ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ОБЕСПЕЧЕНИИ И ПОВЫШЕНИИ БЕЗОПАСНОСТИ БАНКОВСКИХ ОПЕРАЦИЙ В ЦИФРОВОЙ ЭКОНОМИКЕ

Матякупова Мадина Кузибай кизи
m.matyakupova@tsue.uz
Носиркулов Асаджон Ахмаджон угли
a.nosirkulov@tsue.uz
Преподаватель кафедры информационных систем и технологий Ташкентского государственного экономического университета.

Аннотация. *В статье рассмотрены информационная структура банковских и кредитных организаций, информационная архитектура, формирование информации о клиентах и банковских организациях, вопросы обучения информационной безопасности. Также проанализированы электронные цифровые подписи и асимметричные криптографические алгоритмы, используемые для обеспечения информационной безопасности в банковских системах, и представлены научные результаты.*

Ключевые слова: *Асимметричные криптосистемы, электронная цифровая подпись, финансовая криптография, технологии блокчейн, DSA, ECDSA, Эль-Гамаль, эллиптические кривые, криптографические протоколы, электронная коммерция, электронная торговля, электронные деньги.*

Введение

В настоящее время развитие процессов обмена информацией, использование современных технологий, таких как искусственный интеллект, IoT, блокчейн в совершенствовании экономической и социальной сфер приносят человечеству множество удобств. Эти глобальные информационно-трансформационные процессы не обошли стороной и нашу страну. В настоящее время в Республике Узбекистан высокие результаты современной науки и информационных технологий стремительно внедряются в социально-экономическую, банковско-финансовую, здравоохранительную, производственную и все другие сферы. Также в результате совершенствования систем электронного правительства, процессов цифровизации и трансформации существенно повышаются показатели цифровой экономики в Республике Узбекистан, что положительно сказывается на показателях валового внутреннего продукта Узбекистана [3].

Процессы информатизации в настоящее время затрагивают практически все отраслиэкономики. Для удовлетворения растущих требований рынка и увеличения потребительского спроса организации внедряют технологии, направленные на

развитие информационно-коммуникационных технологий. Современные компьютерные системы способны в кратчайшие сроки собирать, обрабатывать и анализировать большие объемы информации, при этом минимизируя количество ошибок при выполнении операций. Таким образом, новейшие информационные технологии позволяют повысить скорость выполнения поставленных задач, при этом экономя человеческие, временные и финансовые ресурсы организации[1].

Проблемы экономической безопасности являются основополагающими в современной ситуации развития нашей страны. Устойчивость и защищенность банковской системы во многом определяют также устойчивость экономической системы страны. Цифровая трансформация банковского бизнеса и внедрение информационных технологий оказывают все большее влияние на деятельность организаций в краткосрочной и долгосрочной перспективе, становясь ключевым фактором успешной реализации стратегии и достижения целей бизнеса, способствуют повышению его конкурентоспособности. Однако вместе с ростом производительности труда и внедрением новых финансовых продуктов и технологий появляются и сопутствующие риски, требующие повышенного внимания и комплексных решений.

В банковской системе Республики Узбекистан могут быть некоторые слабые стороны, поскольку наши компании в основном опираются на зарубежные программы и средства передачи данных (международная межбанковская система передачи данных и платежей, SWIFT, платежные системы Visa и Mastercard). Поэтому очень важно создать удобную, гибкую и качественную ИТ-систему, которая поможет нейтрализовать риски информационной безопасности (ИБ). Для защиты коммерческих банков от данного вида угроз обычно используются специальные системы защиты информации (СЗИ).

Большинство специалистов коммерческих банков считают, что наличие системы защиты информации является неотъемлемым признаком практически любой кредитной организации, поскольку позволяет минимизировать риски информационной безопасности. Однако пока никто не знает, как должна выглядеть идеальная СИБ, каковы будут ее состав и структура, поскольку крайне важно обосновать достаточно большой объем финансовых ресурсов, которые будут затрачены на ее создание. В настоящее время бюджеты подразделений, отвечающих за информационную безопасность и построение систем защиты информации, не имеют научного обоснования, а определяются лишь возможностями организаций профинансировать данный проект. Чаще всего руководители компаний руководствуются авторитетом представителей служб безопасности банков, имеющих опыт использования каких-либо систем защиты информации, а также действуют под влиянием рекламы услуг компаний, занимающихся продвижением систем на рынке [1,2].

