УДК 681.3.07

В.В. Вишнівський, М.К. Жердєв, І.В. Пампуха

СФЕРИ ЗАСТОСУВАННЯ СПОСОБУ ЗАШИФРУВАННЯ-РОЗШИФРУВАННЯ ІНФОРМАЦІЇ З ВИПАДКОВИМ, ВІДКРИТИМ І АДАПТИВНИМ КЛЮЧЕМ

В статті розглянуто основні положення нового способу зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем. Приведені основні сфери його застосування для захисту інформації в мобільних, комп'ютерних мережах, мережі Інтернет, системах радіолокаційного впізнавання, супутникового зв'язку, охоронної сигналізації та на електронних носіях. Даний спосіб дозволяє забезпечити контроль обміну інформацією, високий ступінь криптографічного захисту інформації, високу надійність її передачі та захист від несанкціонованого доступу хакерів і вірусів.

***Ключові слова*:** шифрування, розшифрування, інформація, несанкціонований доступ.

Вступ

Криптографічні методи захисту інформації інформаційних системах (ІС) можуть застосовуватися як для захисту інформації, що обробляється в ЕОМ або зберігається в різного типу запам’ятовуючих пристроях, так і для закриття інформації, що передається між різними елементами системи.

Проблема використання криптографічних методів в ІС стала зараз особливо актуальною. З одного боку, розширилося використання комп'ютерних мереж, зокрема глобальної мережі Інтернет, по яких передаються великі об'єми інформації державного, військового, комерційного і приватного характеру, що не допускає можливість доступу до неї сторонніх осіб. З іншого боку, поява нових потужних комп'ютерів, технологій мережевих і нейронних обчислень зробило можливою дискредитацію криптографічних систем що ще нещодавно вважалися практично не розкривними.

На сьогодні розроблена велика кількість різних методів шифрування, створені теоретичні і практичні основи їх застосування. Переважна більшість цих методів може бути успішно використана для закриття інформації. Проте, одній з центральних проблем в сучасній криптографії займає стійкість шифру. Це пояснюється тим, що досі немає строгих математичних результатів, необхідних для вирішення такої проблеми. Тому стійкість конкретного шифру оцінюється тільки шляхом різних спроб його розкриття і залежить від кваліфікації криптоаналітиків, що розкривають шифр. Одним із шляхів рішення цієї проблеми являється використання способу зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем (ВВАК).

Виклад основного матеріалу

Спосіб зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем призначений для криптографічного перетворення інформації в ІМ, захисту від атак вірусів і несанкціонованого доступу (хакерів) в комп’ютери через цю мережу. Він може бути реалізований програмно, апаратно і програмно-апаратно.

Кращим захистом від способів криптоаналізу є вибір ключового слова по довжині, рівного довжині відкритих даних (ВД), яке відрізняється від відкритих даних за статистичними показниками. Таку схему було запропоновано інженером компанії AT&T Гілбертом Вернамом в 1918 р., у якій оперують не буквами, а двійковими числами. Коротко це можна виразити формулою [1]:

$$C_i = p_i \oplus k_i,$$

де: p_i – *i-е* двійкове значення ВД; k_i – *i-е* двійкове значення ключа; C_i – *i*-е двійкове значення закритих даних (ЗД); $\oplus$ – операція "виключення АБО".

Таким чином, ЗД генеруються шляхом побітового виконання операції "виключення АБО" для ВД й ключа.

Основною проблемою при цьому є спосіб генерування ключа, який за статистичними показниками відрізнявся б від ВД. Вернам запропонував використовувати закільцьовану

стрічку, тобто циклічне повторення ключового слова, тому насправді виконувалась операція зашифрування ВД, хоч і з дуже довгим, але все-таки ключем, який повторюється. Незважаючи на те, що така схема, в силу дуже великої довжини ключа, значно ускладнює завдання криптоаналізу, схему можна «зламати», маючи в розпорядженні досить довгий фрагмент ЗД, відомі або ймовірно відомі фрагменти відкритих даних або й те, і інше відразу.

При цьому способі зашифрована інформація "зламу" не піддається, якщо в якості ключа використовувати випадкову інформацію, тобто в цьому випадку статистичні характеристики ВД й випадкового ключа не корельовано.

