УДК 004.02

В.Б. Середюк, к.е.н.,
Чернівецький торговельно-економічний інститут КНТЕУ,
м. Чернівці

ЗАХИСТ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ СИСТЕМИ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Анотація

Швидкий розвиток безготівкових та електронних платежів дозволяє підвищити швидкість розрахунків між контрагентами, та в той же час заощадити банківським установам на відкритті нових відділень для обслуговування клієнтів та на заробітних платах касирів. Однак широке застосування платіжних систем вимагає постійного вдосконалення існуючих засобів захисту інформації із застосуванням сучасних алгоритмів криптографії. В даній статті нами наведено порівняльний аналіз можливості застосування найбільш поширених алгоритмів генерування електронних цифрових підписів у сфері банківського обслуговування. Визначено переваги та недоліки кожного із них. Встановлено, що робота більшості цих алгоритмів базується на розв'язанні задач, які пов'язані із дискретним логарифмуванням, факторизацією та дискретним логарифмуванням на еліптичних кривих. Наведено рекомендації щодо підвищення надійності системи електронного цифрового підпису.

Ключові слова: електронний цифровий підпис, електронні картки, схема RSA, Эль-Гамаля, DSA, ECDSA, хеш-функція, симетрична та асиметрична схеми, хакерська атака, криптографія.

В.Б.Середюк, к.э.н.,
Черновицкий торгово-экономический институт КНТЭУ, г. Черновцы

ЗАЩИТА ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ СИСТЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Аннотация

Быстрое развитие безналичных и электронных платежей позволяет повысить скорость расчетов между контрагентами и в то же время сэкономить банковским учреждениям на открытии новых отделений для обслуживания клиентов и на заработных платах кассиров. Однако широкое применение платежных систем требует постоянного совершенствования существующих средств защиты информации с применением современных алгоритмов криптографии. В данной статье нами приведен сравнительный анализ возможности применения наиболее распространенных алгоритмов генерирования электронных цифровых подписей в сфере банковского обслуживания. Определены преимущества и недостатки каждого из них. Установлено, что работа большинства этих алгоритмов базируется на решении задач, связанных с дискретным логарифмированиям, факторизацией и дискретным логарифмированием на эллиптических кривых. Приведены рекомендации по повышению надежности системы электронной цифровой подписи.

Ключевые слова: электронная цифровая подпись, электронные карты, схема RSA, Эль-Гамаля, DSA, ECDSA, хеш-функция, симметричная и асимметричная схемы, хакерская атака, криптография.

Volodymyr B. Seredyuk, Candidate of Economics,
Chernivtsi Trade and Economics Institute of KNTEU, Chernivtsi

DATA PROTECTION SYSTEM WITH THE USAGE OF DIGITAL SIGNATURE SYSTEM

Annotation

The rapid development of non-cash and electronic payments can increase the speed of payments between counterparties, and at the same time economize for banking institutions on the opening of

new outlets for customer service and payroll cashiers. However, widespread use of payment systems requires continuous improvement of existing information security with modern cryptography algorithms. In this paper, a comparative analysis of the possibility of applying the most common algorithms for generating digital signatures in banking is given. Advantages and disadvantages of each of them are defined. It is established that most of these algorithms work based on the challenges that are associated with the discrete logarithm, factorization and discrete logarithms on elliptic curves. Recommendations for improving the reliability of digital signature are given.

Keywords: electronic signature, electronic card scheme RSA, El- Gamal, DSA, ECDSA, a hash function is symmetric and asymmetric schemes, hacking, cryptography.

Постановка проблеми. Ні для кого не секрет, що банківська діяльність характеризується більш високим рівнем ризику порівняно з іншими видами підприємницької діяльності. Насамперед це зумовлено особливістю діяльності установ даної сфери, де практично всі операції, які вони здійснюють, тією чи іншою мірою є ризикованими. Важко заперечити той факт, що найбільше це стосується діяльності фінансово-кредитних установ у сфері кредитування. Однак останнім часом все більшого розвитку набуває система електронних платежів.

