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

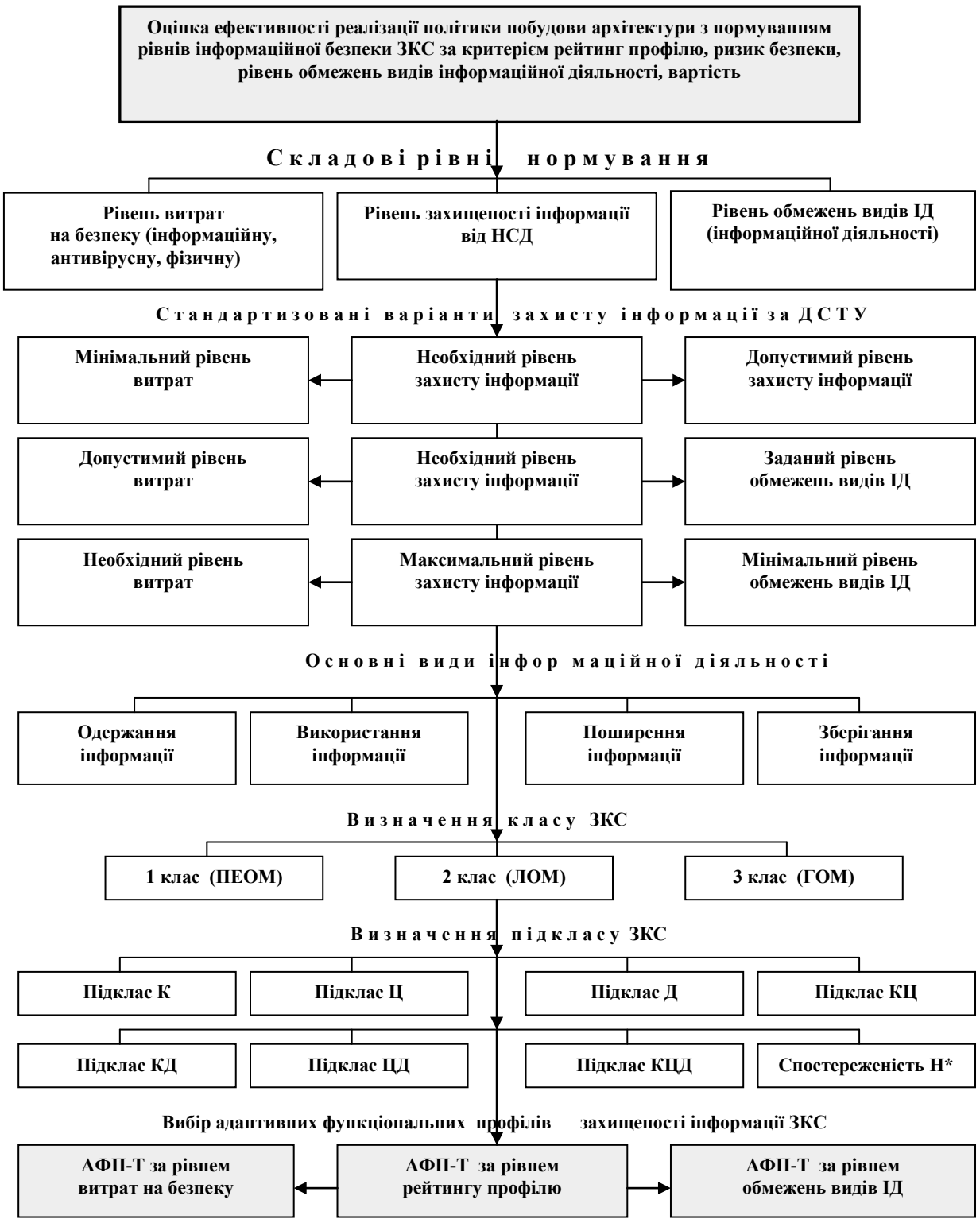
Пропонується нова Концепція політики побудови архітектури захищеної комп'ютерної системи (ЗКС) з нормуванням рівнів її інформаційної безпеки за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Як основний механізм пошуку рішення щодо організації і 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.