Важно оценить создание банковской СИБ с точки зрения соотношения стоимости и эффективности ее будущей деятельности, поскольку архитектура,

техническое оснащение и программное обеспечение могут существенно различаться в зависимости от масштабов деятельности кредитной организации. Для этого необходимо создать методику, позволяющую оценить эффективность защиты информации с выделенными этапами, формирующими алгоритм, по которому следует оценивать риски информационной безопасности.

В приведенной таблице 1 представлены угрозы обеспечения информационной безопасности и финансовой информации в банковских и кредитных организациях. Для предотвращения угроз информации необходимо исследование криптографических алгоритмов защиты информации в банковских системах.

Обзор литературы

Проблема обеспечения информационной безопасности в банковских системах интересует не только банковские и кредитные организации, но и математиков, криптографов. Во всем мире ведутся интенсивные научные исследования по применению современных информационных технологий в банковских системах и обеспечению информационной безопасности.

В частности, в научных трудах А. Л. Белоусова исследованы вопросы применения современных информационных технологий в банковских системах, дан ряд рекомендаций по формированию информационной архитектуры кредитных систем. Научные труды Сургуладзе В. Ш., Пчелина А. А. и Кулика Т., Ларсена П. Г. включают защиту информации и разработку политики информационной безопасности, концептуальное обоснование информационной безопасности в кредитных организациях и анализ криптографических алгоритмов, необходимых для решения задач кибербезопасности.

Также узбекскими учеными Джораевым Г.У., Кабуловым А.В. в научных трудах представлены решения таких вопросов, как концептуальные основы обеспечения информационной безопасности в организациях, криптографические методы обеспечения информационной безопасности, информационная безопасность в банковских системах, применение и создание криптографических протоколов в банковских и финансовых системах. Также в научных трудах Рахимбердиева Кувончбека изучаются вопросы использования технологии блокчейн в банковских системах [3,4,5,6,7,16,17,19,20,21,22].

Методология

В ходе научного исследования использованы методы анализа, синтеза и эмпирического исследования, а также криптографические методы обеспечения информационной безопасности в банковских системах и методы криптоанализа.

ПРИМЕНЕНИЕ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКИХ СИСТЕМАХ

Программно-технические средства обеспечения информационной безопасности в банковских системах

В настоящее время в Республике Узбекистан увеличивается использование банкоматов и количество пользователей электронных платежных систем. Поэтому

особое внимание следует уделять совершенствованию финансовых информационных систем и обеспечению информационной безопасности в нашей стране. Современные симметричные и асимметричные ключевые криптографические алгоритмы могут быть использованы для обеспечения информационной безопасности в банковских системах. Алгоритмы такого типа используются для хранения зашифрованных банковских данных и осуществления электронных платежей [5].

Электронные платежные системы — это технология, позволяющая производить расчеты напрямую между контрагентами с использованием электронной связи. Сегодня популярность электронных платежей растет с каждым днем. Электронные платежные системы используют электронные цифровые подписи и специальные методы шифрования при передаче платежных документов. Их реализация может осуществляться как аппаратно, так и программно. Основными методами криптографического преобразования являются методы перестановки и подстановки. Суть первого метода заключается в разбиении исходного текста на блоки, а затем записи этих блоков и считывании шифртекста по разным траекториям геометрической фигуры. Шифрование методом замены заключается в том, что символы исходного текста (блока), записанные в одном алфавите, заменяются символами другого алфавита в соответствии с принятым преобразованием. Известными стандартами в области криптографии являются комбинированный метод шифрования данных — DES (США) и ГОСТ 28147-89, для работы с электронными цифровыми подписями — RSA (США) и ГОСТ 334.10-94. Стандарт DES на протяжении трех десятилетий рассматривается в международной практике как один из лучших образцов криптографических алгоритмов (он основан на комбинациях операций перестановок, подстановок и сложения по модулю два), используемых при хранении и передаче данных в 10-компьютерных системах, в электронных платежных системах, при обмене коммерческой информацией и т. д. В последнее время стандарт DES (используется усиленная версия стандарта — TripleDES — шифрует информацию трижды с использованием стандарта DES) теряет свои позиции из-за возросшей возможности его взлома методом прямого подбора высокопроизводительными компьютерами (длина ключа стандарта DES составляет 64 символа, аналогично российскому стандарту он гораздо более надежен — у него длина ключа составляет 256 символов).

