14 конференциях различного уровня, в том числе на 4 международных и 4 всероссийских.

Полученные результаты диссертационного исследования были использованы при выполнении научно-исследовательских работ по грантам Правительства Санкт-Петербурга, дипломы № ПСП 15 331, № ПСП 14 044, № ПСП 13038. Результаты диссертационного исследования внедрены при выполнении работ по гранту РФФИ (№14-07-00061 А) на базе СПИИРАН, в учебный процесс Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) и государственного университета морского и речного флота имени адмирала С.О. Макарова.

Личный вклад. Все научные положения, выносимые на защиту, были получены и сформулированы лично автором.

Публикации. Основные результаты по теме диссертации изложены в 25 печатных изданиях, 6 из которых изданы в журналах, 5 из которых опубликованы в ведущих рецензируемых журналах, входящих в перечень ВАК.

Структура и объем работы. Диссертационная работа изложена на 134 машинописных страницах, включает введение, 5 глав, заключение, список литературы (143 наименования), 35 рисунков и 13 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается важность и актуальность исследований, проводимых в рамках данной диссертационной работы, сформулированы цели исследования и решаемые задачи, определена научная новизна и практическая значимость представляемой работы.

В первой главе приведён обзор алгоритмов и протоколов используемых в современных средствах защиты информации в информационно-телекоммуникационных системах. Особое внимание уделено тому, что для решения практических задач по аутентификации, обеспечению конфиденциальности и анонимности используются алгоритмические средства защиты информации, которые основаны на вычислительной стойкости некоторой вычислительно сложной задачи. Отмечается, что на сегодняшний день хорошо изученными и универсальными задачами являются задача дискретного логарифмирования (ЗДЛ) и задача факторизации (ЗФ). Рассматривается применение указанных задач в средствах алгоритмической защиты информации и

оптимальные способы их решения. Отмечается, что все существующие методы оценки безопасности использования алгоритмических средств защиты информации опираются на следующие два факта: 1) решение используемой вычислительно сложной задачи является вычислительно нереализуемым за приемлемое время при использовании наилучшего известного алгоритма её решения, т.е. её вычислительная сложность W достаточна высока; 2) вероятность появления P в ближайшем будущем вычислительно эффективного алгоритма решения указанной задачи пренебрежимо мала. Но безопасность использования алгоритмических средств защиты информации, в основе которых лежат вычислительно сложные задачи, так же должна учитывать и вероятность появления новых прорывных методов их решения. Для учёта обоих параметров Молдовян Н.А. ввёл интегральный показатель безопасности $l = W/P$. Следовательно, увеличение вычислительной сложности W или уменьшение вероятности P ведёт к увеличению данного показателя l.

Поиски вычислительно сложных задач с более высокими оценками вычислительной сложности их решений продолжаются, но на текущий момент, лучшими кандидатами для использования в алгоритмических средствах защиты информации являются ЗФ и ЗДЛ. Существенного увеличения интегрального показателя безопасности l можно достичь путём разработки алгоритмов и протоколов, взлом которых требует решения двух независимых вычислительно сложных задач (таблица 1).

Таблица 1 — Сравнительная характеристика повышения интегрального показателя безопасности при построении алгоритмов и протоколов, взлом которых потребует одновременного решения двух независимых вычислительно сложных задач

Задача	Вероятность P	Стойкость W (операций)	l при $P_{\text{ЗФ}} = P_{\text{ЗДЛ}} = 10^{-3}$	l при $P_{\text{ЗФ}} = P_{\text{ЗДЛ}} = 10^{-6}$	l при $P_{\text{ЗФ}} = P_{\text{ЗДЛ}} = 10^{-32}$	l при $P_{\text{ЗФ}} = P_{\text{ЗДЛ}} = 10^{-z}$
ЗФ	$P_{\text{ЗФ}}$	10^{38}	10^{41}	10^{44}	10^{70}	10^{38+z}
ЗДЛ	$P_{\text{ЗДЛ}}$	10^{38}	10^{41}	10^{44}	10^{70}	10^{38+z}
ЗФ+ЗДЛ	$P_{\text{ЗФ}}P_{\text{ЗДЛ}}$	$10^{38} + 10^{38}$	$2 \cdot 10^{44}$	$2 \cdot 10^{50}$	$2 \cdot 10^{96}$	$2 \cdot 10^{38+2z}$

Рассматриваются все известные способы построения алгоритмических средств защиты информации, взлом которых потребует одновременного решения двух независимых вычислительно сложных задач. Отмечается, что существующие методы построения таких средств, позволяют строить, как правило, единичные конкретные алгоритмы и протоколы или их подмножества, и не являются универсальными, т.е. не очевидно как применить их для построения основных типов алгоритмов и протоколов обеспечения информационной безопасности без значительных модификаций. В основном они применяется для построения протоколов ЭЦП, однако уравнения для генерации и проверки ЭЦП оказываются трудноанализируемыми, и как показала практика, они сравнительно часто содержат ошибки из-за затруднительного анализа стойкости таких протоколов.