Офіцером корпуса зв'язку Джозефом Моборном були запропоновані технічні рішення для покращення схеми Вернама, які зробили цю схему винятково надійною [1]. Він запропонував відмовитися від повторень, а випадковим чином генерувати ключ, довжина якого дорівнює довжині відкритих даних. Така схема одержала назву стрічки однократного використання (або схеми з одноразовим блокнотом) і «злому» не піддається. В результаті її застосування на виході формується випадкова послідовність, яка немає статистичного взаємозв'язку з відкритими даними. Оскільки в цьому випадку ЗД не дають ніякої інформації про ВД, немає способу й «зламати» ключ. Ця ідея була практично реалізована на механічних пристроях. Основним недоліком цієї схеми є низька швидкість передачі інформації. Тому з розвитком електронних засобів зашифрування-розшифрування інформації ця схема втратила актуальність.

Складність практичного застосування цього способу полягає в тому, що як і відправник, так і одержувач повинні мати один і той же випадковий ключ і можливість захищати його від сторонніх [1, 2]. Тому, незважаючи на переваги способу Вернама перед іншими способами, виконаними на електронних пристроях, на практиці його реалізувати складно й дуже дорого. Основна трудність полягає в тому, що генератори випадкових чисел на передавальній і прийомній сторонах повинні працювати синхронно й синфазно.

Авторам запропонованого способу ВВАК вдалося забезпечити синхронну й синфазну роботу випадкових генераторів на передавальній і прийомній сторонах. При цьому відправник й одержувач мають один і той же випадковий ключ. Таким чином, у запропонованому способі зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем реалізована схема Вернама на електронних пристроях. В способі використовуються випадкові (з рівноймовірним розподілом ключі на множині 2^n, де n – розрядність випадкового генератора), особисті і адаптивні ключі, для яких математично доведено, що їх визначити практично не можливо. При цьому ключі спеціально не генеруються, нікому не назначаються і не розподіляються, а автоматично формуються випадковими генераторами, які працюють синхронно й синфазно на передавальній й прийомній сторонах в процесі зашифрування-розшифрування інформації. Ця обставина дозволяє скоротити до мінімуму вплив людського фактору на надійний захист інформації і скоротити сили й засоби, які виділяються в інших способах зашифрування-розшифрування інформації для забезпечення конфіденційності.

Запропонований спосіб дозволив усунути недоліки існуючих способів, спростити процес шифрування-розшифрування інформації й може бути реалізований за допомогою найпростіших мікроконтролерів, в яких передбачено програмно-апаратний захист від несанкціонованого доступу [3, 4].

В статті розглянуто основні сфери застосування розробленого способу ВВАК, який реалізований в пристрої ПЗМТ-1, а саме:

І. Для захисту інформації в комп'ютерних мережах від несанкціонованого доступу при передачі інформації від одного абонента до іншого (рис. 1).

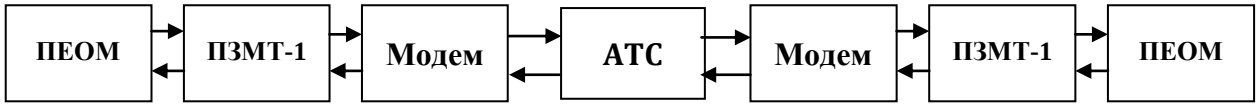

Рис.1. Структурна схема включення ПЗМТ-1 в мережу обміну даними між абонентами

На рис.1 ПЕОМ – персональна електронно-обчислювальна машина; АТС – автоматизована телефонна станція.

II. Для системи захисту інформації на електронних носіях (рис. 2).

Блок спряження з зовнішніми пристроями запису та зчитування інформації	**ПЗМТ-1**	**Простір пам'яті для зберігання інформації**