Згідно із статистичною звітністю, що надається банками-членами платіжних систем Національному банку України, станом на 1 січня 2014 року кількість активних платіжних карток в обігу становила 35 млн. 622 тис., що на 2 млн. 515 тис. (або на 7,6%) більше порівняно з попереднім роком. Загальна сума операцій з використанням платіжних карток, емітованих українськими банками, становила за підсумками 2013 року 916 млрд. 027 млн. грн., що на 174 млрд. 547 млн. грн. більше, ніж рік тому. З них безготівкових платежів було зафіксовано на суму 159 млрд. 138 млн. грн. (що на 67 млрд. 577 млн. грн. більше порівняно з 2012 роком), готівки отримано на суму 756 млрд. 889 млн. грн. (що на 107 млрд. 030 млн. грн. більше порівняно з минулим роком). Кількість банкоматів в Україні станом на 1 січня 2014 року становила 40 тис. 350, що на 4 тис. 198 більше, ніж у 2012-му. Загальна кількість терміналів зросла на 58 тис. 498 одиниць – до 221 тис. 222 [1].

У зв'язку із зростанням темпів розвитку ринку безготівкових розрахунків, більш гостро постає питання забезпечення захисту банківськими установами не тільки рахунків своїх клієнтів, але й трансакцій, які ті проводять. Адже не слід забувати, що окрім звичайних платежів, які здійснюються клієнтами через систему «клієнт-банк», POS-термінали, термінали самообслуговування і т.д., досить багато платежів здійснюються з використанням систем електронних платежів, рівень захисту яких є досить низьким. Все це призводить до збільшення кількості несанкціонованого доступу до рахунків як юридичних, так і фізичних осіб, та як наслідок, до фінансових втрат клієнтів.

Аналіз останніх досліджень і публікацій. Над розв'язанням даної проблеми активно працюють як вітчизняні, так і зарубіжні вчені, серед яких можна виділити: А. Чунарьову [2], Д. В. Танцюру, Ю. Ф. Зіньковського [3], Д Н. Молдовяна [4], Б. Шнайпера [5], О. Л. Зуйкова [7] та ін. У своїх роботах вони досліджують основні схеми реалізації алгоритмів електронного цифрового підпису; надійність інформації та методи її захисту; прикладну криптографію тощо. Однак деяким питанням, зокрема ефективності застосування того чи іншого алгоритму шифрування для розв'язання певної задачі чи застосуванню альтернативних методів захисту інформації, особливо у банківській сфері, приділено недостатньо уваги.

Формулювання цілей статті й аргументування її актуальності. Незважаючи на значні суми, які інвестуються банками та іншими фінансово-кредитними установами у вдосконалення існуючих та розробку нових платіжних систем, кіберзлочинність також розвиває свій арсенал. Проблема захисту інформації та несанкціонованого доступу до неї якраз і є гальмівною силою на шляху розвитку систем електронних платежів.

Саме тому головним завданням служби безпеки банку та інформаційного відділу, крім аналізу надійності позичальника, є недопущення несанкціонованого доступу зловмисників до рахунків своїх клієнтів, а у разі вдалого проведення хакерської атаки оперативно її виявляти, з метою мінімізації фінансових втрат.

Виклад основного матеріалу. Для розв'язання даної проблеми банківські установи активно впроваджують додаткові заходи безпеки, які дозволяють більш чітко ідентифікувати платника. Наприклад, відносно недавно для проведення розрахунків в інтернет-банкінгу, клієнту достатньо було ввести лише свій логін і пароль. Ця пара секретної інформації є статичною та залишається незмінною протягом досить довгого часу. Схожий підхід застосовується і при виробництві нового типу платіжних карт – смарт-карт. Однак карти зі статичною авторизацією можливо клонувати за допомогою спеціальних пристроїв.

Ще однією небезпекою, яка пов'язана з технологічною особливістю смарт-карти, є те, в якому вигляді відбувається обмін даними між картою і зчитувальними пристроями – зашифрованому або відкритому.

Крім того, смарт-карта може працювати в двох режимах: онлайн, коли банкомат надсилає відповідний запит у процесинговий центр для ідентифікації карти та платника і чекає від нього підтвердження чи скасування операцій, і офлайн, коли немає зв'язку з процесинговим центром, і на запити терміналу відповідає мікропроцесор карти. Саме в даному режимі, якщо карта застосовує незашифрований протокол обміну даними, PIN-код може бути з легкістю перехоплений

шіммером-закладкою, встановленою всередині контактної групи банкомату або торгового терміналу.