В связи с этим представляется актуальным разработка нового универсального метода построения алгоритмических средств защиты информации, взлом которых требует решения двух независимых вычислительно трудных задач, являющимся свободным, от указанных недостатков.

Во второй главе описан метод построения алгоритмов и протоколов с повышенным уровнем безопасности. В качестве примитива для построения таких алгоритмов и протоколов рассматривается ЗДЛ по составному модулю $n = pq$, являющимся произведением двух больших простых чисел p, q. ЗДЛ по составному модулю определяется относительно некоторых известных чисел $\alpha < n$ (НОД(α,n) $= 1$), y, и состоит в нахождении такого x, что выполняется следующее выражение $y = \alpha^x \bmod n$, в котором y является открытым ключом, x - секретным ключом, α - генератор группы.

ЗДЛ по трудно факторизуемому модулю эквивалентна решению ЗФ модуля n и решению двух ЗДЛ по модулям каждого делителя модуля n $y = \alpha^x \bmod n \Rightarrow y = \alpha^x \bmod p, y = \alpha^x \bmod q$. В случае когда α имеет простой порядок γ такой, что $\gamma \mid (p-1)$, $\gamma \mid (q-1)$, $\alpha^\gamma = 1 \bmod n \Rightarrow \alpha^\gamma = 1 \bmod p, \alpha^\gamma = 1 \bmod q \Rightarrow y = \alpha^x \bmod n \Rightarrow y = \alpha^{x_1} \bmod p, y = \alpha^{x_2} \bmod q$ значения x_1 и x_2, получаемые при решении ЗДЛ по простым модулям p и q соответственно, будут одинаковы и равны значению $x = x_1 = x_2$. В этом случае следует, что для решения ЗДЛ по трудно факторизуемому модулю $n = pq$, необходимо и достаточно решить: ЗФ модуля n; ЗДЛ по модулю наименьшего простого делителя n (имеющую наименьшую трудоёмкость).

При этом вычислительная сложность решения ЗФ числа $n = pq$, определяется размером меньшего делителя, например $q < p$. Если $|p| = 2|q|$ ($|n|$ - битовый размер числа n), то вычислительная сложность решения ЗДЛ по модулю n, вычислительная сложность решения ЗДЛ по модулю p и вычислительная сложность решения ЗФ n являются значениями одного порядка.

В случае использования составного порядка $\gamma = \gamma'\gamma''$ такого, что $\gamma' \mid (p-1)$, $\gamma'' \mid (q-1)$, $\gamma' \nmid (q-1)$ и $\gamma'' \nmid (p-1)$, $\alpha^\gamma = 1 \bmod n \Rightarrow \alpha^{\gamma'} = 1 \bmod p, \alpha^{\gamma''} = 1 \bmod q \Rightarrow y = \alpha^x \bmod n \Rightarrow y = \alpha^{x_1} \bmod p, y = \alpha^{x_2} \bmod q$ значения x_1 и x_2, получаемые при решении ЗДЛ по простым модулям p и q соответственно, будут различны $x_1 \neq x_2 \neq x$, но сравнимы по модулям множителей порядка γ. Для восстановления исходного значения x потребуется решение данной системы сравнений с использованием китайкой теоремы об остатках. Из этого следует, что для решения ЗДЛ по трудно факторизуемому модулю $n = pq$, необходимо и достаточно решить: ЗФ числа n; ЗДЛ по модулю p; ЗДЛ по модулю q. Если разрабатывать алгоритмы и протоколы таким образом, чтобы вычислительная сложность решения обеих задач будет не ниже некоторого заданного уровня сложности, то в случае появления прорывного алгоритма решения для одной из рассматриваемых задач, стойкость таких алгоритмов и протоколов не изменится. Следовательно, использование ЗДЛ по составному модулю n представляет собой достаточно общий подход к построению алгоритмов и протоколов, применение которого позволит расширить количество и типы упомянутых алгоритмов и протоколов.