Рис.2. Структурна схема системи захисту інформації на електронних носіях

III. Для системи радіолокаційного впізнавання, як військових, так і цивільних об'єктів (рис. 3).

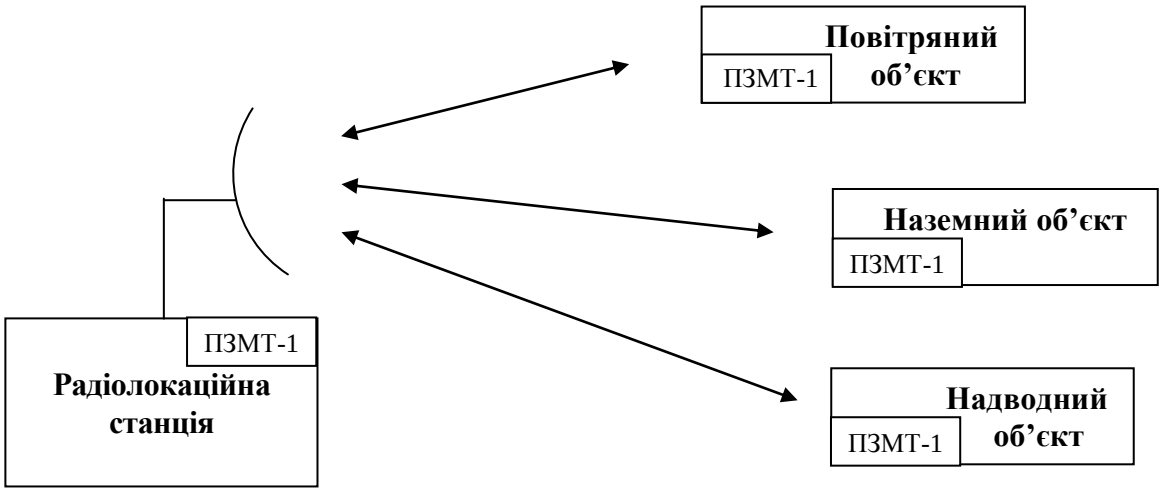

Рис.3. Структурна схема системи радіолокаційного розпізнання об'єктів

IV. Для системи супутникової охорони і спостереження за об'єктами (рис. 4).

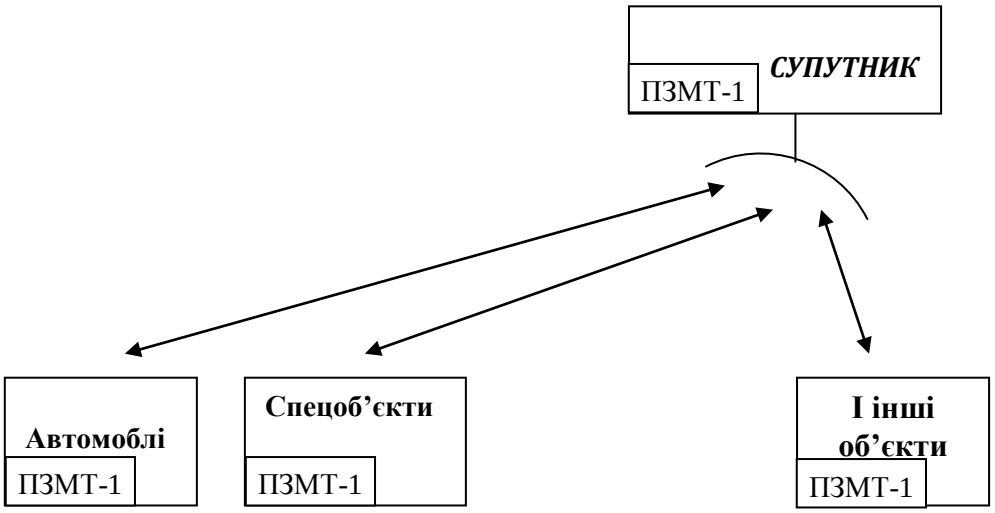

Рис. 4. Структурна схема системи супутникової охорони і спостереження за об'єктами з використанням ПЗМТ-1

