УДК 004.056.5

Р.С. Одарченко[1] , С.Ю. Лукін[2]

[1] *Національний авіаційний університет, Київ*
[2] *Національна академія державного управління при Президентові України, Київ*

# ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ СТІЛЬНИКОВИХ МЕРЕЖ 4G

*Розглядається модель оцінки економічної ефективності впровадження систем захисту стільникових мереж четвертого покоління (4G). Приведений математичний апарат для оцінки доцільності впровадження систем захисту мереж 4G та наведено алгоритм оцінки їх економічної ефективності.*

***Ключові слова:*** *стільникова мережа; покоління 4G; системи захисту; економічна ефективність; імовірність захисту; зниження прибутковості; вразливості; мережеві атаки.*

## Вступ

Вперше в 2009 році рівень зростання передачі даних перевищив зростання числа абонентів. Якщо бізнес операторів зв'язку ріс лінійно в попередні роки, то у 2009 році ситуація кардинально змінилася. Зростання числа абонентів означає нелінійний ріст передачі даних – люди стали користуватися більше мобільними сервісами. Ця тенденція зберігається і досі, а фахівці прогнозують ще більше зростання саме цього сегменту телекомунікаційного ринку.

В цих умовах для користувачів важливо завжди отримувати високошвидкісний та якісний доступ до мережевих ресурсів, не залежно від місця знаходження. Одним із можливих вирішень цього питання є впровадження стільникових мереж четвертого покоління (4G).

В кінці жовтня 2010 року Міжнародний Телекомунікаційний Союз (International Telecommunications Union) завершив оцінку шести технологій, які претендували на стандарт 4G, з тим щоб привласнити кращим з них позначення IMT-Advanced, і позначити тим самим технології, яким офіційно присвоять міжнародний 4G стандарт.

Такими технологіями названі LTE-Advanced1 (на основі стільникового стандарту LTE) і WirelessMAN-Advanced2 (на основі WiMAX 802.16m), які є тепер офіційними технологіями 4G. З вимогами до цих технологій можна ознайомитися в [7] Таким чином, надалі розглянемо саме ці технології.

В США та Азії вже є кілька операторів, які надають послуги за допомогою мереж LTE [8]. Щодо Європи, то Європейським парламентом було схвалено рішення з приводу впровадження 4G 800 МГц. Таким чином, європейські користувачі зможуть отримати новий стандарт бездротового зв'язку не пізніше 2013 року [8]. Очікується, що 4G 800 МГц стане найбільш ефективним способом передачі інформації, адже забезпечує відмінний прийом даних і доступний для великих відстаней.

Відповідальність за впровадження нового стандарту 4G 800 МГц візьмуть на себе країни-члени ЄС. Саме вони докладуть максимум зусиль для стандартизації мережі, адже це дозволить громадянам ЄС підтримувати зв'язок під час подорожей.

В рамках нового стандарту планується поширення 4G 800MHz на мобільне телебачення, транспортні системи, охорона здоров'я, науково-дослідну та енергетичну індустрію. Це допоможе підвищити конкурентоспроможність Європи у світі.

Кожен користувач будь-якої мережі (в тому числі і 4G) прагне забезпечити конфіденційність даних, що передаються та унеможливити спроби мережевих атак на мобільні пристрої. Конфіденційну інформацію у сфері господарської діяльності можна визначати умовно розділити на три сектори:

- Ділова інформація суб'єкта господарювання;
- Інформація, що стосується безпосередньо фактичних даних суб'єкта господарювання (інформація персонального характеру);
- Ноу-хау – так звані секрети виробництва.

Кожен вид інформації може мати різну цінність як для абонентів мереж, так і для зловмисників. Тому, як і в інших видах мереж, в 4G використовуються певні засоби захисту.

**Постановка проблеми.** Під час впровадження систем захисту інформації виникає питання щодо доцільності їх використання. Необхідно чітко сформулювати перелік критеріїв, за якими можна оцінити доцільність використання систем захисту, та математичний апарат їх оцінки. Він повинен адекватно відображати доцільність впровадження захисних механізмів мереж четвертого покоління.

