Порівняно з методом на основі одновимірного ДКП [5] запропонований метод забезпечує менше спотворення при вбудовуванні ЦВЗ. При цьому запропонований метод забезпечує вбудовування у 8 разів меншої кількості бітів ЦВЗ. Цей показник можна збільшити для запропонованого методу, якщо у матрицю 8x8 елементів вбудовувати не один, а декілька бітів. Проте, це може призвести до спотворення векторного зображення. Кількість бітів ЦВЗ на одну матрицю можна збільшити, але якщо рівень спотворення при цьому буде допустимий згідно з поставленими вимогами до якості векторного зображення.

Проведений аналіз показує, що запропонований метод забезпечує збереження високого рівня якості зображення після вбудовування ЦВЗ. При цьому метод, як і більшість існуючих методів вбудовування ЦВЗ у векторні зображення, є достатньо стійким до поширених стеганографічних атак.

V Висновки

Запропоновано стеганографічний метод вбудовування ЦВЗ у векторні зображення для відкритих стеганосистем. Особливістю методу є використання двовимірного ДКП для матриць розміром 8x8 та зміна в них високочастотних коефіцієнтів, яка здійснюється залежно від біту ЦВЗ та двох додаткових ВЧ-коефіцієнтів на середньоарифметичне значення цих коефіцієнтів, збільшене або зменшене на величину *P*, яка забезпечує чітку ідентифікацію бітів при витягуванні ЦВЗ.

Проведений аналіз якості запропонованого методу з точки зору впливу ЦВЗ на якість зображення показав, що запропоновані використання двовимірного ДКП та зміни його коефіцієнтів дозволяють вирішити проблему погіршення якості зображення внаслідок вбудовування ЦВЗ. Проведено порівняльний аналіз використання двовимірного та одновимірного ДКП для захисту векторних зображень у відкритих стеганосистемах на прикладі частини векторної карти, який показав, що використання двовимірного ДКП порівняно з одновимірним дозволяє зменшити негативний вплив ЦВЗ на якість зображення приблизно у 8 разів.

Аналіз стійкості запропонованого методу проводився з точки зору стійкості векторного зображення до активних атак, які спрямовані на знищення чи підміну ЦВЗ. Проведений аналіз показав, що запропонований метод, як і більшість існуючих методів, є достатньо стійким до найпоширеніших видів стеганографічних атак.

Література: ***1.*** *В. О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.* ***2.*** *Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс», 2006. – 288с.* ***3.*** *Liangbin Zheng, Yulu Jia, Qun Wang. Research on Vector Map Digital Watermarking Technology // First International Workshop on Education Technology and Computer Science – 2009. p. 303-307.* ***4.*** *V. Solachidis, N. Nikolaidis and I. Pitas. Fourier descriptors watermarking of vector graphics images // International Conference On Image Processing. – 2000,№3, p.9-12.* ***5.*** *M. Voigt, B. Yang and C. Busch. Reversible watermarking of 2D vector data // ACM Mutimedia and Security Workshop. –2004, p. 160-165.* ***6.*** *Яремчик Ю. Є., Карпінець В. В. Використання цифрових водяних знаків для захисту авторського права в зображеннях // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні - 2006. - №2(13) – с. 63-69.*

УДК 681.3

КРИТЕРІЇ І МЕТОДОЛОГІЯ ОЦІНКИ ЕФЕКТИВНОСТІ ОРГАНИЗАЦІЇ І ПОБУДОВИ АРХИТЕКТУРИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Вячеслав Шорошев
ДНДІ МВС України

Анотація: **Надаються нові вітчизняні критерії кількісної і багатофакторної оцінки ефективності архітектури захищених комп'ютерних систем з використанням концептуальних підходів щодо пріоритетності захисту комп'ютерної інформації від загроз несанкціонованого доступу аналогічно критерію TCSEC (США) і Європейських критеріїв ITSEC (США, Канада, Англія, Німеччина, Франція, Нідерланди). Розглядаються теоретичні і практичні аспекти методології оцінки ефективності організації і побудови архітектури захищених комп'ютерних систем.**

Annotation: **The new domestic criteria of quantitative and multivariable estimation of effektyvnosty architecture of the protected computers systems are expounded with the use of conceptual approaches about priority of zschyty computer information from the threats of unauthorized division in obedience to the criteria of TCSEC (THE USA) and European criteria of ITSEC (The USA, Canada, England,**

Germany, France, Netherlands). The theoretical and practical aspects of mtodologyy estimation of efficiency of organization and construction of architecture of the protected computers systems are examined.