Обнаружена потенциальная возможность, при определённых условиях генерации параметров, быстрой факторизации составного модуля n с использованием алгоритма Евклида (НОД($\alpha - 1$,n) $= p$). Введены ограничения на выбор порядка группы, для предотвращения такого случая. Разработаны алгоритмы для генерации всех требуемых параметров. Рассчитаны длины параметров для обеспечения конкретных уровней вычислительной сложности ЗДЛ по трудно факторизуемому модулю.

В третьей главе приведено описание разработанных алгоритмов и протоколов обмена секретом по открытом каналам связи и защитного преобразования информации, обладающие повышенным уровнем безопасности.

Рассмотрены варианты децентрализованной и частично децентрализованной (с привлечением доверительного центра, которому доверяют все пользователи) генерации параметров с использованием простого порядка группы γ, а так же децентрализованной генерации с использованием составного порядка группы $\gamma = \gamma'\gamma''$. После распределения параметров, два пользователя системы могут сформировать общий секрет, известный только им двоим.

Решена задача генерации различных значений ключей для одних и тех же абонентов в различных сеансах связи. Для этого во все разработанные протоколы введены дополнительные рандомизирующие параметры, которые гарантируют генерацию различных ключей, при выполнении условия запрета на их повторное использование для нескольких сеансов связи.

Решена задача обмена ключами с использованием различных значений модуля у различных пользователей. Для этого в вычислениях каждого пользователя используются значения своего модуля и модуля второго абонента, с которым устанавливается общий секретный ключ.

Благодаря решению указанных задач были разработаны 3 протокола обмена ключами, имеющих повышенный уровень безопасности: 1) с использованием доверительного центра для генерации системных параметров для всех пользователей; 2) с использованием простого порядка группы и генерацией системных параметров пользователями; 3) с использованием составного порядка группы и генерацией системных параметров пользователями. Общая схема протокола обмена ключами, взлом которого потребует решения двух независимых вычислительно сложных ЗФ и ЗДЛ по простому модулю, с использованием простого порядка группы и генерацией системных параметров пользователями, представлена на рисунке 1. По сравнению с оригинальным протоколом Диффи-Хеллмана значения ключей в разных сеансах различны.

Решена задача отправки сообщения пользователю данной системы по открытым каналам связи. Для этого предложен алгоритм защитного преобразования информации с повышенным уровнем безопасности. Его сравнение с аналогами приведено в таблице 2.

В четвёртой главе приведено описание разработанных протоколов ЭЦП. Разработаны протоколы индивидуальной ЭЦП (рисунок 2), слепой ЭЦП, взлом которых требует решения двух независимых вычислительно трудных ЗФ и ЗДЛ. Достигнуто существенное уменьшение размера подпи-

Пользователь i		**Пользователь** j
..... Генерация открытых ключей		
$\gamma_i \leftarrow_\$ (\mathbb{N}, \gamma_i - prime)$		$\gamma_j \leftarrow_\$ (\mathbb{N}, \gamma_j - prime)$
$p_i \leftarrow_\$ (\mathbb{N}, \gamma_i \mid (p_i - 1),$		$p_j \leftarrow_\$ (\mathbb{N}, \gamma_j \mid (p_j - 1),$
$\gamma_i^2 \not\mid (p_i - 1), p_i - prime)$		$\gamma_j^2 \not\mid (p_j - 1), p_j - prjme)$
$q_i \leftarrow_\$ (\mathbb{N}, \gamma_i \mid (q_i - 1),$		$q_j \leftarrow_\$ (\mathbb{N}, \gamma_j \mid (q_j - 1),$
$\gamma_i^2 \not\mid (q_i - 1), q_i \neq p_i, q_i - prime)$		$\gamma_j^2 \not\mid (q_j - 1), q_j \neq p_j, q_j - prjme)$
$n_i = p_i q_i$		$n_j = p_j q_j$
$\alpha_i \leftarrow_\$ (\mathbb{N}, \alpha_i^{\gamma_i} = 1 \bmod n_i)$		$\alpha_j \leftarrow_\$ (\mathbb{N}, \alpha_j^{\gamma_j} = 1 \bmod n_j)$
$x_i \leftarrow_\$ (\mathbb{N}, x_i < \gamma_i, \lvert x_i \rvert \approx \lvert \gamma_i \rvert)$		$x_j \leftarrow_\$ (\mathbb{N}, x_j < \gamma_j, \lvert x_j \rvert \approx \lvert \gamma_j \rvert)$
$y_i = \alpha_i^{x_i} \bmod n$	$\xrightarrow{OK_i : (y_i, \alpha_i, \gamma_i, n_i)}$	$y_j = \alpha_j^{x_j} \bmod n$
	$\xleftarrow{OK_j : (y_j, \alpha_j, \gamma_j, n_j)}$	
..... Обмен случайными значениями		
$u_i \leftarrow_\$ (\mathbb{N}, u_i < \gamma_j,$ $\lvert u_i \rvert \approx \lvert \gamma_j \rvert)$		
$R_i = \alpha_j^{u_i} \bmod n_j$	$\xrightarrow{R_i}$	$u_j \leftarrow_\$ (\mathbb{N}, u_j < \gamma_i,$ $\lvert u_j \rvert \approx \lvert \gamma_i \rvert)$
	$\xleftarrow{R_j}$	$R_j = \alpha_i^{u_j} \bmod n_i$
..... Вычисление общего секрета		
$Z'_{ij} = y_j^{u_i} \bmod n_j$		$Z'_{ji} = y_i^{u_j} \bmod n_i$
$Z''_{ij} = R_j^{x_i} \bmod n_i$		$Z''_{ji} = R_i^{x_j} \bmod n_j$
$Z_{ij} = Z'_{ij} Z''_{ij}$		$Z_{ji} = Z'_{ji} Z''_{ji}$
..... $Z_{ij} = Z_{ji} = Z$		