Следует отметить, что современное многофункциональное программное обеспечение, такое как СУБД, ОС и т. д., имеет встроенные процедуры криптографической защиты информации. Существуют специализированные программы, например, Best Sentry 2020, Cryptext и т. д., позволяющие шифровать (расшифровывать) данные на основе ряда алгоритмов (стандартов) на жестких дисках и различных типах носителей информации.

Преимущества программного обеспечения для шифрования:

• высокая устойчивость к дешифрованию.

Недостатки программного обеспечения для шифрования:

• затраты ресурсов (время, оборудование, снижение пропускной способности и т. д.);

• возможность взлома высокопроизводительных систем с помощью прямого подбора ключа.

Преимущества аппаратного шифрования:

• усиление безопасности самих криптографических средств (криптографические функции гарантированно защищены от несанкционированного доступа к ним, что исключает возможность манипуляции ключами со стороны злоумышленника);

• повышение производительности системы за счет выполнения трудоемких криптографических операций на специализированном оборудовании.

Отсутствие аппаратного шифрования:

• высокая стоимость оборудования и его обслуживания

4.2. Моделирование процессов шифрования с асимметричным и симметричным ключом

Выше было отмечено, что основы алгоритмов шифрования формируют математические модели, представляющие алфавитные символы или комбинации символов, представляющие открытую информацию, в алфавитные символы или комбинации символов, представляющие зашифрованную информацию. Поэтому начальный этап классификации алгоритмов шифрования осуществляется на основе типов отражения, основанных на них. Если при шифровании символы открытого алфавита данных заменяются символами алфавита шифруемых данных, то такой алгоритм шифрования на основе отражения относится к классу подстановочного шифрования[7].

Согласно общей идее, математические модели представлений алгоритмов подстановочного шифрования представляются многозначными функциями. Такая ситуация вызывает различные неудобства в процессе декодирования. Поэтому удобно использовать отражения, представленные однозначными (обратными) функциями. Поэтому, естественно, алгоритмы подстановочного шифрования делятся на классы однозначных и многозначных шифрования. В однозначных алгоритмах шифрования каждому символу открытого алфавита данных сопоставляется один символ алфавита зашифрованных данных. В многозначных алгоритмах шифрования каждому из символов открытого информационного алфавита сопоставляется два или более конечного числа символов алфавита шифроинформации, то есть символу открытого информационного алфавита сопоставляется конечный набор $\{y_{i1}, y_{i2}, ..., y_{it}\}$ алфавита шифроинформации любой полученный символ $y_{ij}, (1 \le j \le t)$ будет сопоставлен[9].

Алгоритмы шифрования делятся на симметричные и асимметричные классы в зависимости от типов используемых ключей. Если процессы шифрования и дешифрования выполняются с одним и тем же ключом, то такой алгоритм шифрования относится к классу алгоритмов симметричного шифрования. Если процесс шифрования осуществляется с ключом k_1, а процесс дешифрования осуществляется с ключом k_2, где $k_2 \neq k_1$, и задача нахождения ключа k_2 при знании

ключа k_1 относится к сложным задачам, то такой алгоритм шифрования является асимметричным шифрованием и относится к классу алгоритмов Если в процессе шифрования отдельно полученный символ открытого информационного алфавита всегда заменяется на a_i фиксированный символ b_j шифроинформационного алфавита, то такой алгоритм шифрования относится к классу одноалфавитного шифрования. Если на разных этапах процесса шифрования один полученный символ открытого информационного алфавита заменяется на разные символы зашифрованных данных $b_j, b_l, ..., b_t$ то такой алгоритм шифрования относится к классу многоалфавитного шифрования.

