9. Золотухин С. А. Преимущества и недостатки массовых открытых онлайн-курсов // Журнал научных публикаций «Дискуссия». 2015. №4 (56)

References

1. S. Brown Back to the future with MOOCs? In Proceedings of the 2013 Ed. of ICICTE [Electronic resource]. — Available from: http://www.icicte.org/ Proceedings2013/Papers %202013/06-3-Brown.pdf.

2. McAuley, B. Stewart, G. Siemens, D. Cormier The MOOC Model for Digital Practice (2010) / [Electronic resource]. — Available from: http://davecormier.com/edblog/wp-content/uploads/ MOOC_Final.pdf.

3. V. Kukharenko Innovations in e-Learning: a mass open distance course / Vysshee obrazovanye v Rossyy. 2011. № 10. S. 93–99 [in Russian].

4. K. Buhaychuk Mass open online courses: history, typology, perspectives / Vysshee obrazovanye v Rossyy. 2013. №3. S. 148–155 [in Russian].

5. N. Datsun, L. Urazaeva MOOC aggregator as a recommended system. Information technology in science, management, social sphere and medicine. 2016. S. 337–339 [in Russian].

6. K. Jordan MOOC Completion Rates: The Data [Electronic resource]. — Available from: http://www.katyjordan.com/MOOCproject.html

7. T. Basu Why No One Finishes An Online Course — And Why It Does Matter [Electronic resource]. — Available from: https://www.influencive.com/why-no-one-finishes-online-courses

8. M. Spiridonov Your courses do not pass through? Here is how to fix it [Electronic resource]. — Available from: https://rb.ru/opinion/ne-zakonchili-onlajn-kursy/

9. S. Zolotukhin Advantages and disadvantages of mass open online courses. Journal of Scientific Publications «Discussion». 2015. №4 (56).

Статтю подано до редакції 18.01.2019 р.

УДК 004.62 DOI: 10.33111/mise.97.5

Ващаєв С. С., к.е.н., доцент
кафедри економіко-математичного моделювання,
Мамонова Г. В., к.фіз.-мат.н.,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Нечаєв Ю. А.,
студент 3-го курсу спеціальності «Кібербезпека»,
Київський національний економічний університет
імені Вадима Гетьмана

Vashchaiev S. S., PhD in Economics,
Associate Professor of the Economic and Mathematical Modelling Department
Mamonova G. V.
PhD in Physics and Mathematics,
Associate Professor of the Computer Mathematics and Information Security Department
Nechaev Y. A.,
3rd year Student at the «Cybersecurity» speciality,
Kyiv National Economic University named after Vadym Hetman

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РОЗПОДІЛУ СЕКРЕТУ В КРИПТОГРАФІЇ