**Аналіз досліджень та публікацій.** Існує велика кількість літератури, присвяченої проблемам інформаційної безпеки в інформаційно-комунікаційних системах та мережах. Завдання створення, організації та дослідження процесів функціонування, вдосконалення та розвитку СЗІ в тій чи іншій мірі знайшли відображення в працях ряду вітчизняних та зарубіжних вчених, серед яких Е.С. Вент-

цель, В.Ю. Гайкович, В.А. Галатенко, А.Ю. Першин, В.А. Герасименко, В.І. Гарбарчук, Ю.В. Демченко, В.І. Завгородній, В.К. Задирака, А.Г. Карпова, В.В. Лебедєва, В.В. Мельникова, А.Н. Назаров, А.С. Олексюк, А.З. Пєскозуб, А.П. Пятібратова, В.К. Размахнін, С.П. Расторгуєва, Ю.А. Самохіна і багато інших [1-4]. Виокремити можна праці [5-6], які присвячені оцінці економічної ефективності систем захисту в телекомунікаційних системах. Проте питання щодо оцінки економічної ефективності систем захисту стільникових мереж 4G у вітчизняній та зарубіжній літературі зовсім не розглянуте. Взагалі питання щодо систем захисту мереж LTE та WiMAX досить слабко розроблене вітчизняними вченими, а тому представляє великий інтерес і обґрунтовує актуальність теми дослідження.

## Виклад основного матеріалу дослідження

Вихідною передумовою при розробці моделей є припущення, що при порушенні захищеності інформації завдається деякий збиток, а забезпечення захисту інформації пов'язане з витратами [6]. Очікувану вартість захисту можна визначити сумою витрат на захист і збитком від її порушення. Зазначену залежність графічно ілюструє рис. 1 [6]. Очевидно, що оптимальним рішенням є виділення на захист інформації коштів у розмірі $B_{опт}$, оскільки саме при цьому забезпечується мінімізація загальної вартості захисту інформації.

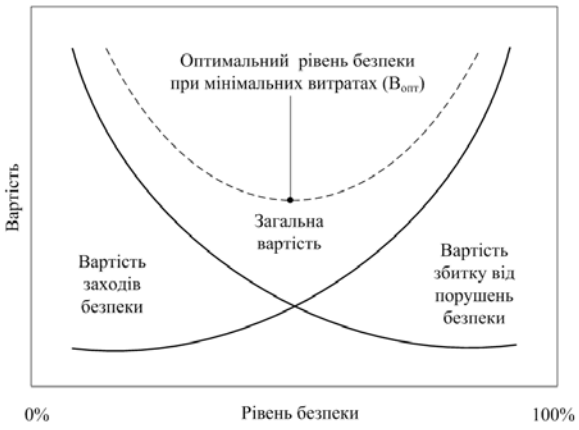


Рис. 1. Вартісні залежності захисту інформації

Існує ряд чинників, які впливають на економічну ефективність використання систем захисту інформації у інформаційно-комунікаційних системах та мережах. До них насамперед слід віднести вартість інформації, що передається чи дохід від її передавання; потенційні збитки; імовірність здійснення атаки тощо. Тому необхідною є розробка моделі, яка зможе поєднати в собі всі ці критерії.

В [5,6] запропоновано модель, яка надає змогу кількісно оцінити доцільність впровадження систем захисту до інформаційно-комунікаційної системи.

Чистий прибуток від передавання інформації орендованим каналом визначається з виразу

$$Q = D - S, \qquad (1)$$

де D – дохід від передавання інформації каналом зв'язку (вартість інформації; S – вартість оренди каналу зв'язку (вартість послуг оператора зв'язку).

Дохід від передавання інформації D із формули (1) ототожнимо із вартістю інформації, що передається. Вартість інформації можна встановити за наступною моделлю [9]:

D=Simple Information Cost = Sale Cost + Possible Damage + Half-received Profit, (2)

де Sale Cost – ринкова вартість інформації, тобто, за яку вартість можливо продати інформацію будь-якому покупцеві; Possible Damage – можливі завдані збитки у грошовому еквіваленті. Його величина залежить від багатьох факторів: міцність зв'язків компанії з клієнтами, якість інформації, структура інформаційної політики компанії і т.д.; Half-received Profit – недоотриманий прибуток.