Рисунок 1 — Протокол обмена ключами, взлом которого потребует решения двух независимых вычислительно сложных ЗФ и ЗДЛ по простому модулю, с использованием простого порядка группы и генерацией системных параметров пользователями

Таблица 2 — Сравнение характеристик предложенного протокола защитного преобразования информации с аналогами

Протокол	Коэффициент увеличения передаваемых значений	Трудоёмкость защ. преобр. (возв. в ст. по мод.)	Трудоёмкость обр. преобраз. (возв. в ст. по мод.)
предложенный	2	2	1
Цисс 2013	2	3	2
Измаил 2011	2	3	2
Харн 1994	1	5	3
Мак-Кёрлей 1988	2	2	1

си и трудоёмкости алгоритма генерации и проверки ЭЦП (таблица 3 и 4).

Разработаны протоколы коллективной ЭЦП и слепой коллективной ЭЦП. Существенными свойствами разработанных протоколов является фиксированный размер подписи, который не зависит от количества участников протокола.

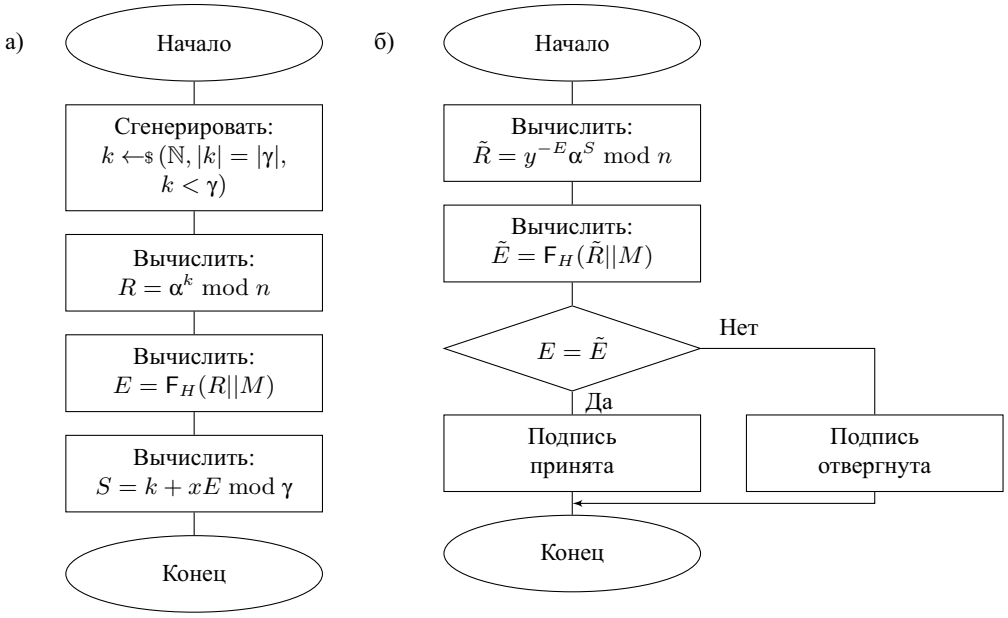

Рисунок 2 — Алгоритмы индивидуальной ЭЦП: а) подписание сообщения M; б) проверка подписи