Если в процессе шифрования символы открытого информационного алфавита или комбинации символов алфавита заменяются символами шифроинформационного алфавита или их комбинациями путем выполнения операции, то такой алгоритм шифрования относится к классу геймифицированного шифрования. Если в процессе шифрования символы открытого информационного алфавита или комбинации символов алфавита заменяются символами шифроинформационного алфавита или их комбинациями путем выполнения операции, то такой алгоритм шифрования относится к классу геймифицированного шифрования [8,9].

Входящее финансовое сообщение представлено в кодировке ASCII:

Если открытые данные созданы с помощью компьютера и состоят из символов стандартного алфавита кодов ASCII, то зашифрованные данные создаются в результате применения алгоритма подстановочного шифрования, который заключается в замене одного из символов стандартного алфавита кодов ASCII на другой. После этого процесс шифрования осуществляется на основе следующей таблицы подстановок:

Таблица 2. Входящие биты финансовой информации в формате ASCII

Открытый алфавит данных (стандартные символы кода ASCII)	AS CII_0	AS CII_1		AS CII_{255}
Алфавит шифровальной информации (символы двоичной системы счисления)	$x_0^0 x_1^0 ... x_7^0$	$x_0^1 x_1^1 ... x_7^1$	..	$x_0^{255} x_1^{255} ... x_7^{255}$

Здесь $x_i^j \in \{0;1\}$, восемь бит достаточно для представления 256 различных символов стандартного алфавита кодов ASCII в битах, т.е. $2^8 = 256$.

Это будет равно общему числу ключей алгоритма, представляющего процесс шифрования. Согласно (2) формуле Стирлинга, сложность криптографического алгоритма

следующая[12]:

$$256!=\left(\frac{256}{2,7}\right)^{256}\sqrt{2\cdot 3,14\cdot 256}>\left(\frac{256}{4}\right)^{256}\sqrt{2\cdot 2\cdot 256}>\left(\frac{256}{4}\right)^{256}\sqrt{2\cdot 2\cdot 256}>$$

$$>\left(\frac{4\cdot 2^6}{4}\right)^{256}\sqrt{2\cdot 2\cdot 2^8}=2^{6\cdot 256}\cdot 2^5=2^{1541}$$

4.3. Алгоритм электронной цифровой подписи EL – GAMAL (EGSA)

Развитие науки и использование информационно-коммуникационных технологий (ИКТ) внесли большой вклад в область криптографии. В 1984 году американский ученый Тахер Эль-Гамаль разработал алгоритм ERI "EL-GAMAL" для надежного и стабильного использования подписей на персональных компьютерах. Этот алгоритм, в отличие от других алгоритмов, показал высокую криптостойкость, и в 1991 году алгоритм EL-GAMAL был принят в качестве национального стандарта СШАВ основе алгоритма EL-GAMAL ERI лежит расчет задачи дискретного логарифмирования, которая сложнее деления целых чисел на простые множители[13]. Это устраняет некоторые недостатки алгоритма цифровой подписи RSA Согласно алгоритму ERI "EL-GAMAL", мы можем выбрать некоторые большие простые числа P и Q, $(Q<P)$ для генерации пар ключей. Абоненты, отправляющие и получающие подписанный документ, используют большие целые числа одного и того же значения, числа в диапазоне $P\left(\approx 10^{308}\ or\ 2^{1024}\right)$, $Q\left(\approx 10^{154}\ or\ 2^{512}\right)$.

Абонент, отправляющий документ, выбирает случайное число X, $\left(1\le X\le (P-1)\right)$ и вычисляет выражение

$$Y=Q^X\ mod P \qquad (2)$$

В этом случае число Q является открытым ключом, используемым для проверки подписи абонента, отправляющего сообщение. Число Y отправляется абонентам, получающим документ по открытым каналам. В данном случае число X является секретным ключом для подписи документов, который необходимо хранить в тайне от других злонамеренных подписчиков [14]. Теперь рассмотрим процесс подписания документа. Чтобы подписать данный документ M, сначала хешируйте его до целого числа m, используя хеш-функцию H,

$$m=H(M),(1<m<(P-1)) \qquad (3)$$

где K и P-1 — взаимно простые числа. Затем отправляющий абонент вычисляет целое число a следующим образом.

$$a=Q^k\ mod P \qquad (4)$$

и вычисляет целое число b, используя секретный ключ X, используя расширенный алгоритм Евклида:

$$m=X*a+K+b\left(mod\left(P-1\right)\right) \qquad (5)$$

Пара (a,b) образует электронную цифровую подпись S, которая помещается на документ M.

$$S=(a,b) \qquad (6)$$

Тройка чисел (M,a,b) отправляется адресату, а пара (X,K) сохраняется в тайне.

