УДК 004.052.42

Захариудакис Лефтериос, аспирант

МЕТОД БЫСТРОЙ АУТЕНТИФИКАЦИИ УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ КОНЦЕПЦИИ "НУЛЕВЫХ ЗНАНИЙ"

Zacharioudakis Eleftherios. **Method for high speed remote user authentication based on zero-knowledge conception.**

The method for high speed remote abonent authentication has been proposed. Proposed method realized the progressive zero-knowledge conception of cryptographically strong authentication. From mathematical point of view developed method is based on Boolean irreversible transformation in contradistinction to known method which realized zero-knowledge conception utilized the function transformation based on modular arithmetic. The Boolean irreversible transformation in proposed method are implemented by using of standard irreversible hash transformation. Such solution provides a high degree of security against to attacks.

The procedures for remote user registration and authentication cycle were developed in detail. The evaluation of the effectiveness of the proposed method compared to the existing systems of realizing progressive zero-knowledge conception remote abonent authentication of the multi-user system was made. It has been shown that utilization of proposed authentication technology allowed to increase the identification rate by 2-3 orders.

Key words: remote abonent authentication, interactive authentication, strong authentication methods, zero-knowledge authentication conception, hash algorithms.

Захаріудакіс Лефтеріос. Метод швидкої автентифікації віддалених користувачів на основі концепції "нульових знань".

Запропоновано метод прискореної аутентифікації віддалених абонентів багатокористувацьких систем на основі криптографічно строгої концепції "нульових знань". На відміну від відомих методів реалізації вказаної концепції, що мають за основу модулярну арифметику, запропоноване рішення базується на використанні незворотних булевих перетворень, що реалізовані за допомогою стандартизованих хеш-перетворень. Це забезпечує високий рівень стійкості до атак, а також значне спрощення обчислювальних процедур. Проведена теоретична та експериментальна оцінка ефективності довела, що запропонований метод забезпечує підвищення швидкості аутентифікації на 2-3 порядки в порівнянні з відомими методами.

Ключові слова: аутентифікація віддалених користувачів, інтерактивна аутентифікація, строга аутентифікація, концепція аутентифікації "нульових знань", хеш-алгоритми.

Захариудакис Лефтериос. **Метод быстрой аутентификации удаленных пользователей на основе концепции "нулевых знаний".**

Метод быстрой аутентификации удаленных пользователей на основе концепции "нулевых знаний". Предложен метод ускоренной аутентификации удаленных абонентов многопользовательских систем на основе криптографически строгой концепции "нулевых знаний". В отличии от известных методов реализации указанной концепции, которые основываются на модулярной арифметике, предложенное решение базируется на использовании необратимых булевых преобразований, которые реализованы с помощью стандартизированных хеш-преобразований. Это обеспечивает высокий уровень устойчивости к атакам, а также значительное упрощение вычислительных процедур. Проведенная теоретическая и экспериментальная оценка эффективности показала, что предложенный метод обеспечивает ускорение аутентификации на 2-3 порядка по сравнению с известными методами.

Ключевые слова: аутентификация удаленных пользователей, интерактивная аутентификация, концепция аутентификации "нулевых знаний", хеш-алгоритмы.

Вступление

Постановка задачи. Появление компьютерных сетей означает формирование информационного пространства как нового явления, которое перевело жизнь человечества в новое качественное состояние. Разрешив наметившуюся к концу прошлого века проблему "информационного бума", сетевые технологии открыли принципиально новые возможности доступа к данным. Явление глобальной информационной интеграции стало в значительной мере определять прогресс человечества во всех сферах его деятельности.

Оборотной стороной информационной интеграции является настоятельная необходимость в контроле за ее распространением. Значительная часть представляющих практический интерес информационных продуктов является результатом трудоемких исследований и разработок, то есть представляет собой товарный продукт, распространение которого требует возмещения затрат на его создание. Ограничения на использование другого широкого класса информационных ресурсов обусловлены их конфиденциальным характером. Вместе с тем, доступ к этим информационным ресурсам в рамках информационной интеграции должен быть обеспечен легализированным пользователям. Соответственно, возникает задача аутентификации пользователей.