Таблица 3 — Сравнение характеристик предложенного протокола индивидуальной ЭЦП с аналогами, взлом которых требует одновременного решения ЗФ и ЗДЛ, для 100 битовой стойкости

Протокол ЭЦП	Размер подписи (бит)	Трудоёмкость генерации ЭЦП (возв. в ст. по мод.)	Трудоёмкость проверки ЭЦП (возв. в ст. по мод.)
предложенный	400	1	2
Чиной 2016	4096+4096	13 (вер. алг.)	3
Нимбакар 2014	2048+2048+2048	2	4
Шао 2014	200+2048	2	5
Мадхур 2012	5*2048	4 (вер. алг.)	5
Молдовян 1 2013	200+2048	1 (вер. алг.)	3
Молдовян 2 2013	200+2048	2	3
Молдовян 3 2013	200+200+200	2	3
Виджей 2012	2048+2048	2	4
Измаил 2011	2048+2048	3	4

Таблица 4 — Сравнение характеристик предложенного протокола слепой ЭЦП с аналогами, взлом которых требует одновременного решения ЗФ и ЗДЛ, для 100 битовой стойкости

Протокол ЭЦП	Размер подписи (бит)	Трудоёмкость генерации ЭЦП (возв. в ст. по мод.)	Трудоёмкость проверки ЭЦП (возв. в ст. по мод.)
предложенный	400	3	2
Молдовян 1 2012	200+2048	5	3
Молдовян 2 2012	600	5	3
Тахат 2009	2048+2048	9	4
Тахат 2008	2048+2048+2048	5	4

Все вычисления, производимые участниками, выполняются параллельно, благодаря чему трудоёмкость алгоритма генерации ЭЦП не зависит от количества участников протокола (рисунок 3). Трудоёмкость проверки ЭЦП,