Ключові слова: **Організація архітектури, побудова архітектури, механізм рейтингових оцінок, рейтинг профілю, модель архітектури, несанкціонований доступ, критерій рейтинг профілю-ризик безпеки-гарантія безпеки.**

I ВСТУП

За результатами проведених багаторічних досліджень пропонуються концептуальні шляхи рішення проблеми організації і побудови архітектури захищених інформаційно-телекомунікаційних систем (в перших нормативних документах НД ТЗІ використався термін комп'ютерні системи) з нормуванням їх інформаційної безпеки за сандартизованими рівнями, а також за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Надалі буде використатись і термін захищені комп'ютерні системи (ЗКС).

Одним із основних методологічних шляхів пошуку рішення проблеми організації та побудови архітектури ЗКС у даній статті вважається використання методів концептуальної евристики. Вони передбачають визначення множини таких релевантних шляхів рішення проблеми, серед яких з достатньою імовірністю є і результативний шлях.

При аналізі початкової ситуації людина-експерт не просто збирає інформацію, необхідну для рішення задачі, а будує багатофакторну структуровану концептуальну модель проблемної ситуації, виокремлює найважливіші елементи, відносини між ними і формує їх основні узагальнені елементи та відносини між ними. Такі узагальнені елементи і відносини між ними в концептуальних евристиках визначаються як *концепти* [1]. На їх основі надається можливість досягнення обраної мети при традиційному об'єкті дослідження ЗКС, але при нових концептуальних напрямках предмета дослідження як в теоретичному, так і в практичному аспектах.

При організації і побудові архітектури ЗКС має враховуватися, насамперед, пріоритетність вимог чинних вітчизняних нормативно-правових документів, їх треба дотримуватись та надавати їм подальший розвиток щодо шляхів їх практичної реалізації, в тому числі з урахуванням міжнародного досвіду та за результатами досліджень. Це і покладено в основу статті [2].

II Основна частина

Розроблена перспективна концептуальна модель політики побудови архітектури захищеної комп'ютерної системи з нормуванням її інформаційної безпеки стандартизованими рівнями, а також за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Проблема формування політики безпеки та експертна оцінка її ефективності за чотирма обраними факторами сама по собі складна як в програмно-математичному, так і в практичному аспектах. Чотирьохфакторний функціонал сам по собі потребує використання чутливих математичних методів до змін факторів. В запропонованій моделі зміни цих факторів формалізуються їх стандартизованими рівнями (Layer).

Так, захищеність інформації регламентується двома рівнями – необхідний та максимальний. Види інформаційної діяльності регламентуються допустимим, заданим та мінімальним рівнями обмежень. Рівень захисту інформації регламентується необхідним і максимальним рівнями. Витрати на захищеність інформації регламентуються мінімальним, допустимим та необхідним рівнями. Це стандартизовані ДСТУ рівні [3 – 5].

Завдання дослідження полягає в тому, щоб визначити і запропонувати такі концептуальні, найбільш ефективні і результативні шляхи *(концепт-правила)* рішення проблеми підвищення ефективності за рахунок формування відповідної (адаптивної) політики побудови та організації архітектури ЗКС.