В современных условиях задача аутентификации имеет тенденцию к усложнению, что обусловлен динамичный ростом количества пользователей и расширением технических возможностей для реализации несанкционированного доступа к информационным ресурсам. Это требует адекватного совершенствования методов и средств аутентификации удаленных пользователей, как в плане снижения риска незаконного доступа к информации, так и в плане повышения скорости аутентификации.

С этих позиций повышение эффективности аутентификации удаленных пользователей интегрированных систем представляется актуальной и практически важной для современного этапа развития компьютерных технологий.

Анализ литературных источников. Основным требованием к системам аутентификации удаленных пользователей интегрированных систем обработки информации является обеспечение практической невозможности:

- доступа к ресурсам системы несанкционированным пользователям.
- имитации системой обращения к ней абонента;
- имитации предоставления пользователю ресурсов заинтересованной стороной.

Исходя из анализа методов незаконного получения злоумышленниками доступа к ресурсам многопользовательских систем можно сформулировать следующие требования к системам аутентификации удаленных пользователей:

- при передаче идентификационной информации от пользователя к системе и обратно она должна изменяться от сеанса к сеансу с тем, чтобы не позволить реализовать несанкционированный доступ путем перехвата и повторного использования такой информации злоумышленником;
- аутентификация пользователей должна выполняться, исходя из наличия у них идентифицирующей информации, которая не должна передаваться по линиям связи и которая должна однозначно определять объем информационных ресурсов, доступных пользователю;
- в системе не должно храниться информация, позволяющая реконструировать в полном объеме идентификационную информацию пользователя с тем, чтобы система не могла имитировать обращения к ней со стороны пользователя или незаконное проникновение в систему (с использованием вирусов) не открывало возможностей получение доступа к ресурсам системы под видом и за счет пользователя;
- система аутентификации удаленных абонентов, являясь системой массового обслуживания, должна обеспечивать высокую скорость реализации процесса идентификации пользователей.

В литературе [1] методы идентификации, удовлетворяющие первым трем из приведенных требований называют “строгими”, в противовес остальным, которые называются “слабыми”. К классу “строгих” процедур относятся, большей частью, методы аутентификации, в основе которых лежит концепция “нулевых знаний”. Суть этой концепции состоит в том, что:

- пользователь единолично обладает математической процедурой генерации “правильных” паролей, которые меняются при каждом обращении к системе;
- система обладает математической процедурой, которая позволяет проверить правильность пароля пользователя, но не сама не может сгенерировать “правильный” пароль.

К классу “слабых” процедур аутентификации относится, например, процедура аутентификации пользователей, используемая в операционной системе UNIX [1]. Эта процедура предусматривает сохранение в системе только хеш-образов паролей пользователей, что, при использовании необратимых хеш-преобразований, исключает возможность воспроизведение пароля системой; однако сами пароли не меняются, что позволяет достаточно просто их перехватить.

Наиболее известным из протоколов аутентификации, реализующих прогрессивную концепцию “нулевых знаний” является метод FFSIS (Feige Fiat Shamir Identification Scheme) [2]. FESIS представляет собой относительно простую и вместе с тем достаточно эффективную схему аутентификации абонентов многопользовательских систем, на основе которой создано ряд имеющих практическое значение модификаций. Базовой вычислительной операцией метода является модулярное возведение в квадрат чисел, разрядностью 2048-4096. В плане практического использования основным недостатком FFSIS считается:

- необходимость в большом числе обменов данными между пользователем и системой, что заметно нагружает линии передач и замедляет процесс аутентификации;
- большая вычислительная сложность операции модулярного возведения в квадрат, выполняемой над числами, разрядность которых значительно превышает разрядность процессора.

Другие схемы идентификации, реализующие концепцию “нулевых знаний” с использованием модулярной арифметики, предложенные в [3] требуют существенно меньшего объема пересылок, но предусмотренные ими процедуры имеют большую вычислительную сложность, поскольку вместо операции возведения в квадрат, в них используются операции модулярного экспоненцирования.