Величини Possible Damage і Half-received Profit оцінюються виходячи з якості інформації, і її впливу на основну діяльність компанії. В кожному окремому випадку, для кожної окремої фірми чи фізичної особи необхідно користуватися індивідуальними методиками таких оцінок, при цьому не виключено використання галузевих рекомендацій.

Далі необхідно визначити доцільність проведення заходів із захисту інформації. У разі проведення заходів щодо захисту інформації чистий прибуток від передавання інформації знизиться і його можна визначити наступним чином:

$$Q_З = D - S - C_З \cdot \frac{T}{T_0} - C_В \cdot (1 - p_0), \qquad (3)$$

де $C_З$ – вартість організаційно-технічних заходів із захисту інформації; T − час передавання повідомлення; $C_В$ – загальні збитки від втрати інформації; $p_0$ – ймовірність відбиття загрози.

Найбільш загальна оцінка – ймовірність захищеності мережі – знаходиться на підставі наступного співвідношення [10]:

$$p = p' \times p'', \qquad (4)$$

де $p'$ – ймовірність захищеності від факторів, проти яких немає системи захисту, а $p''$ – ймовірність захищеності від факторів, проти яких є захисні засоби. відповідно,

$$p' = \prod_{i=0,n}(1 - p_i) \qquad (5)$$

де n – загальна кількість факторів, проти яких відсутня система захисту, а $p_i$-ймовірність виникнення і-ої загрози.

$$p'' = \prod_{i=0,m}(1 \quad (p_i \cdot \prod_{j=0,k}(1 \quad p_{ij}{}^{C3})), \qquad (6)$$

де m – загальна кількість факторів, проти яких існує система захисту, $p_i$ – ймовірність виникнення і-ої загрози цього типу, k – загальна кількість різних засобів захисту, спрямованих на нейтралізацію і-ої

загрози, $p_{ij}^{сз}$ – ймовірність спрацьовування j-го захисного механізму, об'єктом впливу якого є j-та загроза.

Шляхом коректного проектування бази даних всіх компонентів, необхідних для моделювання, можна без особливих зусиль алгоритмізувати наведені формули.

Далі введемо поняття ймовірного збитку як твори збитку, що наноситься і-ой загрозою j-ому об'єкту і вираженого в відносних одиницях (скажімо від нуля до ста), і ймовірність виникнення і-ої загрози. Це комплексна характеристика, що відображає ступінь уразливості об'єкта в матеріальному аспекті. Якщо в процесі розрахунку ймовірності захищеності для кожного виду загрози знаходити ймовірний від неї збиток, то отримана картина дозволить порівняти деструктивні дії різних загроз і визначити яку реальну небезпеку несе в собі той чи інший фактор і в якій послідовності необхідно нейтралізувати дії яких загроз.

Безліч значень ймовірного збитку можна отримати за формулою [3]:

$$S'_i = S_i \cdot p_i \cdot \prod_{j=0,k}(1 - p_{ij}^{сз}). \qquad (7)$$

Якщо отримане безліч відсортувати за спаданням, то отриманий ряд буде відображати потенційну небезпеку окремо взятої загрози при її впливі на об'єкти локальної мережі. Таким чином, в даній моделі усувається недолік, притаманний багатьом іншим моделям захисту інформації, полягає у відсутності обліку збитків від дії дестабілізуючих факторів.

