УДК 338.47:65.012.8

В. М. ГРАНАТУРОВ, Л. В. МИХАЙЛОВА
Одеська національна академія зв'язку ім. О.С. Попова

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ВИТРАТ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙ

Запропоновано підхід до оцінки витрат на забезпечення інформаційної безпеки, який дозволяє побудувати залежності цих витрат від рівня захисту, що є першим кроком на шляху до вирішення проблеми вибору оптимального з техніко-економічної точки зору варіанту системи захисту.

Ключові слова: автоматизовані системи, інформаційна безпека, рівень захисту, профіль захисту, витрати, ефективність.

V. M. GRANATUROV, L. V. MICHAILOVA
A. S. Popov Odessa National Academy of Telecommunications, Odessa, Ukraine

METHODICAL APPROACHE TO ESTIMATING THE COST OF INFORMATION SECURITY OF TELECOMMUNICATIONS

The purpose of the article is a definition and a substantiation of the methodological approach to the evaluation of the cost of information security depending on the level of protection. Decision made on the basis of the construction and use of a matrix model of organization of information security based on recommended by national and international standards, levels of protection, as well as functional components of safety and security profiles, through which the relevant security level requirements. The proposed methodical approach is the first step towards a solution to the problem of choosing the optimal technical-economic point of view, the system of protection.

Keywords: automated systems, information security, security level, security profile, costs, efficiency.

Вступ. Підвищення ролі та значення інформації в житті сучасного суспільства супроводжується бурхливим, навіть безпрецедентним, розвитком телекомунікаційних техніки і технологій. Одночасно, підвищується актуальність проблем захисту інформації, оскільки інциденти у сфері інформаційної безпеки телекомунікацій можуть приводити не тільки до втрати конфіденціальної інформації, що само по собі є вкрай небезпечним для її власників, а також до зривів виробничих процесів у різних сферах діяльності та виникнення надзвичайних ситуацій різного масштабу зі значними негативними наслідками. При цьому, поряд із розвитком інформаційно-комунікаційних технологій (ІКТ), удосконалюються методи та методики атак на ці технології, збільшується розмір шкоди у разі коли ці атаки вдаються. Тому в останній час проблемі попередження та усунення загроз інформаційній безпеці телекомунікацій, удосконаленню системи її підтримки приділяється підвищена увага. Підтвердженням такої уваги є динамічне зростання сектору інформаційної безпеки. Так, наприклад, світовий ринок інформаційної безпеки у 2012 році збільшився на 7,9% (до $19,135 млрд) у зрівнянні з 2011 роком [1], а прибуток компаній виробників збільшився на 9,7% (до $1,9 млрд) [2].

Слід відзначити, що існуючі технічні рішення в сфері захисту інформації дають можливість забезпечити високий рівень інформаційної безпеки. Проте, їх впровадження та обслуговування потребує значних коштів. Як показують дослідження, у крупних організаціях витрати коштів на захист інформації досягають 20–30% усього бюджету компанії на ІТ [3]. В цих умовах актуальною стає проблема аналізу ефективності та доцільності вкладення коштів у реалізацію проектів щодо забезпечення інформаційної безпеки.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Зростання актуальності проблеми інформаційної безпеки, та як наслідок, обсягів впровадження відповідних засобів захисту, а також зростання обсягів витрат на ці цілі викликає інтерес науковців та практичних робітників до проблеми визначення та обґрунтування ефективності цих витрат, вибору оптимального з техніко-економічної точки зору варіанту системи захисту. Як правило, у літературних джерелах з цієї проблеми використовуються загальнометодичні підходи оцінки економічної оцінки ефективності різноманітних проектів, у відповідності до яких оцінка ефективності заходів щодо забезпечення інформаційної безпеки передбачає зіставлення витрат на ці заходи з ефектом від їх реалізації [3–10]. При цьому, більшість дослідників стверджують, що витрати на засоби захисту інформації мають детермінований характер, оскільки вони вже матеріалізовані у конкретні міри, способи та засоби захисту, а шкода, яку можуть нанести несанкціоновані дії, – є випадковою величиною. Такий якісний аналіз дозволяє науковцям висувати припущення про те, що існує область економічно оптимальних засобів захисту інформації, які забезпечують віддачу вкладених коштів [3, 10]. Слід відзначити, що ці припущення супроводжуються ілюстраціями, які, на думку авторів, відображують взаємозв'язок між витратами на інформаційну безпеку, рівнем захищеності та економічним ефектом, що досягається. Проте, ці припущення не дозволяють використовувати існуючі залежності для вибору оптимального варіанту системи інформаційної безпеки для