MATHEMATICAL MODELING OF SECRET DISTRIBUTION IN CRYPTOGRAPHY

Анотація. *У сучасному світі безпечне збереження інформації, створення алгоритмів, що певним чином зашифровують і розшифровують, стали одними з найголовніших аспектів у криптології.*
Для надійнішого та безпечнішого зберігання та передачі інформації у деяких випадках дуже доцільно використовувати метод розділення секрету.
Доцільно змодулювати таку ситуацію. Багата бабуся роздумує про свою волю і хоче розподілити своє майно порівну між п'ятьма дітьми. Але її діти дуже жадібні, і жінка знає, що якщо вона покине цей світ, її онуки вдаватимуться до неетичних заходів, щоб спробувати отримати більше, ніж їм справедливо визначено. В одному з страхітливих сценаріїв вона турбується, що старші четверо дітей об'єднаються, щоб познущатися над молодшою дитиною і змусити відмовитися від спадщини! Вона відчайдушно хоче, щоб вони співпрацювали, тому вона вирішує заблокувати заповіт, і ключовим є секретне ціле число H. Питання полягає в тому, як вона може поширити цей секретний номер своїм дітям, щоб єдиним способом вони відкрили сейф, якщо всі вони присутні і бажають?
У наш час збереження даних, що надійно заховані, але відкриваються єдиним, цілісним ключем, — не така вже й хороша ідея. Розумний криптоаналітик, дізнавшись всю необхідну інформацію про ключ, розшифрує його та з легкістю отримає доступ до усієї, такої важливої інформації. Саме тому, коли існує значна ймовірність заволодіння даними, застосовуються протоколи поділу секрету для розподіленого та безпечного зберігання необхідної інформації. Найчастіше такою інформацією виявляються секретні ключі або паролі будь-якого абонента. Питання довіри інформації або доступу до даних грає вирішальну роль у компаніях і структурах, які побоюються витоку відомостей і розголошення того, що повинно бути надійно захищено. Принцип розділення даних досить рідкісний і специфічний спосіб захисту інформації. Однак останнім часом він набуває все більшої популярності — і не тільки в сфері національної безпеки. Частини розподіляються та шифруються таким складним чином, аби ніхто не зміг зібрати всі частини ключа та відтворити первинний ключ доступу.
Ключові слова: *криптографія, ключ, захищеність, сертифікація, протоколи безпеки.*

Abstract. *In today's world, secure storage of information and the creation of algorithms that encrypt and decrypt in some way have become one of the most important aspects in cryptology.*
For more secure and secure storage and transfer of information, in some cases it is advisable to use the method of separation of the secret.
It is advisable to modulate the following situation. A rich old woman is drafting her will and wants to distribute her expansive estate equally amongst her five children. But her children are very greedy, and the woman knows that if he leaves her will unprotected her children will resort to nefarious measures to try to get more than their fair share. In one fearful scenario, she worries that the older four children will team up to bully the youngest child entirely out of his claim! She desperately wants them to cooperate, so she decides to lock the will away, and the key is a secret integer N. The question is, how can she distribute this secret number to her children so that the only way they can open the safe is if they are all present and willing?
Nowadays, storing data that is securely hidden but opened with a single, holistic key is not such a good idea. A smart crypto-analyst, having learned all the necessary information about a key, decrypts it and will easily access all such important information. That is why, when there is a significant likelihood of data capture, secret sharing protocols are used to distribute and securely store the necessary information. Most often, this information reveals the secret keys or passwords of any subscriber. The issue of trusting information or access to data plays a crucial role in companies and entities that fear leakage and the disclosure of what needs to be securely protected. The principle of data separation is a rather rare and specific way of protecting information. However, in recent times it has become increasingly popular — and not just in the field of national security. The parts are distributed and encrypted in such a complicated way that no one can collect all the parts of the key and recreate the primary access key.
Keywords: *cryptography, key, security, certification, security protocols.*

Вступ: Інтернет речей — це нова і перспективна технологія, що має на меті глобальну зміну нашого світу шляхом об'єднання фізичних об'єктів («речей») і кіберпростору. Концепція Інтернету речей включає багато технологій, наприклад Інтернет, розподілені обчислення, машинне навчання, комунікації, великі дані, сенсорні технології, взаємодія машина-людина, машина-машина.

Постановка проблеми: Математика розділення секрету найчастіше застосовується для зберігання секретного ключа центру сертифікації, а також у державній і військовій сфері. Також порогові схеми знаходять застосування в хмарних середовищах і схемах електронного голосування.

Метою статті є дослідження основних понять, що стосуються математики розділення секрету та найвідоміших технік розділення секрету. Визначити основні переваги та недоліки схем.

Виклад основного матеріалу: Розділення секрету — термін у криптографії, під яким розуміють будь-який зі способів розподілу секрету серед групи учасників, кожному з яких дістається певна частина секрету. Секрет може відтворити тільки коаліція учасників з первісної групи, причому входити в коаліцію має не менше деякого відомого спочатку числа.