В работе [4] предложена система, реализующая идентификацию удаленных пользователей на основе концепции “нулевых знаний” с использованием многозначных необратимых булевых функциональных преобразований. Эта схема позволяет ускорить процесс аутентификации пользователей за 2-3 порядка по сравнению с методами, основанными на модулярной арифметике больших чисел. Однако, рассматриваемая система имеет следующие недостатки:

- процедура генерации неоднозначных необратимых преобразований достаточно сложная и ее реализации требует значительных вычислительных ресурсов;
- хранение таблиц нелинейных булевых преобразований от большого числа переменных требует для каждого из многих тысяч пользователей системы требует больших объемов памяти;
- устойчивость системы к различным видам взломам не достаточно изучена и доказана. В частности, остается открытым вопрос об устойчивости предложенных булевых преобразований к методам дифференциального анализа.

Нерешенные вопросы. Проведенный анализ литературных источников позволяет сделать следующие выводы: расширение использования распределенных систем хранения и обработки данных а также “облачных технологий” требует повышения эффективности аутентификации удаленных пользователей как в плане обеспечения высокого уровня защищенности удаленных ресурсов от незаконного доступа, так и в плане повышения скорости выполнения соответствующих процедур. Наиболее высокий уровень защиты обеспечивают протоколы аутентификации, в основе которых лежит теоретическая концепция “нулевых знаний”. Существующие методы аутентификации, реализующие эту прогрессивную концепцию не обеспечиваю высокой скорости выполнения процедуры аутентификации в силу того, что используют мультипликативные операции модулярной арифметики, имеющие высокую вычислительную сложность.

Цель и задачи исследования. Целью исследований является повышение эффективности аутентификации удаленных пользователей за счет сокращения времени выполнения

соответствующих вычислительных процедур при сохранении высокого уровня защищенности.

Для достижения поставленной цели в работе решаются такие задачи:

- разработка метода аутентификации удаленных пользователей, реализующего теоретическую концепцию нулевых знаний на основе использования стандартизированных криптографических примитивов;
- теоретическое и экспериментальное исследование эффективности разработанного метода как в плане достигаемого уровня защищенности так и в плане скорости реализации вычислительных процедур, связанных с реализацией аутентификации.

1. Метод ускоренной аутентификации

Поставленная цель – радикальное ускорение вычислительной реализации аутентификации, основанной на концепции “нулевых знаний” может быть достигнута за счет применения в качестве базового криптографического преобразования необратимых булевых функций вместо модулярного экспоненцирования. Теоретически считается принятым [1], что в основе любого криптографического механизма лежит математическое необратимое преобразование, то есть преобразование, для которого определено аналитически прямое преобразование, но из которого аналитическим путем принципиально не может быть получено обратное преобразование. На практике криптографической защиты данных в качестве необратимых математических преобразований чаще всего модулярное экспоненцирование (алгоритмы RSA, DSA), операции на эллиптических кривых (алгоритмы ECC) или нелинейные булевы преобразования, которые являются базовыми для построения всех алгоритмов симметричного шифрования (алгоритмы AES и Rijndael в частности), а также все хеш-алгоритмы (SHA-1 и Ripemd-160). Известно, что основным достоинством использования в качестве необратимых преобразований нелинейных булевых функций по сравнению с операциями модулярного экспоненцирования является высокая скорость вычислительной реализации. Так, применительно к задачам шифрования принято считать, что при примерно равном уровне защищенности, алгоритмы симметричного шифрования типа Rijndael обеспечивают на 3 порядка большую скорость по сравнению с алгоритмом шифрования с открытым ключом - Rijndael [5].

Таким образом, использование криптографических механизмов, в основе которых лежат булевы преобразования, для реализации прогрессивной концепции “нулевых знаний” применительно к аутентификации пользователей потенциально позволяет существенно уменьшить время аутентификации.