У даній моделі для оцінки збитку, що наноситься дестабілізуючими факторами, і вартості об'єктів системи застосована єдина відносна ієрархічна шкала. Єдина шкала означає рівність ціни всіх компонент, що мають одну і ту ж порядкову оцінку, так як лінійний порядок дозволяє порівнювати окремі компоненти по цінності відносно один одного. Одна з переваг цією підходу полягає в можливості оцінити сумарну вартість компонент об'єкта захисту або ж загальний наноситься системі матеріальний збиток в грошових одиницях. Так, якщо є дані про збиток або вартості всіх компонент системи, визначені в одиницях відносної шкали, і якщо точно відомо значення вартості в грошових одиницях хоча б однієї з компонент, то не складе ніяких труднощів (заділяний лише апарат пропорційного перерахунку) перерахувати вартість в грошових одиницях всіх інших компонент, І навпаки, якщо апріорно відома загальна вартість інформації (всієї системи в цілому), то відносні оцінки в порядкової шкалою дозволяють обчислити ціни компонент.

Відносну складність в рамках даної моделі може вибувати визначення на етапі підготовки моделі до роботи значень збитку, що наноситься системі різними дестабілізуючими факторами. Одним із способів, які дозволяють спростити цю задачу, є оцінка можливих втрат на основі отриманих раніше вартостей об'єктів захисту, виходячи з прогнозу можливих загроз цим об'єктам. Можливості загроз оцінюються ймовірностями відповідних подій, а втрати підраховуються як сума математичних очікувань втрат для компонент з розподілу можливих загроз.

В [5] було введено поняття коефіцієнта зниження прибутковості захищеної системи передавання інформації $K_З$, який може бути обчислений за формулою (8):

$$К_з=Q_з/Q. \qquad (8)$$

Цей показник дозволяє оцінити наскільки зменшиться прибуток організації після, впровадження заходів щодо захисту інформації. Якщо організація (фізична особа) не бажає впроваджувати заходи щодо захисту власної інформації, необхідно оцінити ймовірне зменшення прибутку в разі перехоплення останньої.

Коефіцієнт зниження прибутковості незахищеної системи $K_Н$ можна представити формулою (9):

$$К_н=Q_н/Q. \qquad (9)$$

Цілком очевидно, що якщо $K_Н > K_З$, то будь-які заходи щодо захисту інформації в системі не мають сенсу. Цю нерівність можна записати таким чином

$$0 < Z = К_Н - К_З. \qquad (10)$$

Отримані результати дозволяють приймати рішення щодо доцільності проведення заходів по захисту інформації в ІКС.

Таким чином, на основі запропонованої моделі можна визначити економічну ефективність впровадження систем захисту інформації до інформаційно-комунікаційних систем та мереж і також до мереж 4G зокрема.

Для проведення оцінки економічної ефективності використання систем захисту інформації в стільникових мережах четвертого покоління необхідно визначити можливу цінність інформації, яка циркулюватиме в мережах такого типу, імовірність виникнення загроз, основні можливі види атак на мережі 4G, вартість організаційно-технічних заходів із захисту інформації від несанкціонованого впливу або пошкодження.

Щодо вартості інформації, яка передаватиметься в мережах WiMAX або LTE, то вона матиме зовсім різну величину для різних груп користувачів. Мережами четвертого покоління зможуть користуватися як прості користувачі, так і, наприклад, власники різних компаній, які зможуть передавати важливу конфіденційну інформацію

Наступним кроком оцінки економічної ефективності систем захисту мереж четвертого покоління є аналіз систем захисту та їх потенційних вразливостей.

До табл. 1 зведено відомості про наявні засоби захисту інформації в мережах LTE [11] та WiMAX [12].

Таблиця 1

Порівняльна характеристика систем захисту мереж четвертого покоління

| Властивості системи | LTE | Wi-MAX |
|---|---|---|
| 1.Ідентифікація мобільних користувачів | Використання ME/USIM; MME; протокол PDCP; ієрархія ключів EPS; алгоритм автентифікації HMSC-SHA-1-96 з розміром ключа 160 та 512 біт; протоколи обміну ключами через мережу Інтернет IKEv1 та IKEv2 | сертифікат X.509, ідентифікуючий абонентську станцію, а також сертифікат X.509, що ідентифікує виробника абонентської станції; 160-бітовий ключ авторизації (authorization key, AK); 4-бітовий ідентифікатор ключа авторизації; 128-бітовий ключ шифрування ключа (Key encryption key, KEK); Ключ HMAC для низхідних (downlink) та висхідних (uplink) повідомлень при обміні ключами TEK; Список data SA, для яких дана абонентська станція авторизована; Privacy and Key Management Protocol; Extensible Authentication Protocol (EAP,розширюваний протокол автентифікації) |
| 2.Шифрування даних | AES-CBC зі 128-бітним ключем; 3DES-CBC з 3x64 бітним ключем | DES, AES |
| 3. Протоколи управління безпекою | Encapsulating security payload; ESP | PKM (privacy and key management protocol) |