практичних цілей, оскільки на усіх ілюстраціях градації рівня захищеності відображені у якісних характеристиках: «низький – середній – високий», «захист відсутній (великий ризик) – досконалий захист (ризик відсутній», «0 (захист відсутній) – 1 (повний захист)» і т.п. Аналіз наукової літератури з цієї проблеми свідчить також про те, що сьогодні наголос робиться на структурі витрат на інформаційну безпеку та методи їх визначення без урахування залежності цих витрат від рівня безпеки, який досягається. Такий стан не дозволяє визначати реальний оптимальний рівень інформаційної безпеки, який можна застосовувати у практичній діяльності, а також ускладнює розрахунки ключових економічних показників, пов'язаних із реалізацією заходів щодо забезпечення інформаційної безпеки.

Мета статті. Метою статті є визначення та обґрунтування методичного підходу до оцінки витрат на забезпечення інформаційної безпеки телекомунікацій в залежності від конкретного рівня захисту, який може бути підґрунтям для подальших досліджень стосовно вибору оптимального з техніко-економічної точки зору варіанту системи інформаційної безпеки.

Виклад основного матеріалу дослідження. Як показує аналіз, за останні 10-15 років методологія розрахунку витрат на різні види інформаційних технологій взагалі, та інформаційну безпеку зокрема, в цілому достатньою мірою сформувалася та активно використовується на практиці. Найбільш часто для цієї мети використовується розроблена компанією "Gartner Group» методика сукупної вартості володіння (англ. Total Cost of Ownership, TCO) [7]. Слід відзначити, що методика передбачає оцінку витрат за двома групами – прямими та посередніми витратами на створення, експлуатацію та супроводження системи інформаційної безпеки. Якщо абстрагуватися від різних ступенів деталізації складу прямих витрат, які зустрічаються у літературних джерелах з проблеми, то можна констатувати, що до прямих витрат відносять вартість: проектних робіт; апаратно-програмних засобів, їх монтажу та наладки; експлуатації системи захисту; навчання персоналу; аудиту системи безпеки; періодичної модернізації системи безпеки. Посередні витрати (інколи їх називають прихованими) характеризують витрати, які виникають у результаті необхідності ліквідації негативних наслідків реалізації загроз інформаційній безпеці, та які мають імовірнісний характер, на нашу думку, слід розглядати у взаємозв'язку із оцінкою ефекту від впровадження системи інформаційної безпеки та враховувати в цьому ефекті. Тому, в подальшому, зосередимо увагу на питаннях визначення саме прямих витрат на інформаційну безпеку залежно від рівня захисту.

Виходячи з мети дослідження, яка полягає у визначенні та обґрунтуванні методичного підходу до оцінки витрат на забезпечення інформаційної безпеки телекомунікацій залежно від конкретного рівня захисту, слід зробити таке попереднє зауваження. Більшість витрат на створення та функціонування системи інформаційної безпеки, які віднесено до прямих, є умовно постійними у відношенні до рівня захисту. Виключенням є витрати на апаратно-програмні засоби, їх монтаж та наладку, та, частково, на експлуатацію системи захисту (стосовно амортизаційних відрахувань), які суттєво залежать від рівня захисту. Це положення, а також використання вимог та рекомендацій існуючих нормативно-правових документів, які встановлюють можливі рівні захисту інформації, покладено в основу вирішення задекларованої мети дослідження.