Тому банківські установи, крім звичайної пари – логіна і пароля, вимагають від свого клієнта введення разового сесійного ключа, який або генерується спеціальним брелоком чи програмою у мобільному телефоні, або банк сам висилає клієнту такий ключ через СМС-повідомлення.

Ще одним досить дієвим методом недопущення несанкціонованого доступу до рахунку клієнта є використання електронного цифрового підпису чи електронного цифрового ключа. Дані заходи дозволяють однозначно ідентифікувати відправника (клієнта); уникнути перехоплення, модифікації чи підробки повідомлень та інших даних, які пересилаються в мережі.

Електронний цифровий підпис може бути створений із застосуванням однієї з двох схем: 1) симетрична схема – передбачає наявність третьої особи, яка користується довірою відправника та адресата; 2) асиметрична схема – відноситься до криптосистем з відкритим ключем та не потребує наявності третьої особи. Саме асиметричні схеми є найбільш поширеними при застосуванні електронного цифрового підпису [2].

На сьогодні найбільш поширеними є такі алгоритми генерування цифрового підпису: схема RSA, Эль-Гамаля, DSA, ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002, робота більшості з яких базується на складності розв'язання однієї з трьох задач: дискретного логарифмування; факторизації; дискретного логарифмування на еліптичних кривих.

Залежно від алгоритму функції обчислення підпису можуть бути детермінованими або ймовірнісними. Детерміновані функції завжди обчислюють однаковий підпис за однаковими вхідними даними. Імовірнісні функції вносять у підпис елемент випадковості, що підсилює крипостійкість алгоритмів електронного цифрового підпису. Однак для імовірнісних схем необхідне надійне джерело випадковості (або апаратний генератор шуму, або криптографічно надійний генератор псевдовипадкових бітів), що ускладнює реалізацію.

У наш час детерміновані схеми практично не використовуються. Навіть у детерміновані алгоритми зараз внесено модифікації, що перетворюють їх в імовірнісні (так, в алгоритм підпису RSA друга версія стандарту PKCS # 1 додала попереднє перетворення даних (OAEP), що включає в себе зашумлення). Першою і найбільш відомою у всьому світі системою електронного цифрового підпису стала система RSA, яка ґрунтується на складності задачі факторизації великих чисел, що забезпечує дуже високу криптостійкість алгоритму. Завдяки цьому схема RSA є найбільш поширеною та використовується практично в усіх сучасних програмах для створення електронних цифрових підписів.

Надійність даної схеми пов'язана із складністю розкладу великого складеного числа на прості множники. Процедура шифрування за схемою RSA полягає в модульному піднесенні до степеня за допомогою функції:

$$E(x) = x^e \pmod n, \tag{1}$$

а процедура дешифрування здійснюється з використанням функції:

$$D(x) = x^d \pmod n, \tag{2}$$

де e – частина значення ключа шифрування, d – частина значення ключа дешифрування.

Нехай $n = pq$ – ціле число, що дорівнює добутку двох великих простих чисел p та q. Виберемо числа e і d, які задовольняють умову:

$$ed = l\left(\bmod \eta(n)\right), \tag{3}$$

де $\eta(n) = \eta(p)\cdot\eta(q) = (q-1)\cdot(p-1)$ – значення функції Ейлера.

За відкритий ключ k_2, беруться числа n і d, а за закритим ключем k_1– числа p, q, e. Якщо припустити, що A – відкритий текст, C – криптограма, тоді рівняння шифрування та дешифрування у системі RSA (для електронного цифрового підпису), відповідно, визначатиметься за формулами [3]:

$$C = E_{k_1}(A) \equiv A^e \pmod n; \qquad A = D_{k_2}(C) \equiv C^d \pmod n \tag{4}$$

Таким чином, виходячи із рівнянь (4), можна зробити висновок, що при використанні процедури шифрування за схемою RSA, зловмисник може зламати шифр, тільки знаючи закритий ключ e. Звідси випливає, що з одного боку, розв'язати систему відносно p і q можливо тільки при відомому значенні $\eta(n)$, а з іншого – знаючи p і q, можна з легкістю визначити $\eta(n)$.

Таким чином, обидва випадки, в яких можна визначити закритий ключ, еквівалентні і становлять задачі однієї складності. Тому для надійності алгоритму пропонується вибирати такі значення простих чисел p та q, для яких значення n буде досить великим, що дозволить підвищити стійкість системи до загрози з можливими параметрами продуктивності злому.