Не дивлячись на значну насиченість систем захисту, вони мають і деякі свої вразливості. Пропонується розділити можливі атаки на користувачів мереж 4G на ті, які безпосередньо можливі через вразливість систем захисту, та ті, які можливі в мережі Інтернет.

Отже, до першого класу вразливостей відносять [12]:

- Атаки фізичного рівня, такі як глушіння передачі сигналу, що веде до відмови доступу або лавинний наплив кадрів (flooding), що має метою виснажити батарею станції.
- Самозвані базові станції, що пов'язане з відсутністю сертифіката базової станції. У стандарті проявляється явна несиметричність у питаннях автентифікації. Запропонований розв'язок цієї проблеми - інфраструктура керування ключем у бездротовому середовищі (WKMI, wireless key management infrastructure), заснована на стандарті IEEE 802.11i. У цій інфраструктурі є взаємна автентифікація за допомогою сертифікатів X.509.
- Уразливість, пов'язана з не випадковістю генерації базовою станцією ключів авторизації. Взаємна участь базової й абонентської станції, можливо, розв'язало б цю проблему.
- Можливість повторно використовувати ключів TEK, чий строк життя вже минув. Це пов'язане з дуже малим розміром поля EKS індексу ключа TEK. Тому що найбільший час життя ключа авторизації 70 діб, тобто 100800 хвилин, а найменший час життя ключа TEK 30 хвилин, то необхідне число можливих ідентифікаторів ключа TEK – 3360. А це означає, що число необхідних біт для поля EKS – 12.
- Ще одна проблема зв'язана, як уже згадувалося з небезпекою використання шифрування DES. При досить великому часі життя ключа TEK і інтенсивному обміні повідомленнями можливість злому шифру являє реальну загрозу безпеки. Ця проблема була усунута із уведенням шифрування AES у виправленні до стандарту IEEE 802.16e та LTE Rel. 10. Однак, велика кількість користувачів до цих має встаткування, що підтримує лише старий стандарт IEEE 802.16.

До другого класу вразливостей користувачів мереж 4G слід віднести всі можливі види атак через мережу Internet, адже вона буде одним із основних середовищ спілкування та обміну даними [13]:

- Фрагментація даних.
- Атака Ping flooding.
- Нестандартні протоколи, інкапсульовані в IP.
- Атака smurf.
- Атака DNS spoofing.
- Атака IP spoofing.
- Нав'язування пакетів.
- Sniffing – прослуховування каналу.
- Перехоплення пакетів на маршрутизаторі.
- Нав'язування хосту хибного маршруту за допомогою протоколу ICMP.
- WinNuke.
- Підміна довіреної хоста.
- Fishing.
- Whaling.

Для захисту від деяких типів мережевих атак на мобільні пристрої може застосовуватись антивірусне програмне забезпечення (наприклад, Kaspersky Mobile Security – захист мобільного пристрою від

мережевих атак, шкідливого ПЗ та SMS-спаму тощо) [14].

Величина збитків від втрати інформації в мережах 4G може варіюватися в широкому діапазоні, а імовірності виникнення різних типів атак, їх відбиття можна знаходити за допомогою статистичного аналізу інформації щодо кількості різних типів атак на різні види ресурсів та за допомогою формул (4)-(7).