Схеми поділу секрету застосовуються у випадках, коли існує значна ймовірність компрометації одного або кількох зберігачів секрету, але ймовірність її змови значної частини учасників, у більшості випадків, вважається мізерно малою.

Існуючі схеми мають дві складові: розподіл і відновлення секрету. До поділу відноситься формування частин секрету і розподіл їх між членами групи, що дозволяє розділити відповідальність за секрет між її учасниками. Зворотна схема повинна забезпечити його відновлення за умови доступності його зберігачів у деякій необхідній кількості.

Для того, щоб скласти уявлення про завдання, для вирішення яких треба було б створювати схеми поділу секрету, наведемо такий історичний приклад.

У книзі «Gent und seine Schoenheiten» (Thill-Verlag, Bruessel, 1990) описується такий історичний приклад. У IIX-XIV вв. у бельгійському місті Генті була побудована ратушна вежа. У «секреті», тобто самому надійному приміщенні, зберігалися статути і привілеї, які мали важливе значення. Приміщення мало двоє дверей, кожна з трьома замками. Ключі від цих замків перебували у володінні різних цехів. Документи зберігалися в шафі, замкненій на три замки. Один ключ від шафи зберігався у фогта, а два інших — у головного шеффена. Таким чином, отримати доступ до документів могли тільки спільно присутні представники трьох цехів, фогт і шеффен. Тому інтерес до протоколів поділу секрету виник задовго до появи криптографічних протоколів як наукового напрямку.

Протоколи поділу секрету застосовуються для розподіленого зберігання інформації. Найчастіше такою інформацією виявляються секретні ключі або паролі будь-якого абонента. Наприклад, головний бухгалтер підприємства тримає секретну робочу інформацію зашифрованою, а ключ, довжиною 64 біта, зберігає в надійному місці, відомому тільки йому.

Небезпека втрати даних з'являється, коли відбуваються певні непередбачені ситуації, наприклад звільнення бухгалтера, що є основним держателем ключа чи викрадення схованки із ключем. У такому разі втрата ключа призведе до руйнівних наслідків для всього підприємства. Зменшити рівень небезпеки втрати можна видавши по копії ключа заступнику головного бухгалтера і директору підприємства. Проте тоді існувати велика ймовірність впливу людського фактору на безпеку інформації. Заступник може скористатися копією свого ключа і підмінити інформацію у системі або продати дані конкурентам.

Можна запропонувати такий вихід: розділити ключ на чотири частини по 16 біт і видати одну частину генеральному директору, іншу — його заступнику, третю — заступнику головного бухгалтера, а четверту — чоловікові (дружині) головного бухгалтера. Але що як заступники домовляться змістити своїх начальників і скористаються своїми частинами ключа? Тоді для того, щоб відновити ключ, зловмисникам потрібно підібрати лише 32 біта, що буде потребувати всього $2^{32} \approx 4{,}3 \cdot 10^9$ операцій замість $2^{64} \approx 18{,}5 \cdot 10^{18}$ при підборі 64 бітів. Зловмисники зможуть відновити ключ у цілком найближчому майбутньому. Розумним буде розділити цей 64-бітовий ключ K так, щоб кожному дісталося по 64 біта. Генеральному директору, і заступникам можна видати по випадковому 64-бітовому рядку S_1, S_2, S_3, відповідно, а дружині (чоловіку) головного бухгалтера — рядок

$$S_4 = K - S_1 - S_2 - S_3 (mod 2^{64}). \quad (1)$$

Тоді кожен з них буде мати випадковий рядковий біт, по якому ключ можна відновити тільки перебором 64-бітового числа.

Навіть з'єднавши три будь-яких частини, не можна отримати ніякої інформації про ключі, і не можна зменшити кількість бітів, які перебираються. Але, при з'єднанні всіх чотирьох частин ключ обчислюється однозначно.

$$S_1 + S_2 + S_3 + S_4 = K (mod 2^{64}). \quad (2)$$

Тільки що було описано найпростішу схему поділу секрету з однією дозволеної групою учасників, що складається з 4-х абонентів.