Для практической реализации указанной возможности предлагается метод аутентификации удаленных пользователей, который реализует концепцию “нулевых знаний” с использованием стандартизированных криптографических примитивов – хеш-алгоритмов. Хеш-алгоритм осуществляет необратимое преобразование сообщения произвольной длины в код хеш-сигнатуры фиксированной длины. Основное свойство хеш-алгоритмов состоит в их необратимости, то есть в том, что нахождение двух разных сообщений с одинаковой хеш-сигнатурой представляется практически невозможным. Хеш-алгоритмы, прошедшие тщательное и всестороннее тестирование, дополненное опытом практического использования получают статус стандарта, необратимость которого гарантируется соответствующими государственными органами. Наиболее известными стандартизированными хеш-алгоритмами являются SHA-1, MD-5 и Ripemd-160 [1].

Предлагаемый метод включает в себя процедуры регистрации пользователя и непосредственно аутентификации.

Процедура регистрации пользователя состоит из следующей последовательности действий:

1) Пользователем определяется число n предполагаемых циклов обращения к системе, выбирает инициирующую символьную строку S, случайным образом формируется маскирующая строка Z.

2) Пользователем вычисляется код $p_n=H(S||n)$, где || - операция конкатенации, H-хеш-преобразование, регламентируемое одним из стандартизированных хеш-алгоритмов.

3) Рекуррентно осуществляется вычисление n кодов сеансовых паролей $p_{n-1}, p_{n-2},\ldots,p_1, p_0$ в соответствии со следующей формулой:

$$\forall j \in \{0,1,\ldots,n-1\} : p_j = H(p_{j+1} \| j). \qquad (1)$$

4) Коды сеансовых паролей $p_{n-1}, p_{n-2},\ldots,p_1, p_0$ сохраняются в закрытой от постороннего вмешательства памяти пользователя.

5) Пользователем генерируется случайным образом ключ ϑ симметричного блокового шифра.

6) Системой сообщается пользователю общедоступный закрывающий системный ключ $K_з$. Этот ключ используется системой на этапе регистрации пользователей как составная часть несимметричного шифра типа RSA. Открывающий ключ K_0 этого шифра содержится системой в секрете.

7) С использованием закрывающего ключа $К_з$ системы, пользователем шифруются код p_0, сгенерированный ключ ϑ и маскирующая строка Z : C_1 = НСШ(p_0, $К_з$), C_2 = НСШ (ϑ, K_3), C_3 = НСШ(Z, K_3), где через аббревиатуру НСШ(x,y) обозначено несимметричное шифрование (например с использованием алгоритма RSA) сообщения x ключом y. Полученные коды C_1 , C_2 и C_3 пересылаются системе.

8) Система с использованием секретного открывающего ключа $К_0$ производит расшифровку полученных кодов: p_0 = НСДШ(C_1, K_0) и ϑ = НСДШ(C_2, K_0), Z= НСДШ(C_3, K_0) где аббревиатурой НСДШ(x,y) обозначено несимметричное дешифрование закодированной посылки x ключом y. Восстановленные коды p_0, Z и ϑ сохраняются системой в защищенной памяти вместе с номером η последнего сеанса (η=0). Значение p_0 сохраняется в виде переменной λ: $\lambda = p_0$.

Выполнение j-го цикла аутентификации, $j \in \{1,2,\ldots,n\}$ сводится к следующей последовательности действий:

1) Пользователем выбирается из защищенной памяти код j-того сеансового пароля p_j. С использованием ключа ϑ шифруется конкатенация p_j сеансового пароля и номера j сеанса обращения пользователя к системе: U_j = СШ(p_j || j, ϑ) , где аббревиатурой СШ(x,y) обозначено симметричное шифрование сообщения x ключом y.

2) Зашифрованный сеансовый пароль U_j посылается пользователем системе.

3) Системой с использованием ключа ϑ производится дешифрование сеансового пароля U_j, восстанавливая пересланные ей пользователем значения p_j и $j : p_j \| j =$ СДШ(U_j, ϑ), где аббревиатурой СДШ(x,y) обозначено симметричное дешифрование закодированной посылки x ключом y.