После получения подписанного документа проверяется совместимость подписи S(a,b) с сообщением M. Для проверки совместимости вычисляется m=h(M) на полученном сообщении M, то есть хэшируется сообщение M. После этого значение выражения [15],

$$A = Y^a a^b (mod P) \quad (7)$$

вычисляется. Если существует только выражение то электронная цифровая подпись считается действительной, в противном случае проверяется следующее отношение, а $Y^a a^b (mod P) = Q^m (mod P)$ если равенство, если оно не выполняется, делается вывод, что подпись поддельная. Последнее (6) равенство выполняется только в следующем случае.

Если подпись S(a,b) в документе получена с использованием открытого ключа Y и секретного ключа X. Каждое сообщение, подписанное алгоритмом EL-GAMAL, требует нового выбора случайного значения K документа. Если значение K используется повторно, то злонамеренный подписчик может найти секретный ключ X (рисунок 3) [16].

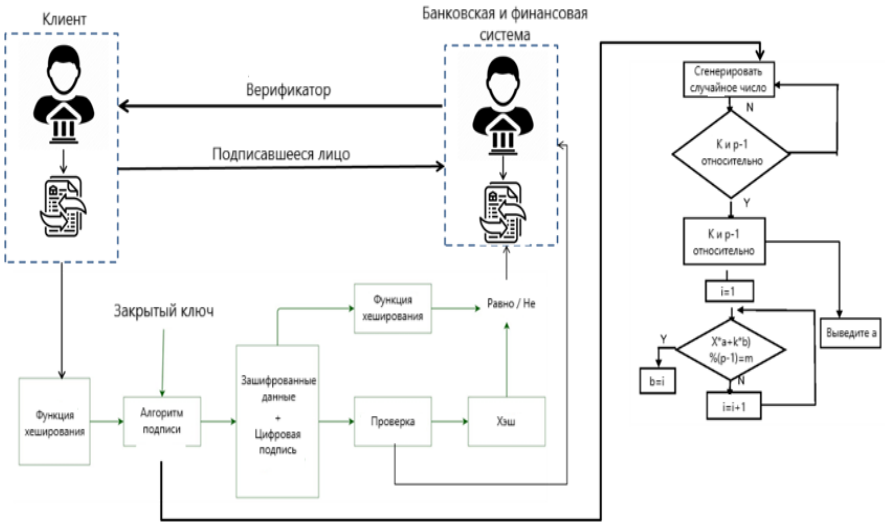

Рисунок 3. Применение алгоритма электронной цифровой подписи Эль-Гамаля в банковской сфере

4.4. DSA — это алгоритм электронной цифровой подписи

Алгоритм электронной цифровой подписи DSA (далее ERI) был предложен Национальным агентством по стандартам США в 1991 году для использования в стандарте DSS. Этот алгоритм был разработан путем усовершенствования алгоритмов Эль-Гамаля и К. Шнорра [17].

В этом алгоритме абонент, отправляющий и получающий документы, использует в вычислениях большие числа q и p Каждое из чисел q и p состоит из L бит $(512 \le L \le 1024)$, g — 160-битное простое число, являющееся делителем $(p-1)$. Числа q, p, g открыты и служат общим образом для всех сетей. Для формирования ERI абонент,

отправляющий документ, выбирает целое число $X, 1<x<g,$ и это число выступает в качестве секретного ключа.

Затем вычисляется значение $Y = q^x mod p$ (8) Число Y является открытым ключом для проверки подписи и оно рассылается всем подписчикам, получающим документ. Алгоритм представляет собой односторонний h hash - хеширование используется через функцию, а в качестве стандарта хеширования используется алгоритм SHA (Secure Hash Algorithm). Итак, алгоритм реализуется в следующей последовательности.