Примітка: 1. * позначено, що послуга безпеки Спостереженість Н* є необхідною для уісх підкласів і класів ЗКС.

2. Послуги гарантії безпеки враховуються окремо та в АФП-Т через порядковий номер технології Т обробки інформації, що захищається, в ЗКС.

Рисунок 1 – Концептуальна модель політики побудови архітектури ЗКС з нормуванням рівнів рейтингу профілю, гарантій безпеки, обмежень видів інформаційної діяльності, вартості

Так, захищеність інформації регламентується двома рівнями – необхідний та максимальний. Види інформаційної діяльності регламентуються допустимим, заданим та мінімальним рівнями обмежень. Рівень захисту інформації регламентується теж двома рівнями - необхідним і максимальним. Витрати на захищеність інформації регламентуються мінімальним, допустимим та необхідним рівнями. Це рівні, що стандартизовані ДСТУ [14 – 16].

Рівні гарантії безпеки регламентуються за вимогами НД ТЗІ 2.5-004, але в неявному вигляді опосередковано і з деякими особливостями. Вони зазначаються окремо та явно за рівнями гарантій Г-1…Г-7 й опосередковано в СФП-Т через порядковий номер технології Т обробки інформації, що захищається, в обраному стандартному функціональному профілі (СФП). Так, в СФП-Т вони враховуються за рівнем Г-3 через умовно-необхідні послуги безпеки для послуг "Аналіз прихованих каналів" першого, другого і третього рівнів, тобто КК-1, КК-2, КК-3, а також для послуги "Конфіденційність при обміні" четвертого рівня, тобто КВ-4 [1 – 16].

Ризик безпеки залежить від рівня захищеності інформації (необхідного, максимального), обраного СФП захищеності інформації та рівня гарантії безпеки Г-1…Г-7. В Концепції прийнято наступний підхід, при якому для експертної оцінки стану безпеки інформації в ЗКС доцільно використовувати узагальнені критерії замість множини 110 часткових критеріїв [4, 5, 2].

По-перше, визначати рейтинг Е профілю захищеності, який чисельно оцінюється імовірністю надання повної низки елементарних ФПБ - ПБ-ЕФ, умовно-необхідних ПБ-УН та елементарних гарантійних ПБ-ЕГ послуг безпеки для кожної обраної профільної послуги безпеки ПБ-П в певній ЗКС. Рейтинг Е визначається як функціонал F послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ.

По-друге, визначати ризик безпеки R інформації в комп'ютерній системі (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-П у певній КС.

Ризик безпеки визначається як функціонал F послуг безпеки ПБ-П, ПБ-ЕФ, ПБ-УН, ПБ-ЕГ та рівнів гарантії безпеки Г-1....Г-7.

По-третє, визначати певний рівень гарантії безпеки Г-1…Г-7 для певного рейтингу Е чи ризику безпеки R обраних профілів захищеності інформації СПЗІ для захищених КС (АС) певного класу та підкласу згідно з вимогами НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99.

В Концепції пропонуються програмно-алгоритмічні методи обчислення рейтингу профілю, ризику безпеки і гарантії безпеки, які вже визначено в роботі [2] щодо концептуальної моделі політики безпеки архітектури захищених комп'ютерних систем за критерієм рейтинг профілю-ризик безпеки-гарантія безпеки, а також в новій багатофакторній моделі рис. 1.

Таким чином, у загальному вигляді математичне співвідношення запропонованих узагальнених критеріїв можна визначити такими виразами:

$$E = F\ (ПБ\text{-}П,\ ПБ\text{-}ЕФ,\ ПБ\text{-}УН,\ ПБ\text{-}ЕГ) \quad (1)$$

$$R = F\ (E,\ Г\text{-}1...Г\text{-}7) \quad (2)$$

Програмно-математична реалізація наведених співвідношень досить складна і вирішується різними програмно-математичними методами шляхом обчислення певних ймовірностей – граф (дерево) подій, співвідношення числа успішних подій до їх можливої повної низки, формули Байеса, але при цьому за основу приймається обов'язкове дотримання вимог елементарних послуг безпеки, регламентованих в НД ТЗІ 2.5-004-99, тобто послуг безпеки ПБ-ЕФ, ПБ-УН, ПБ-ЕГ.