V. Для системи охоронної сигналізації (рис. 5).

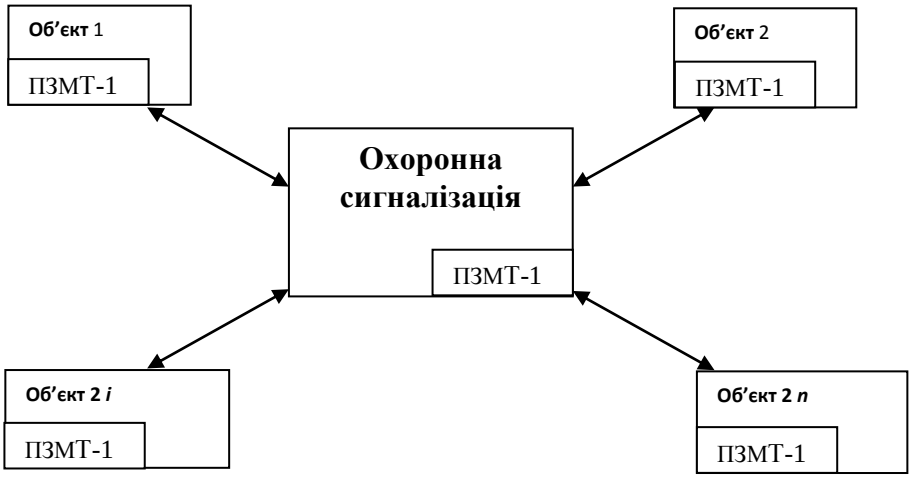

Рис. 5. Структурна схема системи охоронної сигналізації з використанням ПЗМТ-1

VI. Для системи супутникового зв'язку (рис. 6).

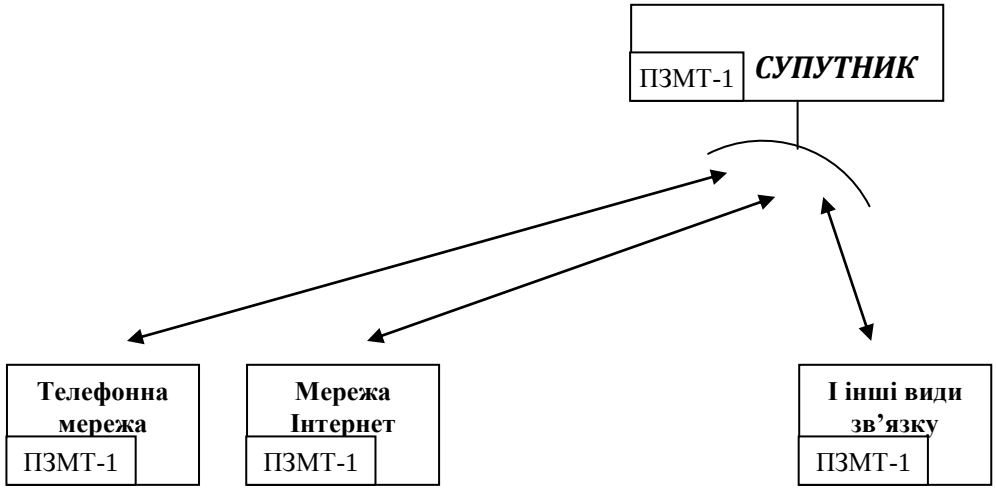

Рис. 6. Структурна схема системи супутникового зв'язку

VII. Для системи захисту банківських рахунків і операцій у банкоматах (рис. 7).

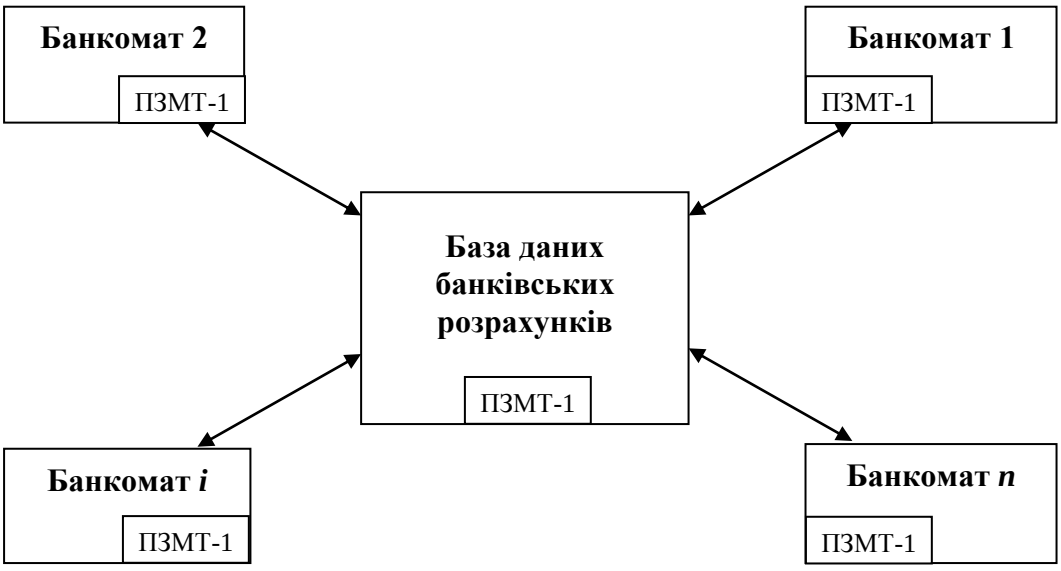

Рис. 7. Структурна схема системи охоронної сигналізації