4) Системой производится контроль синхронизации сеансов аутентификации путем сравнения кодов j и η. Если $j = \eta+1$, то сеансы пользователя и системы синхронизированы и выполняется переход на п.5. Если $j > \eta+1$, то нарушение синхронизации состоит в том, что система не восприняла предыдущие сеансы аутентификации со стороны пользователя. В этом случае система посылает соответствующее сообщение пользователю, зашифрованное ключом ϑ. Получение такого сообщения означает что имела место имитации системы заинтересованной стороной. Для восстановления синхронизации пользователь выполняет j-η-1 пустых циклов аутентификации начиная с (η+1)-го цикла. Если $j < \eta+1$, то нарушение синхронизации означает, что к системе были обращения заинтересованной стороны от имени пользователя или что система сама делала попытки имитации обращения к ней со стороны пользователя, имея ввиду определенный коммерческий интерес. В этом случае система посылает соответствующее сообщение пользователю, зашифрованное ключом ϑ. Для восстановления синхронизации система устанавливает значение $\eta = j$ -1 и актуализирует соответствующее значение $\lambda = p_{\eta-1}$.

5) Системой выполняется хеш-преобразование $r = H(p_j \| j)$ и полученный результат сравнивается с хранящимся в системе значением λ. Если $r = \lambda$, то идентификация пользователя произведена успешно и ему предоставляются соответствующие права доступа к ресурсам системы. При этом, системой сохраняется в переменной λ значение p_j, а в переменной η значение j: $\lambda = p_j$ и $\eta = j$.

6) Системой выполняется хеш-преобразование $r_j = H(p_j \| Z)$ и полученный код пересылается пользователю.

7) Пользователь, по получении от системы кода r_j производит хеш-преобразование $d = H(p_j \| Z)$. Если $d = r_j$, то считается подтвержденным, что пользователь действительно работает с системой.

2. Анализ эффективности

2.1 Анализ криптостойкости. Важнейшим фактором эффективности предложенного метода аутентификации удаленных пользователей, реализующего криптографически строгую концепцию "нулевых знаний" является оценка уровня защищенности от попыток получить несанкционированный доступ к ресурсам системы.

Повторное использование передаваемого по каналу зашифрованного сеансового пароля U_j на j-том сеансе полностью исключается тем, что сам сеансовый пароль меняется в каждом сеансе.

Если сторона, осуществляющая нарушение защиты имеет доступ к информации, передаваемой по открытому каналу, то при отслеживании h сеансов в ее распоряжении могут оказаться h кодов: $U_1, U_2, \ldots, U_h$ и h хеш-сигнатур $r_1, r_2, \ldots, r_h$. Каждый из кодов $U_1, U_2, \ldots, U_h$ представляет собой шифротекст соответствующего из сеансовых паролей $p_1, p_2, \ldots, p_h$, зашифрованных неизвестным ключом ϑ. Единственным рациональным вариантом действий злоумышленника является перебор всех возможных ключей ϑ, дешифрация наблюдаемых кодов с получением кодов $\zeta_1, \zeta_2, \ldots, \zeta_h$. Если $\zeta_1 = H(\zeta_2 \| 2)$, $\zeta_2 = H(\zeta_2 \| 3)$, …, $\zeta_{h-1} = H(\zeta_h \| h)$, то ключ ϑ подобран правильно. Подбор ключа симметричного алгоритма шифрования представляет собой ресурсоемкую задачу, поскольку объем перебора составляет 2^l, где l – разрядность ключа. При типовом для настоящего времени значении $l = 256$ объем перебора 2^{256} требует предельно больших ресурсов. Но даже восстановив перебором код ключа ϑ, злоумышленник не имеет возможности сгенерировать корректный сеансовый пароль в силу того, что, согласно (1), последний перехваченный им сеансовый пароль является результатом необратимого преобразования над следующим сеансовым паролем. Это означает, что для восстановления текущего пароля злоумышленнику придется каждый раз выполнять процедуру нахождения кода, хеш-сигнатура которой совпадает с последним использованным паролем. При использовании стандартизированных хеш-алгоритмов эта процедура считается практически невыполнимой. Таким образом, предложенный метод обеспечивает фактически двойную защиту сеансового пароля пользователя от стороннего злоумышленника.