Концепція безпеки КС за критерієм ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість призначена для надання науково-методичних рекомендацій щодо забезпечення можливих шляхів рішення двох основних задач.

1. Експертна оцінка поточного стану інформаційної безпеки КС за критерієм рейтинг профілю-ризик безпеки-гарантія безпеки.

2. Підтримка прийняття рішення щодо забезпечення належного стану інформаційної безпеки КС шляхом її чотирьохфакторної оптимізації за критерієм ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість.

Як і будь-яка, запропонована Концепція визначає основні принципи і підходи рішення проблеми. У нашому випадку це визначення підходів щодо рішення двох основних задач, зазначених вище.

Оптимізація по факторам ризик безпеки, гарантія безпеки, вид інформаційної діяльності, вартість на даний час, *по-перше*, в такій постановці задачі нова і досить актуальна для подальшого розвитку нормативно-правового забезпечення щодо можливих шляхів рішення проблеми безпеки КС.

По-друге, наразі в Україні поки що відсутня базова методика оцінки захищеності інформації в КС від

несанкціонованого доступу

Основна увага в Концепції щодо підходів до оптимізації за чотирма факторами зосереджена на визначенні моделі політики безпеки, а також вимог і шляхів її реалізації.

Експертна оцінка стану інформаційної безпеки КС здійснюється в два етапи.

На ***першому етапі*** оцінка здійснюється за кількісним критерієм ризик безпеки-гарантія безпеки за програмно-алгоритмічними правилами вже існуючої експертної системи "Торсіон-1", описаної в Концепції безпеки комп'ютерних систем за критерієм рейтинг профілю-ризик безпеки-гарантія безпеки [2].

На другому етапі необхідно розробити нові програмно-алгоритмічні правила для оцінки за кількісним критерієм ризик безпеки - гарантія безпеки - вид інформаційної діяльності - вартість. Принциповим при цьому є підхід до визначення "ваги" 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, рівнів гарантії послуг безпеки Г-1…Г-7 та рівнів витрат.

При виборі **"**ваги**"** та математичного "методу оптимізації" послуг безпеки для кожного із чотирьох факторів моделі політики безпеки (рис. 1) важливо дотримуватись реалізації:

принципу поступового нарощування захищеності інформації або, що теж саме, ***поступового зниження ризику безпеки:***

при появі в обраному стандартному профілі захищеності інформації ***нової функціональної*** послуги безпеки або ***більш високого її рівня;***

при підвищенні рівня ***гарантії*** безпеки;

при підвищенні ***вимог до рівня обмежень*** кожного із обраних ***видів інформаційної діяльності*** (одержання, використання, поширення, зберігання інформації) за обраною політикою інформаційної, антивірусної та фізичної безпеки КС;

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.

Слід прокоментувати цей принцип більш докладно.

При виборі "ваги" ***функціональних та гарантійних*** послуг безпеки необхідно дотримуватись наступного правила: поступове нарощування захищеності інформації (зниження ризику безпеки) КС здійснювати тільки за обраним стандартним функціональним профілем СФП-Т при появі в ньому додаткової *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). Проведені дослідження показують, що при цьому можливі повторні значення "ризику безпеки".

Для їх запобігання та більшої чутливості критерія ризик безпеки - гарантія безпеки - вид інформаційної діяльності - вартість доцільно надавати "вагу" у відносних значеннях від 0.000 до 1 окремо для сукупностей послуг за підкласами К, Ц, Д, Н, КЦ, КД, ЦД, КЦД та сукупностей 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 виконується нормування до 1 (О.7+0.100+0.100+0.100 = 1.000). Можливі інші ваги.