Як відомо, законодавством України [11] сформульовано нормативно-методичну базу для вибору та реалізації вимог із захисту інформації в автоматизованій системі (АС), а також рівнів, з якими має забезпечуватися захист від існуючих загроз. Залежно від конфігурації апаратних засобів, їх фізичного розміщення, кількості категорій оброблюваної інформації, кількості користувачів і категорії користувачів усі АС поділено на 3 класи. За критеріями необхідності забезпечення конфіденційності (К), цілісності (Ц) та доступності (Д) інформації в межах кожного класу виділяються підкласи, сполучення яких зумовлює наявність семи підкласів (Н, Ц, Д, КЦ, КД, ЦД, КЦД). Кожному підкласу поставлено у відповідність множину стандартних функціональних профілів захищеності (ФПЗ) – упорядкованого переліку рівнів функціональних послуг безпеки, кожна з яких дозволяє протистояти певній множині загроз, та може включати декілька рівнів. Зростання рівня захищеності може досягатися як посиленням певних послуг, тобто включення у профіль більш високого рівня послуги, так і включенням в профіль нових послуг. Найбільша кількість рівнів, що розглядаються, залежить від підкласу. Так, наприклад, у відповідності до сукупності характеристик телекомунікацій їх можна віднести до 3 класу. Тоді, у відповідності до [11], опис функціональних профілів, що входять у состав класу 3 з підвищеними вимогами (рівня 5) до забезпечення конфіденційності, цілісності та доступності (3.КЦД.5) включає 24 елементи (ФЗП) – КД-4, ЦД-4 тощо. Одночасно, для цього класу з вимогами рівня 1 (3.КЦД.1) включено 15 елементів – КД-2, ЦД-1 тощо. Окрім вимог конфіденційності, цілісності та доступності до усіх профілів включено вимоги спостереження та гарантії, реалізація яких є необхідною умовою забезпечення інших вимог.

Усього визначеним вище нормативним документом передбачено використання 84 підкласів АС, для формування безпеки яких застосовуються 73 стандартних ФЗП. Склад критеріїв, а також відповідних їм ФЗП, які використовуються для формування захисту певного рівня, наведено на рис.1.

Викладені основні положення щодо вибору та реалізації вимог із захисту інформації в АС можуть бути використані для оцінки витрат на забезпечення інформаційної безпеки в залежності від рівня захисту. Ядром такого підходу є побудова моделі процесу організації інформаційної безпеки. Модель зображується у виді матриці, у рядках якої (i) міститься перелік підкласів (рівнів захисту) АС, а у стовбцях (j) – перелік

усіх стандартних ФЗП і вартість їх фізичної реалізації. Тобто розмір матриці складає 84?73. На перехрещенні рядків та стовбців матриці виділяються лише ті ФЗП, які використовуються для формування безпеки даного підкласу.

Визначення витрат на забезпечення безпеки даного підкласу ($З$) здійснюється шляхом сумування вартості реалізації цих ФЗП з наступного виразу:

$$З = \sum_{j \in I} ФЗП_j, \quad i = 1 \dots n.$$

До отриманих витрат, що характеризують витрати на апаратно-програмні засоби додаються умовно-постійні витрати.