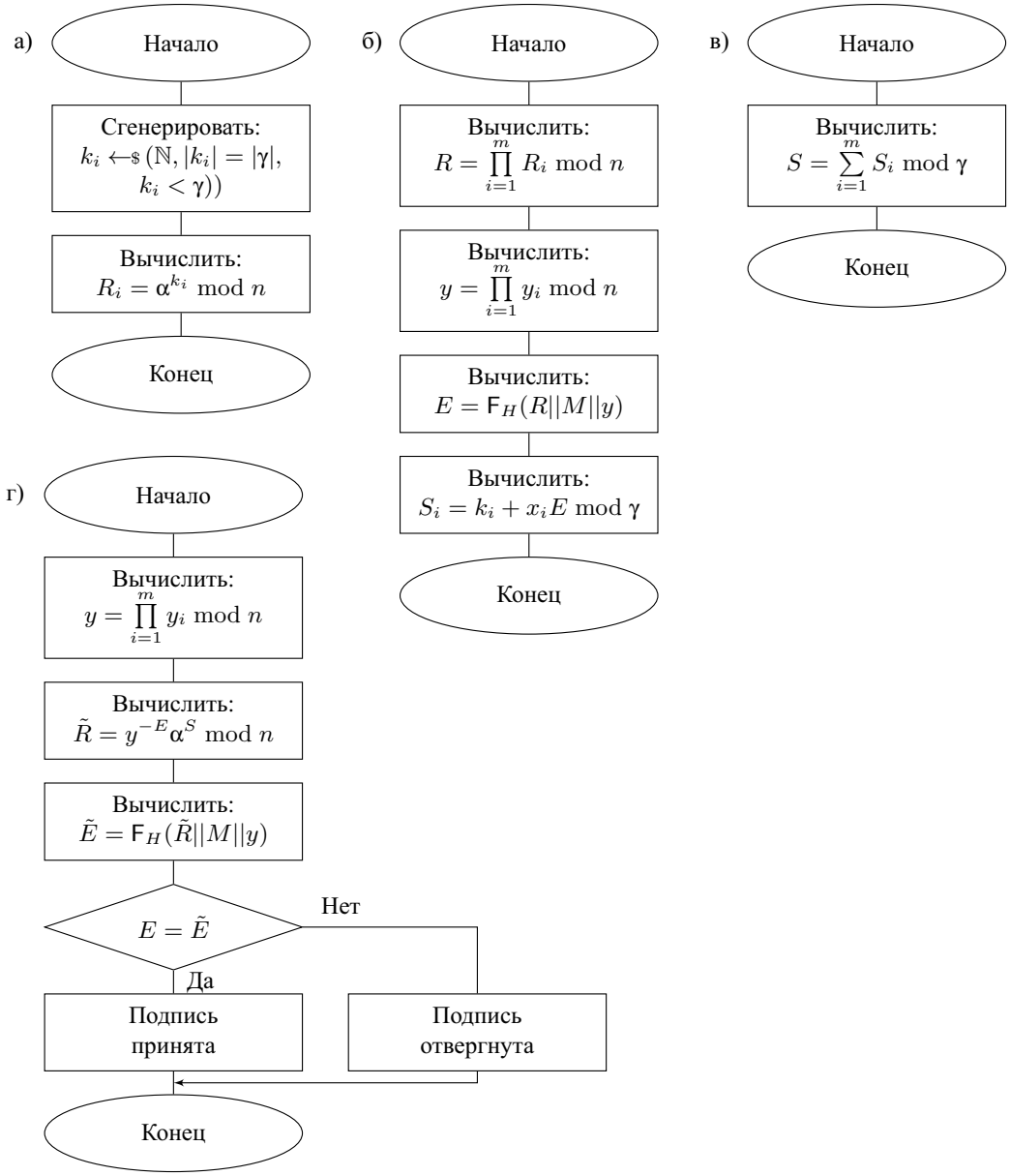

Рисунок 3 — Алгоритмы коллективной ЭЦП для сообщения M: а) генерация рандомизирующих параметров; б) вычисление первого элемента подписи E и вычисление индивидуальной части второго элемента подписи S_i; в) вычисление второго элемента подписи S; г) проверка коллективной ЭЦП

при заранее вычисленном значении коллективного ключа, совпадает с трудоёмкостью проверки индивидуальной ЭЦП. Ключевым моментом всех ранее упомянутых протоколов является одинаковая процедура проверки ЭЦП.

Разработан протокол утверждаемой групповой ЭЦП. Протоколы такого типа призваны максимально повторять действия по ведению работы с документами на реальных предприятиях, где применяется многоступенчатые операции по визированию и утверждению документа. Данный протокол состоит из следующих основных шагов: сотрудники визируют документ путём формирования предподписи к документу; руководитель проверяет визы (предподпись), определяет кто визировал (подписывал) документ, после чего утверждает документ путём формирования из предподписи конечной ЭЦП.

В пятой главе приведено описание специальных протоколов и алгоритмов с повышенным уровнем безопасности. Предложены два варианта про-

токола удалённой аутентификации субъекта, взлом которых требует решения двух независимых вычислительно сложных ЗФ и ЗДЛ по простому модулю: интерактивный и двухшаговый протоколы аутентификации. Интерактивный протокол использует множество запросов для аутентификации пользователя, в то время как двухшаговому достаточно пересылки двух сообщений по открытому каналу связи (рисунок 4 и таблица 5). Оба протокола относятся к классу протоколов с нулевым разглашением, в результате выполнения которых, не происходит никакой утечки о секретном ключе.

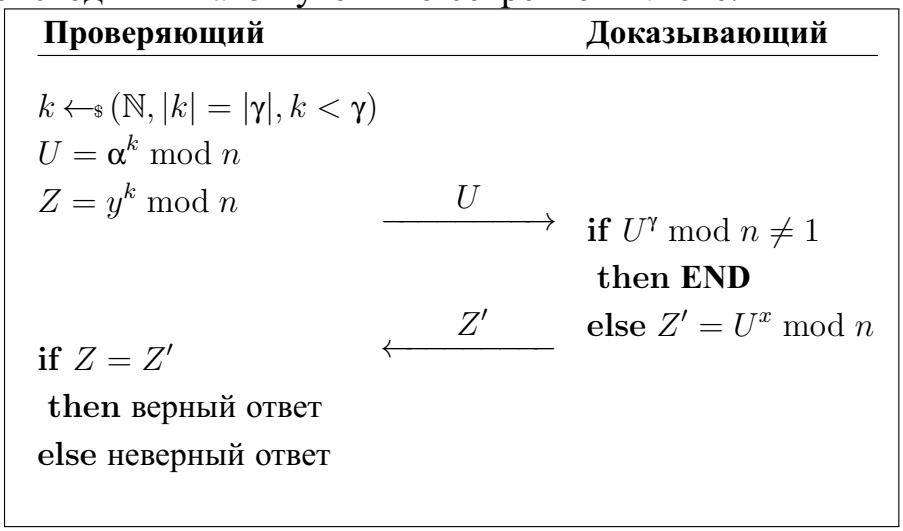

Рисунок 4 — Двухшаговый протокол аутентификации субъекта

Таблица 5 — Сравнение характеристик предложенного протокола двухшаговой аутентификации с аналогами