Для кращого розуміння будь-якої математичної моделі, прийнято її описувати формально, тож опишемо порогову схему розділення секрету формально.

Нехай M — секрет, який необхідно розділити між n учасниками, а структура доступу складається із однієї множини $G = P = \{P_1, P_2 \dots, P_n\}$, тобто відновити секрет можуть лише всі учасники схеми, об'єднавши свої частини. Обирається модуль $d > M$.

Фаза роздачі секрету.

Дилер обирає випадкові числа $S_1, S_2, \dots, S_{n-1}$ із Z_d та обчислює число:

$$S_n = M - S_1 - S_2 - \cdots - S_{n-1}(mod\ d). \quad (3)$$

Оскільки $S_1, S_2, \dots, S_{n-1}$ — це випадкові числа, то і S_n теж буде випадковим числом. Після цього частини секрету $S_1, S_2, \dots, S_n$ дилер розсилає усім учасникам за принципом: i-тий учасник отримує число S_i і так далі.

Фаза відновлення секрету. Учасники $P_1, P_2, \dots, P_n$ об'єднують свої частини секрету та обчислюють: $M = S_1 + S_2 - \cdots + S_{n-1} + S_n(mod\ d)$.

Описана схема є досконалою та ідеальною. Досконаліть випливає з того, що, об'єднавши менш ніж n частин секрету, учасники вирахують випадкове число, яке не дасть ніякої інформації про M. Ідеальність очевидна, оскільки кожен учасник отримує частку секрету, розмір якої дорівнює розміру самого секрету.

Ідея, на якій заснована дана схема, полягає в тому, що для інтерполяції многочлена ступеня k-1 потрібно k точок. якщо ;відомо меншу кількість точок, то інтерполяція буде неможливою. позначимо:

p — велике просте число (більше будь-якого секрету M, який передбачається розділяти в цій схемі). Тоді $M \in Z_p$;

n — число часток секрету;

k — мінімальний розмір дозволеної групи.

1) Підготовча фаза. Дилер вибирає випадковим чином коефіцієнти $s_1, s_2, \dots, s_{k-1} \in Z_p$ і складає секретний многочлен

$$S(x) = s_{k-1}x^{k-1} + s_{k-2}x^{k-2} + \cdots + s_1x + M, \quad (4)$$

де M — розділювальний секрет, а інші коефіцієнти — довільні елементи поля (коефіцієнти многочлена дилер зберігає в таємниці). Очевидно, $S(0) = M$.

Далі дилер вибирає n різних несекретних ненульових елементів $r_1, r_2, \dots, r_n$. Кожен з яких стає у відповідність одному учаснику схеми.

2). Фаза роздачі секрету.

Дилер обчислює значення многочлена

$$c_1 = S(r_1), c_2 = S(r_2), \dots, c_n = S(r_n), \quad (5)$$

Частина кожного користувача A_i — це пара чисел (r_i, c_i), $i = 1, 2, \dots, n$. Частини роздаться учасникам схеми.

3) Фаза відновлення секрету.

Щоб відновити секрет M, треба скористатися інтерполяційної формулою Лагранжа: якщо потрібно побудувати многочлен $S(x)$ ступеня $(k-1)$, який при $x_1, x_2, \dots, x_k$ приймає відповідно значення $y_1, y_2, \dots, y_k$, то цим многочленом буде:

$$S(x) = \sum_{i=0}^{k-1} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}, \quad (6)$$

Так як у схемі поділу секрету многочлен покладено вибрати так, щоб $S(0) = M$, то з формули Лагранжа слідує:

$$M = \sum_{i=0}^{k-1} c_i S_i, \text{ де } S_i = \prod_{j \neq i} \frac{r_j}{r_j - r_i}\, p, \quad (7)$$

Приклад. Розділити секрет M = 11, по (3, 5) – пороговій схемі, в якій будь-які 3 із 5 користувачів можуть відновити секрет. Показати, як 2, 3 і 5 користувачі разом можуть відновити секрет.