Проаналізувавши схему RSA, можна зробити висновок, що перевагою даного алгоритму є забезпечення високої криптостійкості при певній довжині ключа та відносна простота самого алгоритму. Недоліком RSA є низька швидкість роботи алгоритму порівняно з симетричними алгоритмами. Вважається, що для забезпечення необхідної криптостійкості потрібно використовувати відкритий ключ розміром не менше 1024 біт та прості числа – множники розміром не менше 512 біт. Для створення електронно-цифрового підпису при заданих параметрах необхідні великі обчислювальні ресурси, тому час, який відводиться на створення електронного цифрового

підпису, збільшується. Сьогодні відомі деякі способи злому алгоритму RSA, тому при практичному використанні даного алгоритму необхідно також дотримуватися певних умов підбору параметрів системи p і q [4].

Більш надійний і зручний для реалізації на персональних комп'ютерах є алгоритм цифрового підпису, який був розроблений в 1984 р. американцем арабського походження Тахер Ель Гамалем. Схема цифрового підпису Ель Гамаля має низку переваг порівняно зі схемою цифрового підпису RSA:

1) при заданому рівні стійкості алгоритму цифрового підпису цілі числа, які використовуються в обчисленнях, мають на 25% коротший запис, що зменшує складність обчислень майже вдвічі і дозволяє помітно скоротити обсяг використовуваної пам'яті;

2) при виборі модуля p достатньо перевірити, що це число є простим і що число (p – 1) має великий простий множник;

3) процедура формування підпису за схемою Ель Гамаля не дозволяє обчислювати цифрові підписи під новими повідомленнями без знання секретного ключа (як в RSA) [5].

Однак алгоритм цифрового підпису Ель Гамаля має і деякі недоліки порівняно зі схемою підпису RSA. Зокрема, довжина цифрового підпису в 1,5 рази більша, що, в свою чергу, збільшує час її обчислення [6].

Алгоритм цифрового підпису DSA (Digital Signature Algorithm) запропонований в 1991 р., – це розвиток алгоритмів цифрового підпису Ель Гамаля і К. Шнорра. Суть даного алгоритму складається з наступних кроків:

1. Клієнт та банківська установа генерують великі цілі числа g, p, q, які надалі будуть використовуватись при обчисленнях та є відкритими параметрами криптосистеми, при чому g і p – прості числа розмірністю L біт кожне (512 < L < 1024), q – просте число довжиною 160 біт (дільник числа (p –1)).

2. Клієнт вибирає випадкове ціле число x (1 < x < q), що є його секретним ключем, після чого обчислюється значення відкритого ключа:

$$y = g^x \bmod p\,, \tag{5}$$

яке передається банківській установі, в якій обслуговується даний клієнт.

Для того щоб підписати документ A, клієнт хешує його в ціле хеш-значення m з використанням односторонньої функції хешування h(·), визначеної в алгоритмі безпечного хешування SHA:

$$m = h\left(A\right),\ 1 < \mathrm{m} < \tag{6}$$

Хеш-функція – це функція перетворення певним чином вихідного повідомлення (інформації) у відповідний повідомленню код – згортку, яка слугує для контролю цілісності даних та не є частиною алгоритму

електронного цифрового підпису, тому в схемі може бути використана будь-яка надійна хеш-функція. Згортка шифрується з відкритим ключем і, як наслідок, – стає невід'ємною частиною повідомлення (тобто прикріплюється до нього). Особливістю шифрування з відкритим ключем є те, що для шифрування і дешифрування використовуються два різні, взаємонезалежні ключі – закритий і відкритий відповідно. Закритий ключ – це той ключ (набір символів), за допомогою якого відбувається шифрування згортки і який відомий лише власнику відповідного електронного цифрового підпису. Відкритий ключ – це той ключ, який слугує для дешифрування згортки (перевірки електронного цифрового підпису) і публікується центром сертифікації ключів (тобто є загальновідомим).

3. На даному кроці клієнт генерує випадкове ціле число k, 1 < k <q та за допомогою секретного ключа x обчислює:

$$\begin{aligned} r &= \left(g^{k} \bmod p\right) \bmod q \\ s &= \left(m + r \cdot x\right) / k \bmod q \end{aligned} . \qquad (7)$$

Таким чином пара чисел (r, s) = S утворює цифровий підпис S під документом A (наприклад, платіжним дорученням).