У розробленній моделі підвищення ефективності організації та побудови архітектури захищених комп'ютерних систем *вперше* в теорії ТЗІ пропонується визначати та реалізовувати в *політиці безпеки архітектури* наступні десять найбільш результативних концептуальних чинників (*концепт-правил*) аналогічно методолгії міжнародного стандарту ISO 17799 щодо десяти принципів управління інформаційною безпекою та десяти ключових засобів її аудиту:

- перше концепт-правило щодо пріоритетності *профілю* захищеності інформації ЗКС, який має бути відповідним (адаптивним), насамперед, підкласу ЗКС, в якому визначаються і надаються підвищені вимоги до захисту від порушень політики конфіденційнсті К, цілісності Ц і доступності Д інформації та який повинен ефективно протидіяти загрозам їх порушення за обраним рівнем безпеки (Layer) залежно від обраного підкласу К, Ц, Д, КЦ, КД, КЦД;

- друге концепт-правило щодо пріоритетності *підкласів* кожного класу захищеної комп'ютерної системи,

які реалізуються в архітектурі захищеної комп'ютерної системи шляхом використання адаптивних загрозам функціональних профілів з технолгією Т обробки інформації для надання відповідних загрозам послуг безпеки (АФП-Т);

- третьє концепт-правило щодо *профільної* послуги безпеки (ПБ-ПР), під якою у даному дослідженні визначається функціональна послуга безпеки (ФПБ) тільки її *одного* певного рівня, яка комплексно з іншими ФПБ, обраними за їх рейтингом, використується у складі профілю з *повним* або *поточним* (неповним) набором для цього рівня так званих *елементарних* функціональних послуг безпеки (ПБ-ЕФ), множина яких регламентована в таблично-текстовому форматі в *критеріях* захищеності інформації від несанкціонованого доступу за вимогами нормативного документу НД ТЗІ 2.5-004-99 [6], а також особливо з урахуванням нових вагомих внесків в теорію ТЗІ щодо методичних вказівок нормативних документів НД ТЗІ 2.7-009-09 та НД ТЗІ 2.7-010-09 [7, 8];

- четверте концепт-правило щодо *вагомості* профільної послуги безпеки для підвищення ефективності політики організації і побудови *архітектури* з обов'язковим визначенням для неї необхідних умов (ПБ-НУ, тобто необхідних додаткових послуг безпеки), без виконання яких неможливе комплексне надання послуг безпеки у *складі* профілю з використанням обраного *рівня* профільної послуги безпеки;

- п'яте концепт-правило щодо *вагомості* обраного профілю для *протидії загрозам* порушення конфіденційнсті К, цілісності Ц і доступності Д, а також спостереженості Н інформації, яка кількісно обчислюється його *повним* або *поточним* (неповним) рейтингом для кожного підкласу К, Ц, Д, КЦ, КД, КЦД;

- шосте концепт-правило - вперше запропонованй механізм профільних послуг безпеки за поточним рейтингом профілю має одну системно-істотну перевагу, яка полягає в його чутливості до повноти набору визначених вище *елементарних* функціональних послуг безпеки ПБ-ЕФ та необхідних ПБ-НУ, саме тому він може бути практично використаний експертом для електронного документування результатів оцінювання рівня гарантій коректності реалізації функціональних і гарантійних послуг безпеки за вимогами принципово важливого і нового нормативного документу НД ТЗІ 2.7-010-10 [8];

- сьоме концепт-правило - кожний профіль визначається за рівнем витрат на безпеку, за рівнем рейтингу профіля, за рівнем обмежень видів інформаційної діяльності, а також комплексно характеризується так званою технологією Т обробки захищуваної інформації залежно від кількості і рівнів профільних послуг безпеки, а також підкласу і класу ЗКС;

- восьме концепт-правило - вперше запропонований для побудови та організації архітектури ЗКС рівень обмежень видів інформаційної діяльності може бути використаний на об'єкті інформаційної діяльності з використанням захищених комп'ютерних систем першого, другого чи третього класу, він визначається і реалізується за окремими спеціальними вимогами;

- дев'яте концепт-правило - дотримання *трьох* основних *системних принципів реалізації* послуг безпеки: *принцип показу* (послуга є чи ні), *принцип демонстрації* (послуга безпеки функціонує чи ні), *принцип доказу* (послуга безпеки ефективна чи ні);