Рішення.

Оскільки $k = 3, n = 5$, нехай $p = 13$.

Фаза роздачі секрету: вибираємо секретний многочлен $S(x) = 7x^2 + 8x + 11 (mod\ 13)$.

Обираємо несекретні ненульові елементи: $r_1 = 1, r_2 = 2, r_3 = 3, r_4 = 4, r_5 = 5$ поля. Обчислюємо:

$$c_1 = S(r_1) = S(1) = 7 + 8 + 11 (mod\ 13) \equiv 0 (mod\ 13);$$

$$c_2 = S(r_2) = S(2) = 7*4 + 8*2 + 11 (\text{mod } 13) \equiv 3 (\text{mod } 13);$$

$$c_3 = S(r_3) = S(3) = 7 * 9 + 8 * 3 + 11 (mod\ 13) \equiv 7 (mod\ 13);$$

$$c_4 = S(r_4) = S(4) = 7 * 16 + 8 * 6 + 11 (mod\ 13) \equiv 12 (mod\ 13);$$

$$c_5 = S(r_5) = S(5) = 7 * 25 + 8 * 5 + 11 (mod\ 13) \equiv 5 (mod\ 13).$$

Частини кожного користувача: $(1,0), (2,3), (3,7), (4,12), (5,5)$.

Фаза відновлення секрету: відновимо секрет, зібравши частини 2, 3 і 5 користувачів разом: $M = c_2S_2 + c_3S_3 + c_5S_5$. Обчислимо:

$S_2 = \prod_{j \neq i} \frac{r_j}{r_j - r_2} = \frac{r_3}{r_3 - r_2} * \frac{r_5}{r_5 - r_2} = \frac{3}{3-2} * \frac{5}{5-2} = 3 * 5 * 3^{-1} \equiv 5(mod\ 13)$;

$S_3 = \frac{r_2}{r_2 - r_3} * \frac{r_5}{r_5 - r_3} = \frac{2}{2-3} * \frac{5}{5-3} = -2 * 5 * 2^{-1} \equiv 8(mod\ 13)$;

$S_5 = \frac{r_2}{r_2 - r_5} * \frac{r_3}{r_3 - r_5} = \frac{2}{2-5} * \frac{3}{3-5} = -2 * 3^{-1} * (-3) * 2^{-1} \equiv 1(mod\ 13)$.

Отже: $M = c_2S_2 + c_3S_3 + c_5S_5 = 3 * 5 + 7 * 8 + 5 * 1 \equiv 11(mod\ 13)$. Дана схема знайшла застосування в апаратних криптографічних модулях, де вона використовується для багатокористувацької авторизації в інфраструктурі відкритих ключів.

Також схема використовується в цифровій стеганографії для прихованої передачі інформації в цифрових зображеннях, для протидії атакам по стороннім каналах при реалізації алгоритму AES.

Крім цього, за допомогою схеми Шаміра може здійснюватися нанесення цифрового водяного знаку при передачі цифрового відео та генерація персонального криптографічного ключа, використовуваного в біометричних системах аутентифікації.

До переваг даної схеми поділу секрету відносять:

– ідеальність: відсутня надмірність — розмір кожної з частин дорівнює розміру секрету;

– масштабованість: в умовах схеми (k, n) число власників частини секрету може додатково збільшитися навіть до p (розмір поля). При цьому кількість частин k, необхідних для отримання секрету, залишиться незмінним;

– динамічність: можна періодично змінювати використовуваний многочлен і перераховувати частини, зберігаючи секрет (вільний член) незмінним. При цьому ймовірність порушення захисту шляхом витоку частин зменшиться, так як для отримання секрету потрібно k частин, отриманих на одній версії многочлена.

– гнучкість: у тих випадках, коли сторони не є рівними між собою, схема дозволяє це врахувати шляхом видачі відразу кількох тіней одній стороні.