Таким чином, підписане повідомлення – це множина чисел [A, r, s].

Банківська установа, одержавши підписане платіжне доручення [A, r, s], перевіряє виконання умов 0 < r < q, 0 < s < q і не приймає документ на обробку, якщо хоча б одна з цих умов не виконана.

Потім одержувач обчислює хеш-функцію $m = h(M)$, значення $w = 1/s \mod q$ і числа $U_1 = (m \cdot w) \bmod q$; $U_2 = (r \cdot w) \bmod q$.

Після перевірки умови $v = r$ (де $v = \left(\left(g^{U_1} \cdot y^{U_2}\right) \bmod p\right) \bmod q$) з використанням для цього відкритого ключа y, підпис S = (r, s) під платіжним дорученням A визнається банківською установою як справжній [7].

Порівняно з алгоритмом цифрового підпису Ель Гамаля алгоритм DSA має наступні основні переваги:

1. При будь-якому допустимому рівні стійкості, тобто при будь-якій парі чисел g і p (від 512 до 1024 біт), числа q, x, r, s мають довжину по 160 біт, скорочуючи довжину підпису до 320 біт.

2. Більшість операцій з числами як при обчисленні підпису, так і при її перевірці проводиться за модулем числа q довжиною 160 біт, що скорочує обсяг пам'яті і час обчислення підпису.

Недоліком алгоритму DSA є те, що при підписуванні і при перевірці підпису доводиться виконувати складні операції ділення по модулю q, що знижує швидкість роботи алгоритму.

Алгоритм ECDSA з відкритим ключем для створення цифрового підпису аналогічний за своєю будовою до DSA, але, на відміну від нього, використовує не цілі числа, а групи точок еліптичної кривої. Стійкість алгоритму ґрунтується на проблемі дискретного логарифмування в групі точок еліптичної кривої. До суттєвих переваг ECDSA над DSA можна віднести: 1) секретний ключ в ECDSA є унікальним, а не лише випадковим, як в DSA, що покращує надійність алгоритму; 2) завдяки складності проблеми дискретного алгоритмування по точках еліптичної кривої система ECDSA є більш криптостійкою та надійною. При цьому довжина підпису залишається такою ж, як і в DSA, і складає 320 біт [8].

Висновки і перспективи подальшого розвитку. Таким чином, надійність (стійкість) системи електронного цифрового підпису насамперед залежить від криптосистеми, яка використовується для його створення. Тому з метою підвищення надійності криптосистеми, перш за все, необхідно підвищувати надійність електронних ключів шифрування і генераторів випадкових послідовностей, що досягається шляхом підвищення складності та створення нових комбінацій чисел. Подальший розвиток криптографії пов'язують із розвитком криптографічних засобів захисту інформації шляхом створення ефективних високонадійних хеш-функцій, алгоритмів шифрування та генераторів псевдовипадкових послідовностей, потреба в яких, як показує практика, не зменшується.

Список використаних джерел:

1. Національний банк України констатує тенденцію до збільшення безготівкових розрахунків за підсумками 2013 року [Електронний ресурс]. – Режим доступу: http://ua.racurs.ua/news/22291-ukrayinci-u-2013-roci-vykorystovu valy-35-6-mln-bankivskyh-kartok.

2. Чунарьова А. Практичні схеми реалізації алгоритмів електронного цифрового підпису : науково-технічний збірник / А. Чунарьова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2013. – Вип. 1 (25) – С. 81–88.

3. Танцюра Д. В. Надійність захисту інформації системи електронного цифрового підпису / Д. В. Танцюра, Ю. Ф. Зіньковський // Вісник Національного технічного університету України «КПІ» Серія – Радіотехніка. Радіоапаратобудування. – К., 2007. – №34. – С. 156–163.

4. Молдовян Д. Н. Новый механизм формирования подписи в схемах ЭЦП, основанных на сложности дискретного логарифмирования и факторизации / Д. Н. Молдовян // Вопросы защиты информации. – 2005. – №4 (71). – С. 81–93.

5. Шнайпер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си / Б. Шнайпер. – М. : Изд. ТРИУМФ, 2008. – 816 с.

6. Алгулиев Р. М. Исследование международных и национальных стандартов цифровой подписи на эллиптических кривих / Р. М. Алгулиев, Я. Н. Имамвердиев // Вопросы защиты информации – 2005. – №2 (69) – С. 2–7.