- десяте концепт-правило - рівні гарантії інформаційної безпеки в моделі враховуються за вимогами НД ТЗІ 2.5-004 опосередковано тільки для деяких профільних послуг безпеки, а в неявному вигляді – для всіх адаптивних профільних послуг безпеки АФП-Т. Так, вони зазначаються окремо і явно за рівнями Г-1…Г-7 та опосередковано в АФП-Т через порядковий номер технології Т обробки захищуваної інформації в обраному адаптивному функціональному профілі. Наприклад, в АФП-Т вони враховуються за рівнем Г-3 через умовно-необхідні послуги безпеки для послуги "Аналіз прихованих каналів" першого, другого і третього рівнів, тобто для профільних послуг безпеки КК-1, КК-2, КК-3, а також для послуги "Конфіденційність при обміні" четвертого рівня, тобто профільної послуги безпеки КВ-4 [6, 9, 10].

Ефективність обраної політики побудови архітектури ЗКС можна оцінити за різними варіантами залежно від пріоритетності обраного кінцевого результату - або ефективне нормування рівнів, або ефективний адаптивний загрозам функціональний профіль за підкласами конфіденційності К, цілісності Ц, доступності Д та їх сполучень КЦ, КД, ЦД, КЦД, або вартість. При цьому шкали оцінки ефективності будуть різні.

Пропонується, як вже вперше було успішно реалізовано в міжнародних критеріях ITSEC (Англія, Німеччина, Франція, Нідерланди), CCITCE (США, Канада, Англія, Німеччина, Франція, Нідерланди), а також в Україні при розробці і введенні в дію пакету нормативних документів з питань захисту інформації в комп'ютерних системах від несанкціонованого доступу, обрати найбільш пріоритетним показник стійкості захищеності всієї комп'ютерної системи від несанкціонованого доступу. При такому підході експертну оцінку стану безпеки інформації в ЗКС пропонується використати такі узагальнені критерії замість множини 110 часткових критеріїв за вимогами наданого вище пакету нормативних документів [10, 11].

По-перше, визначати рейтинг Е профілю захищеності, який чисельно оцінюється імовірністю надання повної низки елементарних функціональних ПБ-ЕФ, умовно-необхідних ПБ-УН та елементарних

гарантійних ПБ-ЕГ послуг безпеки для кожної обраної профільної послуги безпеки ПБ-ПР в певній ЗКС. Рейтинг Е визначається як функціонал F послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ, ПБ-ПР.

По-друге, визначати ризик безпеки R інформації в КС, який чисельно оцінюється імовірністю ненадання ні однієї послуги безпеки із повної низки елементарних функціональних ПБ-ЕФ, умовно-необхідних ПБ-УН та елементарних гарантійних ПБ-ЕГ послуг безпеки для кожної обраної профільної послуги безпеки ПБ-ПР в оцінюваній ЗКС.

Ризик безпеки визначається як зворотний функціонал F послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ, ПБ-ПР.

По-третє, визначати певний рівень гарантії безпеки Г-1…Г-7 для певного рейтингу Е чи ризику безпеки R обраних профілів захищеності інформації для захищених КС (АС) певного підкласу згідно з вимогами НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, а також методичних вказівок нових НД ТЗІ 2.7-09-09 і НД ТЗІ 2.7-10-09, які зробили вагомий внесок в розвиток теорії ТЗІ.

Перспективний багатофакторний критерій організації і побудови архітектури ЗКС за факторами рейтинг профілю-ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість призначений для надання науково-практичних рекомендацій в два послідовних етапи.

На першому етапі - експертна оцінка ефективності організації і побудови архітектури ЗКС за кількісним критерієм рейтинг профілю-ризик безпеки-гарантія безпеки, вона може бути практично реалізована за програмно-алгоритмічними правилами вже існуючих експертних систем “Торсіон-1”, “Торсіон-3”.