– Недоліки схеми: ненадійність дилера: за замовчуванням в схемі передбачається, що той, хто генерує і роздає тіні, надійний, що не завжди вірно.

Відсутня перевірка коректності частин сторін. Сторона,що бере участь у розділенні секрету, не може з упевненістю сказати, що її частина справжня оскільки при підстановці у вихідний многочлен завжди виходить правильна рівність.

Схема Шаміра є і досконалою і ідеальною. Її ідеальність випливає з того, що розмір секрету дорівнює розміру p, як і розмір частини, яку необхідно мати кожному учаснику. Для того щоб показати досконаліть, покладемо, що секрет у схемі Шаміра відновлюється шляхом вирішення системи порівнянь. Недозволена множина учасників складе систему з менш, ніж k порівнянь з k невідомими. Рішенням такої системи є множина точок, що лежать на гіперплощинів k-вимірному просторі, а відповідно, ніяке значення секрету не може бути відкинуте, як неможливе.

Висновки. У сучасному світі, довірити весь секрет одній людині дуже небезпечно: її можуть підкупити, залякати і будь-яким іншим способом вивідати відомості. Найочевидніше рішення — поділити секрет на кілька частин і роздати частини різним людям. Головна умова: інформація може бути доступна лише при складанні кількох частин секрету, а краще — при підсумовуванні всіх відразу.

Ідея в тому, щоб довірені до секрету люди могли колективно отримати доступ до інформації, але не окремо. Хоча є і винятки.

Варто зауважити те, що настільки надійний захист, що передбачає поділ таємниці між учасниками, повинен виправдовувати свою складність. Пароль від банківської комірки з коштовностями навряд чи будуть засекречувати за таким принципом. Зате коли мова йде про державну таємницю або доступ до серйозного озброєння, без подібних заходів не обійтися. У бізнесі, особливо великому, поділ секрету теж може стати в нагоді. Припустимо, корпорація веде звітність, вносить дані про доходи або про збитки. Убезпечити доступ можна лише роздавши частини паролів обраним людям — наприклад, з ради засновників, і зробивши їх частки секрету неактивними, без об'єднання усіх частин одночасно.

Література

1. Shamir A. How to share a secret // Com. Of the ACM. — 1979. — Vol. 22, №11. — P. 612-613.

2. Blakley G.R. Safeguarding cryptographic keys // Proc. Of AFIPSNasiona1 ComputerConference. — 1979. — 48. — P.313-317

3. Ященко В.В. Введення в криптографію. — Санкт-Петербург: МЦНМО, 2001. — 237 с.

4. Шнайер Б. Прикладна криптографія. — М.: Изд-во Триумф, 2003. — 816 с.

5. Чмора А. Сучасна прикладна криптографія. — М.: Гелиос АРВ, 2001. -244 с.

6. Блеклі Р.Г., Кабатянский Г.Р. Узагальнення ідеальних схем, розділяючих секрет // Проблеми передачі інформації. — 1997. — Т. 33. — №3. –С. 42–46.

8. Capocelli R.M., De Santis A., Cargano L., Vaccaro U. On the Size of Shares for Secret Sharing Schemes // J. Cryptology. — 1993. V.6 — P. 157–167.

9. Carnin E.D., Greene J.W., Hellman M.E. On Secret Sharing Systems // IEEE Trans.Inform. Theory. — 1983. — V.29. — №1. — P. 231–241.

10. Спельников А.Б. Елліптитчна порогова схема розділення секрету — Вест.Сам. гос. техн. ун-та, серія Физ.-мат. науки — 2009. — №1(18). — С.251-259.

11. C. Asmuth, J. Bloom. A modular approach to key safeguarding // Information Theory, IEEE Transactions on. — 1983. — B. 2. — T. 29.

12. L. Harn, C. Lin. Detection and identification of cheaters in (t, n) secret sharing scheme. — Des. Codes Cryptography — 52(1) — 2009 — P. 15–24.