Со стороны самой системы практически исключается возможность имитации обращения к ней пользователя, поскольку каждый следующий сеансовый пароль известен только пользователю. Система знает только предыдущий сеансовый пароль и для получения следующего ей необходимо выполнить обратное хеш-преобразование, что при использовании стандартизированных хеш-алгоритмов считается практически невыполнимым. По той же причине информации, хранящейся в системе недостаточно для получения следующего сеансового пароля пользователя. Поэтому проникновение к информации, хранящейся в системе с использованием вирусных атак или недобросовестного персона не позволит получить данные, достаточные для обращения к системе от лица пользователя. Это обеспечивает надежную защиту от несанкционированного доступа с правами и за счет пользователя используя информацию самой системы.

Важным достоинством предложенного метода является его ориентация на использование стандартизированных, тщательно оттестированных и хорошо проверенных практикой криптографических механизмов – стандартизированных шифроблоков и хеш-алгоритмов.

2.2. Оценка производительности реализации функций аутентификации.

Основным преимуществом предложенного метода реализации концепции криптографически строгой аутентификации "нулевых знаний" является повышение скорости выполнение вычислительных процедур.

Предложенный метод в вычислительном плане требует выполнения одной процедуры шифрования и двух операций вычисления хеш-сигнатуры. Если считать, что для шифрования используется современный алгоритм Rijndael с размером блока данных 256, то время выполнения процедуры шифрования можно оценить следующим образом. Алгоритм выполняет 14 циклов. В каждом цикле выполняется: 256 операций замены (время выполнения $256 \cdot t_L$, где t_L-время выполнения процессором логической операции), 24 операций сдвига, 24 операций логического сложения. Таким образом, общее число логических команд и операций замены, необходимых для выполнения 14-ти циклов алгоритма Rijndael составляет 4256, время их выполнения примерно равно $4256 \cdot t_L$. Учитывая, что логические операции в современных процессорах выполняются за один такт [6], можно, в оценочном плане, говорить о том, что алгоритм Rijndael может быть реализован за 4256 тактов.

Хеш-алгоритм SHA-1 состоит из 80-ти циклов, причем на первых 20-ти циклах выполняется 10 логических операций, на вторых и последних 20 циклах – 9 логических операций, а на третьей двадцатке циклов – 11 логических операций. Таким образом, суммарное количество логических операций равно 780. Учитывая, что логическая операция выполняется за один такт, можно считать, что хеш-алгоритм SHA-1 требует для своей реализации 780 тактов работы процессора. Общее число тактов работы процессора, требующееся для реализации предложенного метода аутентификации в оценочном плане определяется как $4256 + 2 \cdot 780 \approx 5800$.

Методом FFSIS процедура аутентификации предусматривает 20 циклов обмена данными между пользователем и системой. На каждом из циклов системой выполняется модулярное возведение в квадрат q-разрядных чисел (в большинстве современных протоколов q=2048). Практически q-разрядное число разбивается на κ секций, длина которых равна разрядности процессора. При q=2048 и разрядности процессора 32 число секций равно 64, κ=64. Модулярное возведение в квадрат состоит из κ^2 процессорных умножений и операций суммирования. Среднее количество операций суммирования равно $1.5 \cdot \kappa^2$. Операция редукции (нахождение остатка) включает в себя, в среднем, q операций вычитания q-разрядных чисел, каждая из которых состоит из κ операций процессорного вычитания. Таким образом, время выполнения модулярного возведения в квадрат определяется как $\kappa^2 \cdot (t_m + 1.5 \cdot t_a) + q \cdot \kappa \cdot t_a$, где t_m – время процессорного умножения, t_a – время выполнения процессорной операции сложения или вычитания. Для типичных для практики значений q=2048, κ=64, с учетом того, что операция умножения на современных процессорах выполняется за 10 тактов, а сложения – за 2 такта [6], суммарное число тактов, требующееся для одного модулярного возведения квадрат может быть оценено как $434 \cdot 10^3$.