На другому етапі - підтримка прийняття рішень щодо перспективних шляхів підвищення ефективності архітектури захищених комп’ютерних систем за критерієм рейтинг профілю-ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість з можливістю заключної оптимізації за цими факторами.

Основна увага щодо підходів до оптимізації за чотирма факторами має бути зосереджена на реалізації моделі політики підвищення ефективності організації і побудови архітектури захищених комп’ютерних систем, а також шляхів її реалізації з використанням *принципу покрокової оптимізації* зворотними математичними методами теорії динамічного програмування Беллмана. Тобто, на якому б етапі не почалось підвищення ефективності архітектури оцінюваної ЗКС (розробка, модернізація, впровадження), наступні кроки забезпечення будуть тільки оптимальними та з використанням найменшої кількості варіантів перебору у порівнянні з усіма іншими відомими математичними методами оптимізації. Але для цього необхідно самостійно розробити цільову функцію і рекурентну формулу для її обчислення з прикладною формалізацією фізичного смислу їх класичних математичних показників. Тому метод динамічного програмування обмежено поширений і потребує високого рівня математичної підготовки щодо формалізації багатофакторних прикладних задач. До такого класу задач відноситься і проблема підвищення ефективності організації і побудови архітектури ЗКС.

На другому етапі також необхідно розробити нові програмно-алгоритмічні правила для оцінки ефективності архітектури за кількісним критерієм рейтинг профілю-ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість. Принциповим при цьому є підхід до визначення "ваги" та "нормування" послуг безпеки кожного із чотирьох факторів для здійснення їх кількісної оцінки та подальшої оптимізації. Кількісна "вага" визначається окремо для рівнів обмежень видів інформаційної діяльності, рівнів захищеності інформації, гарантійних послуг безпеки рівнів Г-1…Г-7 та рівнів витрат.

При виборі **“**ваги**”** та математичного **"**методу оптимізації**"** послуг безпеки для кожного із чотирьох факторів концептуальної моделі політики безпеки важливо дотримуватись реалізації принципу поступового нарощування захищеності інформації або, що теж саме, поступового зниження ризику безпеки:

- при додатковому наданні до складу обраного адаптивного профілю АФП-Т *нової профільної* послуги безпеки або *більш високого її рівня;*
- при підвищенні рівня *гарантії* безпеки;
- при підвищенні *вимог до рівня обмежень* кожного із обраних *видів інформаційної діяльності* на об’єкті інформаційної діяльності (одержання, використання, поширення, зберігання інформації) за обраною політикою інформаційної, антивірусної та фізичної безпеки ЗКС;
- при підвищенні *витрат* на безпеку кожного із рівнів та видів інформаційної діяльності;
- при підвищенні *витрат* на функціональні, гарантійні та профільні послуги безпеки від несанкціонованого доступу;
- при підвищенні *витрат* на антивірусну безпеку;
- при підвищенні *витрат* на фізичну безпеку.

Прокоментуємо цей принцип більш докладно.

При виборі “ваги” *функціональних та гарантійних* послуг безпеки необхідно дотримуватись наступного: поступове нарощування захищеності інформації (зниження ризику безпеки) **З**КС здійснювати тільки за обраним адаптивним функціональним профілем АФП-Т при додатковому наданні в ньому *або нової* функціональної послуги безпеки конфіденційності К, цілісності Ц, доступності Д, спостереженості Н, *або*

більш вищого їх рівня, а також більш *вищого рівня* гарантії безпеки Г-1 ... Г-7 за вимогами: НД ТЗІ 2.5-004 (далі Критерії), особливо Додатків А, Б; НД ТЗІ 2.5-005 (далі Класифікація АС); НД ТЗІ 1.1-002 (далі Загальні положення), нових НД ТЗІ 2.7-009-09, НД ТЗІ 2.7-010-09. Проведені дослідження показують, що при цьому можливі повторні значення "ризику безпеки" [10].