Протокол	Кол-во посылок по сети	Трудоёмкость выч. доказывающего (возв. в ст. по мод.)	Трудоёмкость выч. проверяющего (возв. в ст. по мод.)
предложенный	2	2	2
Поинтчеваль 2000	4	1 + хэш	2 + хэш
Бриккель 1992	4	1	2
Жиральт 1991	4	1	2

Решена задача построения коммутативного защитного преобразования информации (таблица 6). Использование составного модуля в механизме коммутативного защитного преобразования накладывает ограничения на кодируемые сообщения, а именно, каждое кодируемое сообщение должно принадлежать мультипликативной группе. Для обхода данного ограничения предлагается использовать механизм расщепления сообщения.

Таблица 6 — Сравнение характеристик предложенного протокола коммутативного защитного преобразования с аналогами

Протокол	Коэффициент увеличения передаваемого значения	Трудоёмкость протокола (возв. в ст. по мод.)	Используемые трудные задачи
предложенный	2	4	ЗФ+ЗДЛ
Молдовян 1 2014	2	8	ЗФ+ЗДЛ
Молдовян 2 2014	2	4	ЗФ
Похлиг-Хеллман 1984	1	4	ЗДЛ

На основе разработанного протокола коммутативного защитного преобразования строится протокол стойкого защитного преобразования информации по ключу малого размера (например, 56 бит). Для этого в протокол

коммутативного защитного преобразования добавляется аутентификация по ключу малого размера (рисунок 5).

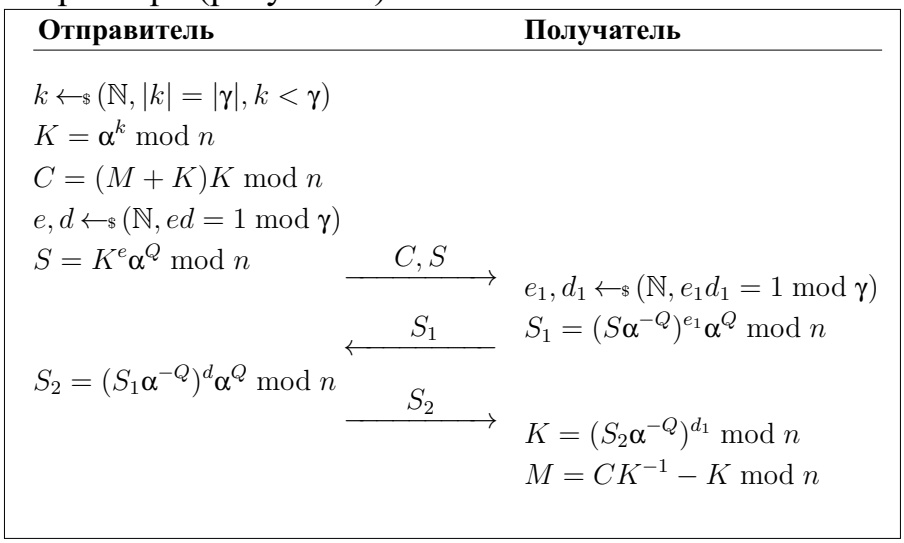

Рисунок 5 — Протокол стойкого защитного преобразования сообщения M по ключу малого размера с повышенным уровнем безопасности

Причём такое применение ключа малого размера отличается от его применения напрямую в алгоритме защитного преобразования информации, так как у нарушителя будет всего одна попытка угадать ключ, в то время как при его использовании в алгоритме защитного преобразования информации у него есть многократная возможность опробования ключа. Вероятность угадывания ключа при длине 56 бит составит 2^{-56}, что является достаточным даже для самых критичных применений.