13.Теорія розділення секрету [Електронний ресурс] — Режим доступу до ресурсу: http://bit.nmu.org.ua/ua/student/metod/cryptology/ %D0 %BB %D0 % B5 %D0 %BA %D1 %86 %D0 %B8 %D1 %8F23.pdf

14. Системи розділення секрету [Електронний ресурс] — Режим доступу до ресурсу: https://dspace.spbu.ru/bitstream/11701/11134/1/vkr.pdf

References

1. Shamir A. How to share a secret // Com. Of the ACM. — 1979. — Vol. 22, №11. — P. 612–613.

2. Blakley G.R. Safeguarding cryptographic keys // Proc. Of AFIPSNasiona1 ComputerConference. —1979. — 48. — P. 313–317.

3. Yashchenko V.V. Introduction to cryptography. — St. Petersburg: ICSMO, 2001. — 237 p.

4. Schneier B. Applied Cryptography. — M .: Triumph Publishing House, 2003. — 816 p.

5. Chmora A. Modern applied cryptography. — M .: Helios ARV, 2001. — 244 p.

6. Blakley R.G., Kabatyansky G.R. Generalization of ideal schemes that share the secret // Problems of information transfer. — 1997. — Vol. 33. — №3. — C. 42–46.

8. Capocelli R.M., De Santis A., Cargano L., Vaccaro U. On the Size of Shares for Secret Sharing Schemes // J. Cryptology. — 1993. V.6 — P. 157–167.

9. Carnin E.D., Greene J.W., Hellman M.E. On Secret Sharing Systems // IEEE Trans.Inform. Theory. — 1983. — V.29. — №1. — P.231-241.
10. Spelnikov AB Elliptical Threshold Separation Scheme — West Sam. state. tech. Univ., Series Phys.-Mat Science — 2009. — №1 (18). — P. 251–259.
11. C. Asmuth, J. Bloom. A modular approach to key safeguarding // Information Theory, IEEE Transactions on. — 1983. — B. 2. — T. 29.
12. L. Harn, C. Lin. Detection and identification of cheaters in (t, n) secret sharing scheme. — Des. Codes Cryptography — 52(1) — 2009 — P. 15–24
13. Secret Sharing Theory [Electronic Resource] — Resource Access Mode: http://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F23.pdf
14. Secret Sharing Systems [Electronic Resource] — Resource Access Mode: https://dspace.spbu.ru/bitstream/11701/11134/1/vkr.pdf

Статтю подано до редакції 17.04.2019 р.

УДК 519.8:330:371.3 DOI: 10.33111/mise.97.6

Великоіваненко Г. І., к.ф.-м.н., професор
кафедри економіко-математичного моделювання
Скіцько В. І., к.е.н., доцент
кафедри економіко-математичного моделювання
Кмитюк Т. Л., к.е.н., доцент
кафедри економіко-математичного моделювання,
Київський національний економічний університет
імені Вадима Гетьмана

Velykoivanenko H. I., PhD in Physics and Mathematical Sciences, Professor of the Ecomomic and Mathematical Modelling Department
Skitsko V. I., PhD in Economics, Associate Professor of the Economic and Mathematical Modeling Department
Kmytiuk T. L., PhD in Economics, Asociate Professor of the Ecomomic and Mathematical Modelling Department
Kyiv National Economic University named after Vadym Hetman

ОСВІТНІ ТЕХНОЛОГІЇ ЯК ДРАЙВЕР РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

EDUCATIONAL TECNOLOGIES AS A DRIVER OF DIGITAL ECONOMY DEVELOPMENT

Анотація. *Цифрова трансформацій є явищем, яке докорінно та безповоротно змінює усталені процеси у бізнесі, суспільстві, освіті, медицині тощо. Завдяки новим технологіям з'являються нові можливості та способи комунікації, виконання професійних завдань, отримання освіти,*