VIII. Для захисту глобальних мереж Інтернет від несанкціонованого доступу й атак вірусів при передачі інформації від одного термінала до іншого (рис. 8).

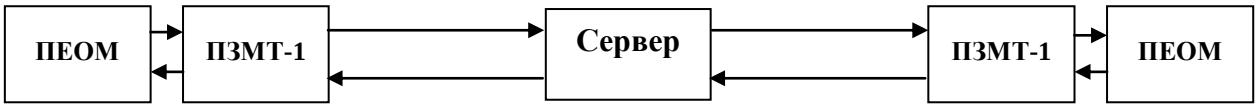

Рис. 8. Структурна схема захисту терміналів в глобальній мережі Інтернет

IX. Для захисту інформації в мобільній мережі між абонентами (рис. 9).

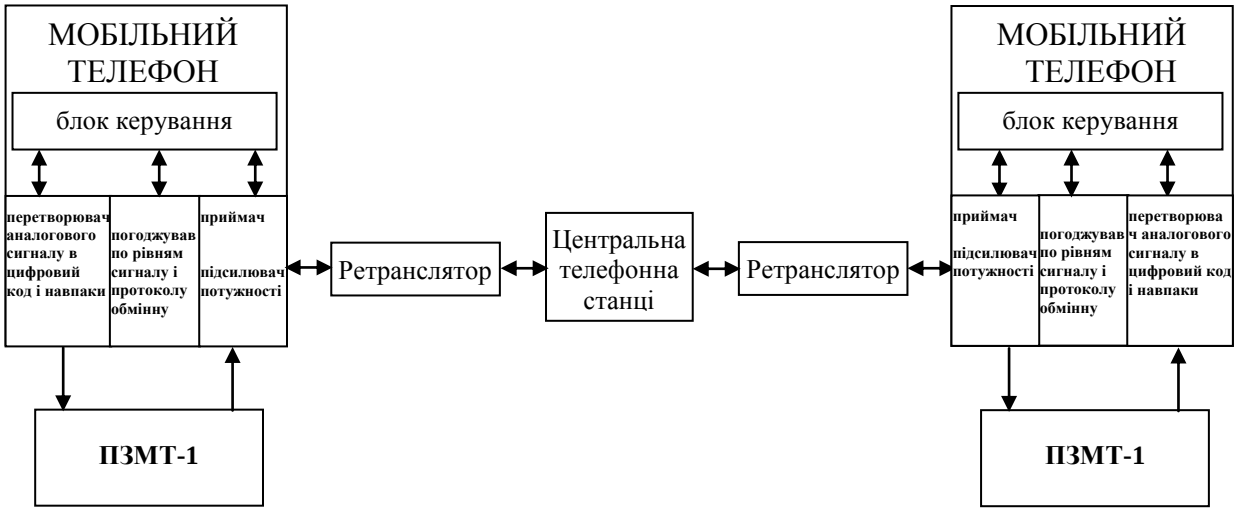

Рис. 9. Структурна схема для захисту інформації в мобільній мережі зв'язку між абонентами