Чтобы подписать документ m, он сначала хэширует его до целого значения m. m=h(M),1<m<q Затем он случайным образом генерирует число K, удовлетворяющее условию 1<k<q, и вычисляет r.

$$r = (g^k mod p) mod q \qquad (9)$$

s — целое число, использующее секретный ключ x.

$$s = (m + r * x) / k \ mod \ q \qquad (10)$$

После этого, $w = 1/s \ mod \ q$ вычисляем выражение и $m = h(M), u_1 = (m * w) mod \ q$, $u_2 = (r * w) mod \ q$, производим вычисления. Затем с помощью открытого переключателя Y . вычисляем значение выражения и проверяем выполнение условия v=r. Если это условие выполняется, то ЭЦП S=(r,s), размещенная в документе M, считается истинной [18].

Анализ и результаты

Процесс создания электронного документа с ЭЦП представлен на рисунке 3, причем сначала вычисляется значение хеш-функции отправляемой информации. Затем, согласно алгоритму цифровой подписи, информация подписывается с использованием закрытого ключа отправителя.

При реализации процессов информационной безопасности и безопасного документооборота в банках и финансовых организациях нами представлено моделирование асимметричных криптосистем и на этой основе — модели и алгоритмы процесса использования алгоритмов электронной цифровой подписи.

Таблица 3. Время генерации и проверки алгоритмов цифровой подписи DSA и EL-Gamal

Algorithm	Время генерации подписи	Время проверки подписи
DSA	0.46/0.34	0.49/0.36
EL-Gamal	0.27/0.19	0.67/0.59

Заключение

В настоящее время в мире стремительно развивается цифровая экономика. В частности, в Республике Узбекистан стремительно развиваются тенденции развития цифровой экономики. Электронное правительство, совершенствование государственных услуг и развитие современных электронных финансовых услуг приносят удобство людям. В то время как совершенствование электронных платежей и дистанционного банковского обслуживания показывает свою экономическую эффективность, в то же время возрастает и актуальность проблемы информационной безопасности. В ходе данного исследования использование алгоритмов цифровой подписи в обеспечении информационной безопасности в банковских и финансовых системах и обеспечении безопасности электронных переводов приводит к эффективным результатам. Также в настоящее время широко используются алгоритмы DSA и EL Gamal. Алгоритмы DSA и El Gamal были проанализированы с использованием нескольких методов и определена их производительность.

ССЫЛКИ

[1] Белоусов А. Л. Некоторые аспекты внедрения информационных технологий в финансовую сферу // Инновационное развитие экономики. Будущее России: материалы и доклады V Всероссийской (национальной) научно-практ. конференции. 2018. С. 7-12.

[2] Г. Джураев и К. Рахимбердиев, Математическое моделирование системы кредитного скоринга на основе задачи Монжа-Канторовича, Международная конференция IEEE по Интернету вещей, электронике и мехатронике 2022 г., Труды IEMTRONICS 2022 г.

[3] Г. Джураев и К. Рахимбердиев, Моделирование процесса принятия решений кредиторами на основе технологии блокчейн, Международная конференция по информационным наукам и коммуникационным технологиям: приложения, тенденции и возможности, ICISCT 2021, стр. 1-5.

[4] Г. Джураев и К. Рахимбердиев, Перспективы применения технологии блокчейн в банковской сфере, Международная конференция по информационным наукам и коммуникационным технологиям: приложения, тенденции и возможности, ICISCT 2022, стр. 1-5.

[5] Кувончбек Рахимбердиев, А.Ишназаров, П.Аллаяров, Ф.Олламберганов, Р.Камалов, М.Матьякупова, Перспективы использования нейросетевых моделей в предотвращении возможных сетевых атак на современные банковские информационные системы на основе технологии блокчейн в условиях цифровой экономики, ICFNDS '22: Труды 6-й Международной конференции по будущим сетям и распределенным системам, декабрь 2022 г., стр. 592–599 https://doi.org/10.1145/3584202.3584291