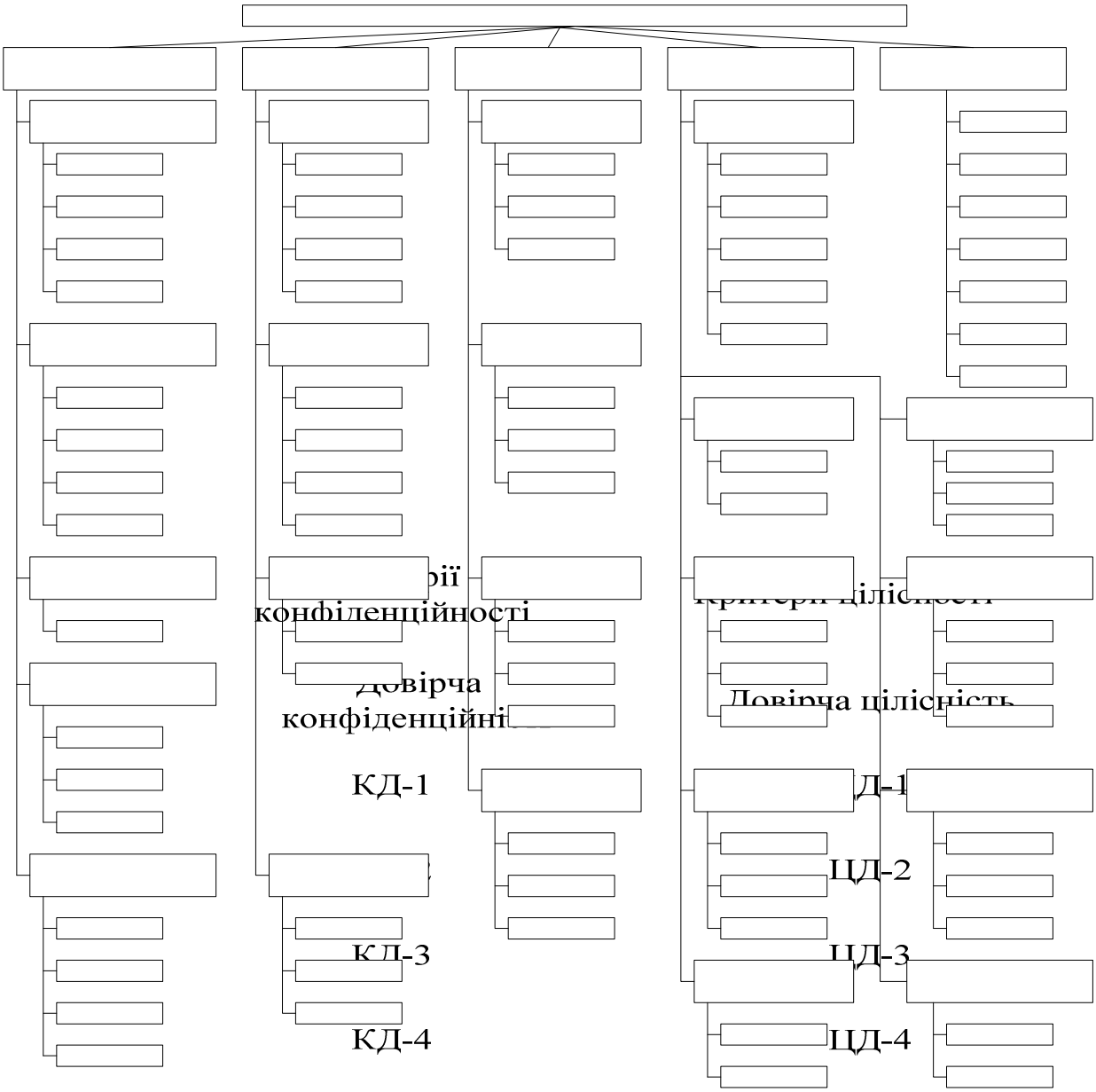

Рис. 1. Склад критеріїв, а також відповідних їм ФЗП, які використовуються для формування інформаційної безпеки певного рівня

Для побудови залежності витрат від рівня захисту використовуються тільки ті підкласи, з розташованих у рядках матриці, що належать до класу АС, безпека яких аналізується. Так, наприклад, у відповідності до [11], для АС 3-го класу максимальна кількість підкласів (рівнів захищеності) дорівнює 34 (З.К.1, …, З.К.6; З.Ц.1, …, З.Ц.5; З.Д.1, …, З.Д.4; З.КЦ.1, …, З.КЦ.6; З.КД.1, …, З.КД.4; З.ЦД.1, …, З.ЦД.4; З.КЦД.1, …, З.КЦД.5). Де, наприклад, З.К.6 – функціональний профіль номер чотири, який відображує вимоги до АС класу 3, основною вимогою якого щодо захисту інформації є забезпечення конфіденційності. Тобто, кількість точок на шкалі рівень захисту та відповідних ним витрат, дорівнюватиме 34. У разі якщо

аналізуються тільки витрати та рівні, які характеризують вимоги до забезпечення конфіденційності, цілісності та доступності (КЦД), таких точок на шкалі рівня захисту буде 5.