Сопоставление числа тактов работы процессора, требующееся для проведения аутентификации предложенным методом (5800) и наиболее быстродействующего аналога – FFSIS показывает, что время реализации предложенной процедуры примерно в 75 раз меньше. На практике метод FFSIS требует примерно 20 выполнений модулярного возведения в квадрат, поэтому расчетное ускорение процесса аутентификации близко к $75 \cdot 20 = 1500$.

Проведенные экспериментальные исследования показали, что время выполнения операции шифрования и двух хеш-преобразований реально в 50-60 раз меньше времени выполнения модулярного возведения в квадрат. Экспериментальная оценка выигрыша во времени полной процедуры аутентификации утруднена тем, что в методе FFSIS выполняется 20 циклов обмена данными по сети между системой и пользователем. Это время, как показали эксперименты, сильно зависит от сетевого трафика. Однако, в целом, можно говорить о том, что предложенный метод обеспечивает ускорение процесса аутентификации удаленных абонентов примерно на 3 порядка.

Вывод

В результате проведенных исследований был предложен метод быстрой аутентификации удаленных абонентов многопользовательских систем, реализующий криптографически строгую концепцию “нулевых знаний”. Особенностью предложенного метода является ориентация на стандартизированные, хорошо и всесторонне испытанные криптографические примитивы – стандартизированные шифроблоки и хеш-преобразования. Это позволяет ускорить процедуру аутентификации, упростить ее реализацию и обеспечивает высокую надежность защиты от попыток несанкционированного доступа в ресурсам системы.

Теоретически и экспериментально доказано, что предложенный метод, за счет использования необратимых булевых преобразований, позволяет на три порядка ускорить вычислительную реализацию аутентификации по сравнению с известными методами реализации строгой аутентификации, в основе которых лежит использование необратимых преобразований теории чисел.

Достигаемое ускорение процедуры аутентификации позволяет увеличить число абонентов многопользовательских систем удаленного доступа к ресурсам, а также повысить уровень защищенности от попыток перехвата третьей стороной процесса обмена данными между системой и пользователем. Разработанный метод ориентирован на использование в облачных технологиях удаленного предоставления информации или вычислительных ресурсов пользователям.

Список использованной литературы

1. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. / B. Schneier - Ed.John Wiley, 1996 - 758 p.

2. Feige U. Zero knowledge proofs of identity / U. Feige., A. Fiat., A. Shamir // Journal of Cryptology.- V.1, №.2.- 1988, - P. 77-94.

3. Soonhwa S. User authentication using mobile phones for mobile payment / S. Soonhwa, Y. Cheong, K. Eunbae, R.Jaecheol // Proceedings of the 2015 International Conference on Information Networking (ICOIN) – 2015 - P. 51-56.

4. Markovskyy O. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution/ O. Markovskyy, N. Bardis, N. Doukas // International Journal of Multimedia Intelligence and Security - V.1,- 2010. - P. 78-82.

5. Зенин О.С. Стандарт криптографической защиты AES./ О.С. Зенин О.С., М.А. Иванов - М.:Из-во Кудиц-Образ.-2002.- 174 с.

6. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы / Б. Брэй пер с англ.- 4 вид.- СПб.: Изд-во “БХВ-Петрербург”, 2005.- 1328 с.

Автор статті

Захаріудакіс Лефтерис – аспірант кафедри обчислювальної техніки, Національний технічний університет України «КПІ» ім. І. Сікорського, Київ, Україна. Тел. +38 097 799 24 62. E-mail: 5b4agl@gmail.com

Author of the article

Zahariudakis Lefteris – post-graduate student of Department Computer systems, National Technical University of Ukraine “Igor Sikorsky KPI”, Kyiv, Ukraine. Tel. +38 097 799 24 62. E-mail: 5b4agl@gmail.com

Дата надходження в редакцію: 05.02.2017 р. Рецензент: д.т.н., проф. М.А. Віноградов