7. Зуйкова О. Л. Основы криптографической защиты информации : учебное пособие / О. Л. Зуйкова; Московский государственный институт електроники и математики. – М., 2005. – 207 с.

8. Чунарьова А. В. Аналіз алгоритмів формування та перевірки електронно-цифрового підпису [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/35_OINBG_2012/Informatica/4_121780.doc.htm

References:

1. National Bank of Ukraine states tend to increase cashless payments on the basis of 2013 (2014). Available at: http://ua.racurs.ua/news/22291-ukrayinci-u-2013-roci-vykorystovuvaly-35-6-mln-bankivskyh-kartok (Accessed 6 March 2014) (in Ukr.).

2. Chunar'ova, A. (2013). Practical implementation scheme of digital signature algorithms. *Pravove, normatyvne ta metrologichne zabezpechennja systemy zahystu informacii' v Ukrai'ni [Legal, regulatory and metrological support information security system in Ukraine],* vol. 25, pp. 81–88 (in Ukr.).
3. Tancjura, D.V. (2007). Reliability of information security of digital signature. *Visnyk Nacional'nogo tehnichnogo universytetu Ukrai'ny «KPI» [Proceedings of the National Technical University of Ukraine «KPI»],* vol. 34, pp. 156–163 (in Ukr.).
4. Moldovjan, D.N. (2005). New mechanism of signature schemes EDS, based on the complexity of the discrete logarithm and factorization. *Voprosy zashhity informacii [Information security],* vol. 4 (71), pp. 81–93 (in Russ.)
5. Shnajper, B. (2008). *Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na C*. [Applied kryptohrafyya. Protocols, algorithms, texts on C]. Izd. TRIUMF, Moscow, 816 p. (in Russ.).
6. Alguliev, R.M. Study of international and national standards of digital signature on an elliptic curve. *Voprosy zashhity informacii [Information security],* vol. 2 (69), pp. 2–7 (in Russ.).
7. Zujkova, O.L. (2005). *Osnovy kryptografycheskoj zashhyty ynformacyy* [Fundamentals of cryptographic protection of information]. Moskovskyj gosudarstvennyj ynstytut elektronyky y matematyky, Moscow, 207 p. (in Russ.).
8. Chunarova, A.V. (2014). Analysis of algorithms for generation and verification of electronic signature. Available at: http://www.rusnauka.com/ 35_OINBG _2012/ Informatica/4_121780.doc.htm. (Accessed 2 March 2014) (in Ukr.).

УДК. 005.57:339.378

М.В. Тарасюк, д.е.н., **М.Г. Гришко,**
Київський національний торговельно-економічний університет, м. Київ

СУТНІСТЬ Й ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ТОРГОВЕЛЬНИМИ МЕРЕЖАМИ

Анотація

У статті оглянуто та проаналізовано основні сучасні наукові підходи до визначення поняття «інформаційне забезпечення». Сформульовано сутнісні характеристики інформаційного забезпечення. Визначено особливості, які слід враховувати при розробці цілісної теоретичної концепції інформаційного забезпечення управління торговельними мережами. Сформовано перелік вимог до інформаційного забезпечення, що обумовлені основним його призначенням, зокрема: надання релевантної інформації, оперативне надання інформації, створення умов для унеможливлення несанкціонованого доступу і належного захисту комерційної таємниці та інші. Запропоновано розглядати інформаційне забезпечення як складову системи та процесу управління, як систему ресурсного забезпечення, як специфічний вид професійної діяльності, а також з економічної, організаційної, технологічної та технічної точок зору. Надано авторське визначення терміна «інформаційне забезпечення управління торговельними мережами». Обґрунтовано доцільність формування інформаційного забезпечення в управлінні торговельними мережами.

Ключові слова: інформація, інформаційне забезпечення, управління торговельними мережами, торговельні мережі.

М.В. Тарасюк, д.э.н., **М.Г. Гришко,**
Киевский национальный торгово-экономический университет, г. Киев

СУЩНОСТЬ И ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ ТОРГОВЫМИ СЕТЯМИ

Аннотация

В статье рассмотрены и проанализированы основные современные научные подходы к определению понятия «информационное обеспечение». Сформулированы сущностные характеристики информационного обеспечения. Определены особенности, которые следует учитывать при разработке целостной теоретической концепции информационного обеспечения