ЗАКЛЮЧЕНИЕ

В диссертационной работе решена актуальная научно-техническая задача разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения, в том числе получены следующие основные результаты:

1. Впервые предложен метод построения алгоритмов и протоколов, взлом которых требует одновременного решения двух вычислительно сложных задач, отличающийся использованием задачи дискретного логарифмирования (ЗДЛ) по трудно факторизуемому модулю n, размер множителей которого выбирается таким образом, что по крайней мере решение ЗДЛ по модулю одного из делителей модуля имеет вычислительную сложность не ниже заданного уровня стойкости.
2. На основе предложенного метода разработаны новые алгоритмические средства аутентификации объектов и субъектов информационных процессов, обладающие повышенным уровнем безопасности: протокол ЭЦП, протокол коллективной ЭЦП, протокол утверждаемой групповой ЭЦП, протокол интерактивной аутентификации субъекта, протокол двухшаговой аутентификации субъекта.
3. На основе предложенного метода разработаны новые алгоритмические средства защиты информации, обладающие повышенным уровнем безопасности: протоколы обмена ключами, протокол защитного преобразо-

вания информации, протокол коммутативного защитного преобразования информации, протокол стойкого защитного преобразования информации с использованием ключа малого размера.

4. На основе предложенного метода разработаны новые алгоритмические средства обеспечения анонимности, обладающие повышенным уровнем безопасности: протокол слепой ЭЦП, протокол слепой коллективной ЭЦП.

Полученные результаты соответствуют пунктам 5, 11, 13 паспорта специальности 05.13.19 Методы и системы защиты информации, информационная безопасность. Перспективными задачами исследования является внедрение разработанных протоколов в общедоступные программные библиотеки.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В изданиях, рекомендованных ВАК Минобрнауки РФ:

1. **Березин А.Н.** Протокол стойкого шифрования по ключу малого размера, взлом которого требует решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации. — 2016. — № 2. — С. 3-8.
2. **Березин А.Н.**, Молдовян Н. А., Латышев Д. М. Протокол 240–битовой коллективной подписи над нециклической конечной группой // Вопросы защиты информации. — 2013. — № 3. — С. 81–85.
3. **Березин А.Н.**, Молдовян Н. А. Построение криптосхем на основе задачи дискретного логарифмирования по трудно разложимому модулю // Известия СПбГЭТУ «ЛЭТИ». — 2013. — № 7. — С. 54–59.
4. **Березин А.Н.**, Молдовян Н. А., Щербаков В.А. Общий метод построения криптосхем, основанных на трудности одновременного решения задач факторизации и дискретного логарифмирования // Вопросы защиты информации. — 2014. — №2. — С. 3–11.
5. **Березин А.Н.**, Молдовян Н.А., Рыжков А.В. Коммутативные шифры на основе трудности одновременного решения задач факторизации и дискретного логарифмирования // Информационно управляющие системы. — 2014. — №4. — С. 106–110.

В других изданиях:

5. **Berezin A.N.**, Moldovyan N.A., Shcherbakov V.A. Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems // Computer Science Journal of Moldova. — 2013. — V. 21. — № 2(62). — P. 280–290.
6. **Березин А.Н.** Подходы к построению криптосхем на основе трудности одновременного решения задач факторизации и дискретного логарифмирования // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. — СПб, 21-22 ноября 2013 г. / СПб.:ВАС, 2013. — С. 72–76.
7. **Березин А.Н.** Подходы к повышению безопасности криптографических алгоритмов и протоколов // 68–я научно–техническая конференция профессорско–преподавательского состава университета. — Санкт-Петербург, 28 января – 5 февраля 2015 г. / Труды конференции. — СПб.:СПбГЭТУ «ЛЭТИ», 2015. С. — 105–108.
8. **Березин А.Н.** Подходы к построению криптосхем на основе задач факторизации и дискретного логарифмирования // Материалы VIII СПб межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)». — Санкт–Петербург, 23-25 октября 2013 / СПб.:СПОИСУ, 2013. — С. 80–81.
9. **Березин А.Н.** Варианты задачи дискретного логарифмирования по составному модулю // Материалы VIII СПб межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2013)». — Санкт–Петербург, 23-25 октября 2013 г. / СПб.:СПОИСУ, 2013. — С. 81–82.
10. **Березин А.Н.** Коммутативные шифры на основе двух трудных задач // XIV Санкт–Петербургская международная конференция «Региональная информатика – 2014». — Санкт–Петербург, 29–31 октября 2014 г. / Материалы конференции. — СПб.:СПОИСУ, 2014. — С. 121–122.