## Висновки

У роботі набули подальшого розвитку моделі оцінки економічної ефективності впровадження систем захисту в телекомунікаційних системах та мережах. Була розроблена узагальнена модель, яка дозволяє кількісно визначити доцільність впровадження систем захисту інформації з економічної точки зору. До складу моделі входять наступні показники: вартість інформації, імовірність відбиття загрози, можливі збитки від втрати інформації тощо. На основі запропонованої моделі був розроблений алгоритм визначення економічної ефективності впровадження систем захисту в мережах четвертого покоління. Не вдалося навести кількісні розрахунки через малу вивченість даного питання та малу кількість статистичної інформації. Тому в подальших дослідженнях планується провести більш повний аналіз статистичних даних та на їх основі точно визначити доцільність використання різних захисних механізмів мереж 4G для різних груп користувачів.

## Список літератури

*1. Киселев В.Д., Есиков О.В., Кислицын А.С. «Современные проблемы защиты в системах ее передачи и обработки» / Под ред. проф. Е.М. Сухарева. – М.:«Солид», 2000. – С. 200.*

*2. Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. – Изд-во: ДМК, 2002. – 134 с.*

*3. Гарбарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации / Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т. – К.; Луцк; Люблин, 2003. – 658 с.*

*4. Задірака В.К., Бабич М.Д., Березовський А.І. та ін. Т-ефективні алгоритми наближеного розв'язування задач обчислювальної математики. – К., 2003. – 216 с.*

*5. Конахович Г.Ф., Голубничий О.Г., Пузиренко О.Ю. Оцінка ефективності систем захисту інформації в телекомунікаційних системах // Проблеми інформатизації та управління: Зб. наук. праць: Випуск 3 (21). − К.:НАУ, 2007. − С. 75 − 83.*

*6. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП ІНТЕРСЕРВІС», 2009. -716 с.*

*7. Официальные 4G - WiMAX и LTE // http://nag.ru/news/newsline/19789/oficialnye-4g---wimax-i-lte.html.*

*8. 4G будет доступен в 2013 // http://ava.ua/article/3183/.*

*9. Оценка стоимости информации // http://www.myinterest.ru/services/?SID=573.*

*10. А.П. Дмитренко, Г.А. Сирченко, В.А. Хорошко Статистическое моделирование для оценки защищенности локальной сети «Вісник ДУІКТ» Т.8, №1, 2010 С. 62-69.*

*11. LTE and the Evolution to 4G Wireless. Design and Measurement Challenges, 2010.*

*12. Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в мережах Wi-MAX та методів їх усунення // Защита информации: Зб. науч. трудов: Випуск 18. − К.:НАУ, 2011. − С . 39 − 44.*

*13. Офіційний сайт Лабораторії Касперського // www.kaspersky.ru.*

*14. Удалённые сетевые атаки // http://ru.wikipedia.org/.*

*Надійшла до редколегії 2.04.2012*

**Рецензент:** д-р техн. наук, проф. Г.Ф. Конахович, Національний авіаційний університет, Київ

### ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ СИСТЕМ ЗАЩИТЫ СОТОВЫХ СЕТЕЙ 4G

Р.С. Одарченко, С.Ю. Лукин

*Рассматривается модель оценки экономической эффективности внедрения систем защиты сотовых сетей четвертого поколения (4G). Приведен математический аппарат для оценки целесообразности внедрения систем защиты сетей 4G и приведен алгоритм оценки их экономической эффективности.*

***Ключевые слова:*** *сотовая сеть; поколение 4G; системы защиты; экономическая эффективность; вероятность защиты; снижение прибыльности; впечатлительности; сетевые атаки.*

### THE ECONOMIC EFFICIENCY OF SECURITY SYSTEMS IN 4G CELLULAR NETWORKS

R.S. Odarchenko, S.Y. Lukin

*A model evaluation of the economic effectiveness of the protection system of fourth generation (4G) cellular networks is considered. The mathematical apparatus to assessfeasibility of introducing the 4G network security and an algorithm for evaluation of their economic efficiency are given.*

***Keywords:*** *cellular network; generation of 4G; systems of defence; economic efficiency; probability of defence; decline of profitability; to impressionability; network attacks.*