Як відзначалося, вирішення задекларованої мети дослідження спирається на використання вимог та рекомендацій одного з існуючих вітчизняних нормативно документів, який встановлює можливі рівні захисту інформації [11]. Проте сьогодні існують й інші НД, які присвячено критеріям оцінки безпеки інформаційних технологій. Найбільш близьким до документу, який нами використано, є міжнародний стандарт ИСО/МЕК [12], в якому також розглядаються три види порушення безпеки (конфіденційність, цілісність та доступність), а також функціональні компоненти безпеки та профілі захисту, за допомогою яких виконуються відповідні вимоги до рівня безпеки. Тобто, запропонований методичний підхід може бути використаний також для визначення залежності витрат від рівня захисту при застосуванні й цього стандарту. Наш вибір на користь документу, який використаний, обґрунтований лише тим, що в ньому детальніше розглянуто питання формування можливих варіантів захисту та їх реалізації за допомогою ФЗП, що спрощує розуміння сутності запропонованого методичного підходу.

Висновки. Запропонований підхід дозволяє побудувати залежності витрат на забезпечення інформаційної безпеки від рівня захисту. Побудовані таким чином залежності є першим кроком на шляху вирішення проблеми вибору оптимального з техніко-економічної точки зору варіанту системи захисту. Подальші дослідження в цьому напрямку повинні передбачати визначення та обґрунтування залежності отриманого ефекту використання системи інформаційної безпеки від рівня захисту, який вона забезпечує. Враховуючи також значний розмір матриці та, як наслідок, значну трудомісткість процесу розрахунків витрат на забезпечення інформаційної безпеки, для полегшення його практичного застосування доцільно розробити спеціальне програмне забезпечення для автоматизації обчислень.

Література

1. Gartner опубликовало результаты исследования мирового рынка информационной безопасности [Електронний ресурс]. – Режим доступу : http://www.securitylab.ru/news/440842.php. – (Дата звернення 17.08.2014).

2. Информационная безопасность (мировой рынок) [Електронний ресурс]. – Режим доступу : http://classtel.ru/информационная-безопасность-мирово/. – (Дата звернення 17.08.2014).

3. Петренко С. Информационная безопасность: экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info Online. – 2003. – № 10 [Електронний ресурс]. – Режим доступу : http://citforum.ru/security/articles/sec/ – (Дата звернення 29.07.2014).

4. Петренко С. Оценка затрат компании на Информационную безопасность [Електронний ресурс]. – Режим доступу : http://citforum.ru/security/articles/ocenka_zatrat/ – (Дата звернення 29.07.2014).

5. Булгаков Я.С. Подходы для определения затрат на защиту информации / Я.С. Булгаков, Т.А. Ужахов [Електронний ресурс]. – Режим доступу : http://stavkombez.ru/conf/2011/04/14/primenenie-elektronnoj-cifrovoj-podpisi/ – (Дата звернення 20.07.2014).

6. Домарев В.В. Моделирование процессов создания и оценки эффективности систем защиты информации / В.В. Домарев [Електронний ресурс]. – Режим доступу : http://www.iso27000.ru/chitalnyi-zai/upravlenie-informacionnoi-bezopasnostyu/modelirovanie-processov-sozdaniya-i-ocenki-effektivnosti-sistem-zaschity-informacii. – (Дата звернення 20.07.2014).

7. Witty R., Dubiel J., Girard J., Graff J., Hallawell A., Hildreth B., MacDonald N., Malik W., Pescatore J., Reynolds M., Russell K., Weintraub A., Wheatman V. The Price of Information Security. Gartner Research, Strategic Analysis Report, K-11-6534. Gartner Research, Strategic Analysis Report, K-11-6534, June 2001.

8. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем / Н.А. Маслова // «Искусственный интеллект» — 2008. —№ 4. — С. 253 — 264.