X. Для захисту інформації в цифрових і аналогових лініях при обміні інформацією між факсами (рис. 10).

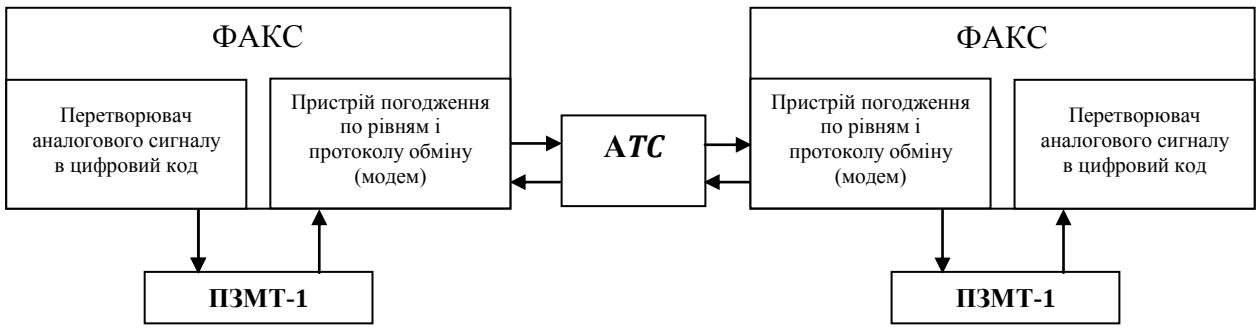

Рис. 10. Структурна схема захисту в мережі телефонного зв'язку між факсами

Використання ВВАК в розглянутих сферах діяльності дозволяють вирішити ряд задач, які на сьогоднішній день зовсім не вирішені або вирішені частково, а саме:

- автоматичний контроль обміну інформацією між абонентами;
- високий ступінь криптографічного захисту інформації, який може автоматично без значних зусиль корегуватися в залежності від заданих вимог;
- висока надійність передачі інформації, так як вона побічно попакетно порівнюється на приймальній і передавальній сторонах за допомогою хеш-функції;
- захист від несанкціонованого доступу хакерів і вірусів;

- автоматизація процесу зміни ключів без використання центру генерації і розподілу ключів.

Висновок

Таким чином, розглянуто основні принципи способу зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем, що призначений для криптографічного перетворення інформації в інформаційній мережі, захисту від атак вірусів і несанкціонованого доступу (хакерів) в комп'ютери через цю мережу. Запропоновано різні варіанти застосування данного спосібу на практиці.

Література

1. Методы и средства защиты информации. В 2-х томах Ленков С.В., Перегудов Д.А., Хорошко В.А., под ред. В.А. Хорошко. – К.: Арий, 2008. – Том 2. Информационная безопасность. – 344 с.

2. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем: Посібник / М. В. Грайворонський, О. М. Новіков. - К.: Видавнича група BHV, 2009. - 608 с.

3. Вишнівський В.В., Жердєв М.К., Лєнков С.В., Пампуха І.В. // Аналіз перспектив розвитку способу застосування способу зашифрування-розшифрування інформації з випадковим, відкритим і адаптивним ключем / Сборник научных трудов Восточноукраинского национального университета им. В. Даля – Луганск, 2008. – С. 42–46.

4. Вишневский В.В., Жердев Н.К., Пампуха И.В., Селюков А.В. Способ самогенерации и распределения индивидуальных случайных ключем // Сборник научных трудов Восточноукраинского национального университета им. В. Даля – Луганск, 2007. – С. 32–37.

5. Ященко В.В. Введение в криптографию. // МЦНМО-ЧеРо, Москва. 2000.- 278 с.

6. Abrams M., Jajodia S., Podell H., et al. Information Security: An integrated Collection of Essays. Los Aiamitos, CA: IEEE Computer Society Press, 1995.- 320 p.

7. Adams C. Constructing Symmetric Ciphers Using the CAST Design. Designs, Codes, and cryptography, 1997.- PP. 33 - 39.

8. Adams C. THE CAST-128 Encryption Algorithm, RFC 2144, May 1997.- PP. 117 – 136.

9. Bellare M. and Rogaway P. Collision-Resistant Hashing: Towards Making UOWHF's Practical // Proceedings, CRYPTO '97,1997, Springer-Verlag.- 460 p.

10. Cheng P., et al. A Security Architecture for the Internet Protocol. // IBM Systems Journal, Number 1, 1998.- 1102 – 1125.

11. Davies C., Ganesan R. BApasswd: A New Proactive Password Checker // Proceeding, 16th National Computer Security Conference, September 1993. – PP. 456 – 458.

Надійшла 29.04.2014 р. Рецензент: д.т.н., проф. Бурячок В.Л.