Пропонується для їх запобігання та більшої чутливості критерія ризик безпеки - гарантія безпеки - вид інформаційної діяльності - вартість надавати "вагу" у відносних значеннях для повної групи випадкових подій від 0.000 до 1 для сукупностей послуг за підкласами К, Ц, Д, КЦ, КД, ЦД, КЦД, але з урахуванням в кожному підкласі повної множини дев'яти послуг спостереженості Н у вигляді сукупності послуг КН, ЦН, ДН, КЦН, КДН, ЦДН, КЦДН. Так, для підкласу К (підвищені вимоги до послуг безпеки конфіденційності К) "вага" повинна нормуватися до 1 для одночасного надання послуг К, Ц, Д, Н, наприклад 0.700 (підвищена вага К), 0.100, 0.100, 0.100 (рівномірна вага послуг Ц, Д, Н), тобто нормування до 1 виконується (0.7+0.100+0.100+0.100 = 1.000). Можливі й інші коефіцієнти ваги.

Для реалізації експертної кількісної оцінки по фактору "вартість" пропонується за результатами проведених досліджень [10] та згідно з вимогами Критеріїв для кожної елементарної функціональної послуги безпеки в таблично-текстовому форматі (ПБ-ЕФ) в розділі 6 Критеріїв (критерії конфіденційності К), аналогічно в розділі 7 (критерії цілісності Ц), розділі 8 (критерії доступності Д), розділі 9 (критерії спостереженості Н), а також для кожної елементарної гарантійної послуги безпеки (ПБ-ЕГ) в підрозділах 10.1...10.4 Критеріїв надавати вартість в у. о. усім послугам ПБ-ЕФ, ПБ-ЕГ за статистичними даними різних їх ліцензіатів. Для узгодженості з критерієм рейтинг профілю-ризик безпеки-гарантія безпеки необхідно критерію "вартість" також, як і критерію "ризик безпеки", кількісну оцінку надавати у відносних значеннях від 0.000 до 1. Аналогічні вимоги стосується критерія "вид інформаційної діяльності", в якому треба додатково врахувати вимоги до категорій оброблюваної інформації обмеженого доступу через рівні обмежень видів інформаційної діяльності, і надавати вагу також у відносних значеннях.

ІІІ ВИСНОВКИ

1. Запропоновані критерії і методологія можуть бути використані для підвищення ефективності організації і побудови архітектури захищених комп'ютерних систем при їх розробці, модернізації і впровадженні в два етапи з використанням кількісного і перспективного критеріїв.

2. Запропоновані десять концепт-правил та концептуальна модель політики побудови архітектури захищених комп'ютерних систем з нормуванням її рівнів безпеки за підкласами кожного класу та за критерієм рейтинг профілю-ризик безпеки-рівень обмежень видів інформаційної діяльності-вартість можуть бути базовою основою для подальшого розвитку теорії побудови й організації архітектури захищених комп'ютерних систем.

3. Для практичної реалізації запропонованих методичних рекомендацій потребуються подальші дослідження з метою розробки та створення Національного електронного каталогу адаптивних загрозам за підкласами профілів захищеності інформації АФП-Т в АС усіх класів і підкласів замість визначеної і неповної низки регламентованих базових профілів захищеності в чинних НД ТЗІ 2.5-005-99 (всього 90 профілів з їх повної низки 740360298600).

Література: ***1.*** *В. А. Герасименко. Защита информации в автоматизированных системах обработки данных. В 2-х кн.% Кн. 1.- М.: Энергоатомиздат, 1994.- 400 с.: ил.* ***2.*** *XIII Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникаионных системах». Тезисы докладов 18-22.05.10. (Программа конференции, семинар №2 20.05.10, Шорошев В. В. «Критерии и методы оценки эффективности организации и построения архитектуры защищенных компьютерных систем», с. 22).* ***3.*** *ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.* ***4.*** *ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.* ***5.*** *ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.* ***6.*** *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.* ***7.*** *НД ТЗІ 2.7 -009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Адміністрація Державної служби спеціального звязку та захисту інформації України, 2009.* ***8.*** *НД ТЗІ 2.7 -010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2009.* ***9.*** *НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні профілі захищеності інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 1999.* ***10.*** *А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного*

департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20.11.2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003р. – 316с. ***11.*** *Шорошев В. В., Илницкий А. Е., Близнюк И. Л. Оценка безопасности информации в компьютерных системах от угроз НСД: обобщенные критерии, табличные методы. Бизнес и безопасность N1, 2003. С.74-75.* ***12.*** *В. Шорошев. Оцінка стану безпеки інформації за стандартними профілями її захищеності в комп'ютерних (автоматизованих) системах. Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні", НТУ України "КПІ", Міносвіти і науки України, ДСТСЗІ СБ України, випуск № 8, 2004. С. 48-56.*

УДК 681.3

НОВА КОНЦЕПЦІЯ ПОЛІТИКИ ПОБУДОВИ ТА ОРГАНІЗАЦІЇ АРХІТЕКТУРИ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ З НОРМУВАННЯМ РІВНІВ ЇЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олександр Дмитренко
УТЗІ ДДЗР МВС УКРАЇНИ

Анотация: **На основі багаторічних досліджень пропонується методологія оцінки ефективності реалізації нової політики концептуальної побудови архітектури захищеної комп'ютерної системи з нормуванням її інформаційної безпеки за критерієм рейтинг профілю, ризик безпеки, рівень обмежень видів інформаційної діяльності, вартість.**

Summary: **On the basis of long-term researches methodology of estimation of efficiency of realization of new policy of conceptual construction of architecture of the protected computer system is offered with setting of norms of its informative safety on a criterion rating of type, risk of safety, level of limitations of informative activity, cost.**

Ключові слова: **Потенційні загрози, несанкціонований доступ, конфіденційність, цілісність, доступність, спостереженість, функціональні послуги безпеки, гарантійні послуги безпеки, профільні послуги безпеки, антивірусна безпека, ідентифікація, автентифікація.**

I Вступ

Пропонується нова Концепція політики побудови архітектури захищеної комп'ютерної системи (ЗКС) з нормуванням рівнів її інформаційної безпеки за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Як основний механізм пошуку рішення щодо організації і побудови архітектури ЗКС пропонується використовувати методи концептуальної евристики [1]. Вони передбачають визначення множини таких шляхів рішення проблемної задачі, серед яких з достатньою імовірністю є і найбільш результативний шлях з використанням функціональних профілів, адаптивних загрозам (АФП).

При аналізі початкової ситуації людина-експерт непросто збирає інформацію, необхідну для рішення задачі, а будує багатофакторну структуровану концептуальну модель проблемної ситуації, виокремлює найбільш важливі елементи, відносини між ними і формує на їх основі узагальнені елементи та відносини між ними. Такі узагальнені елементи і відносини між ними в концептуальних евристиках визначаються як концепти [2, 3]. На їх основі надається можливість досягнення обраної мети при традиційному об'єкті дослідження ЗКС, але при нових предметах дослідження як в теоретичному, так і в практичному аспектах.

Передусім очевидно, що при організації і побудові архітектури ЗКС має бути пріоритетність вимог чинних нормативно-правових документів, їх треба дотримуватись та надавати їм подальший розвиток щодо шляхів їх практичної реалізації, в тому числі з урахуванням міжнародного і вітчизняного досвіду та за результатами власних досліджень.

II Основна частина

На рис. 1 наведена нова концептуальна модель політики побудови архітектури ЗКС з нормуванням рівнів її інформаційної безпеки за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Справа в тому, що експертна оцінка та оптимізація стану інформаційної безпеки за чотирма факторами сама по собі складна як в теоретичному, так і в практичному аспектах. Чотирьохфакторний функціонал сам по собі потребує використання чутливих математичних методів до змін факторів. В запропонованій моделі зміни цих факторів формалізуються стандартизованими рівнями (Layer). Проаналізуємо їх.