9. Солнцев М. В. Методы оценки экономической эффективности комплексных систем защиты информации телекоммуникационных систем передачи и обработки данных : автореферат диссертации на соискание ученой степени кандидата экономических наук : спец. 08.00.13 «Экономико-математические методы» / Солнцев М. В. – Санкт-Петербург : ГУЭИФ, 2000. – 18 с.

10. Тардаскина Т. М. Організаційно-економічні складові інформаційної безпеки телекомунікаційних мереж загального користування : автореферат дис. на здобуття наукового ступеня кандидата економічних наук : спец. 08.00.04 «економіка та управління підприємствами (за видами економічної діяльності)» / Тардаскина Т. М. – Одеса : ОНАЗ ім. О.С. Попова, 2008. – 20 с.

11. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – К. : ДСТСЗІ СБ України. – 16 с.

12. ISO/IEC 15408:2005, Information technology — Security techniques — Evaluation criteria for IT security.

References

1. Gartner opublskovalo rezultaty issledovaniya mirovogo rynka informatsionnoy bezopasnosti, available at: http://www.securitylab.ru/news/440842.php [in Russian].

2. Informatsionnaya bezopasnost (mirovoy rynok), available at: http://classtel.ru/информационная-безопасность-мирово/ [in Russian].

3. Petrenko S., Symonov S., Kyslov R. Informatsionnaia bezopasnost: ekonomicheskie aspekty, 2003/ Jet Info Online, 10, available at: http://citforum.ru/security/articles/sec/ [in Russian].

4. Petrenko S. Otsenka zatrat kompanii na informatsionnuiu bezopasnost, available at: http://citforum.ru/security/articles/ocenka_zatrat/ [in Russian].

5. Bulhakov Ya.S., Uzhakhov T.A Podkhody dlia opredeleniia zatrat na zashchitu informatsii, available at: http://stavkombez.ru/conf/2011/04/14/primenenie-elektronnoj-cifrovoj-podpisi/ [in Russian].

6. Domarev V.V. Modelirovanie protsessov sozdaniia i otsenki effektivnosti system zashchity informatsii, available at: http://www.iso27000.ru/chitalnyi-zai/upravlenie-informacionnoi-bezopasnostyu/modelirovanie-processov-sozdaniya-i-ocenki-effektivnosti-sistem-zaschity-informacii [in Russian].

7. R. Witty , J. Dubiel , J. Girard , J. Graff , A. Hallawell , B. Hildreth , N. MacDonald , W. Malik , J. Pescatore , M. Reynolds , K. Russell , A. Weintraub , V. Wheatman. -- The Price of Information Security. Gartner Research, Strategic Analysis Report, K-11-6534 -- Gartner Research, Strategic Analysis Report, K-11-6534, June 2001.

8. Maslova N.A. Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem, 2008 Iskusstvennyu intellekt.4, pp. 253 — 264 [in Russian].

9. Solntsev M. V. Metody otsenki ekonomicheskoy effektivnosti kompleksnykh sistem zashchity informatsii telekommunikatsionnykh sistem peredachi i obrabotki dannykh: Extended abstract of candidate's thesis spets. 08.00.13 «Ekonomiko-matematicheskie metody». – Sankt-Peterburg: HUEYF, 2000, 18 [in Russian].

10. Tardaskina T. M. Orhanizatsiino-ekonomichni skladovi informatsiinoi bezpeky telekomunikatsiinykh merezh zahalnoho korystuvannia: Extended abstract of candidate's thesis spec. 08.00.04 «Ekonomika ta upravlinnia pidpryiemstvamy (za vydamy ekonomichnoi diialnosti)». Odesa, ONAZ im. O.S. Popova, 2008, 20 [in Ukraine].

11. ND TZI 2.5-005-99. Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhychenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu. DSTSZY SB Ukrainy. 16 [in Ukraine].

12. ISO/IEC 15408:2005, Information technology — Security techniques — Evaluation criteria for IT security.

Надійшла 11.09.2014; рецензент: д. е. н. Орлов В. М.