Для реалізації експертної кількісної оцінки за фактором "вартість" необхідно, згідно з вимогами Критеріїв та за результатами проведених досліджень [2], для кожної елементарної функціональної послуги безпеки надавати вартість в умовних одиницях усім послугам ПБ-ЕФ, ПБ-ЕГ за статистичними даними різних їх ліцензіантів в таблично-текстовому форматі (ПБ-ЕФ) в розділі 6 Критеріїв (критерії конфіденційності К), аналогічно розділі 7 (критерії цілісності Ц), розділі 8 (критерії доступності Д), розділі 9 (критерії спостереженості Н), а також аналогічно для кожної елементарної гарантійної послуги безпеки (ПБ-ЕГ) в підрозділах 10.1...10.4 Критеріїв. Для узгодженості з критерієм ризик безпеки-гарантія безпеки необхідно критерію "вартість" також, як і критерію "ризик безпеки", надавати кількісну оцінку у відносних значеннях від 0.000 до 1. Аналогічні вимоги до критерію "вид інформаційної діяльності", в якому треба додатково врахувати вимоги до категорій оброблюваної інформації обмеженого доступу через рівні обмежень видів інформаційної діяльності і надавати вагу у відносних значеннях.

Програмно-алгоритмічні правила оптимізації стану інформаційної безпеки КС різних класів і підкласів за кількісним критерієм ризик безпеки - гарантія безпеки - вид інформаційної діяльності - вартість повинні

дотримуватись ***наступних принципів:***

- *поступового нарощування* захищеності інформації оцінюваної КС даного класу та підкласу за обраним профілем СФП-Т - або при додатковому наданні в ньому нової функціональної послуги безпеки К, Ц, Д, Н, або більш вищого її рівня, або більш вищого рівня гарантії безпеки Г-1 ... Г-7 за вимогами Критеріїв (особливо Додатків А, Б), Класифікації АС та Загальних положень;

- *покрокової оптимізації* математичними методами теорії динамічного програмування, тобто - в якому б поточному стані не була інформаційна безпека оцінюваної КС, наступні шаги забезпечення її належного стану мають бути найбільш оптимальними, можливі інші математичні методи;

- *комплексної реалізації* вимог нормативно-правового, програмно-технічного та організаційно-кадрового забезпечення належного стану інформаційної безпеки на всіх етапах життєвого циклу оцінюваної КС.

- *реалізації системних* послуг безпеки: ***принцип показу*** (послуга безпеки "ПБ-Пок" є чи ні), ***принцип демонстрації*** (послуга безпеки "ПБ-Дем"функціонує чи ні), ***принцип доказу*** (послуга безпеки "ПБ-Док" ефективна чи ні).

Для урахування кращого міжнародного і вітчизняного досвіду програмно-алгоритмічні правила оцінки поточного та оптимізації належного стану інформаційної безпеки мають бути гармонізовані з вимогами: Конвенції Ради Європи про кіберзлочинність щодо боротьби зі злочинами проти конфіденційності, цілісності, доступності комп'ютерних даних і систем та шахрайства з комп'ютерами; Концепції безпеки комп'ютерних систем за вимогами Закону про основи національної безпеки України щодо загроз та напрямів державної політики в інформаційній сфері; керівних документів Російської Федерації з захисту інформації від НСД щодо врахування кращого досвіду класифікації і вимог до АС і ЗОТ; міжнародних стандартів ISO 15408, ISO 17799 щодо практичних правил управління інформаційною безпекою; Кримінального кодексу України щодо дотримання вимог "Злочини з використанням електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем і мереж та систем електрозв'язку".

Базовими вихідними даними для експертної оцінки та оптимізації безпеки КС за критерієм ризик безпеки - гарантія безпеки - вид інформаційної діяльності - вартість визначається стандартний функціональний профіль з заданим порядковим номером технології обробки (Т) інформації, що захищається, (СФП-Т). Певний СФП-Т в конкретній КС визначається в результаті проведення аналізу загроз, оцінки ризиків підкласу АС за вимогами Класифікація АС [5, 4].

III Висновки

1. Новизна Концепції політики побудови та організації архітектури захищених комп'ютерних систем полягає в наступних концептуальних чинниках: пропонується визначати найбільш пріоритетною і *комплексною* послугою безпеки адаптивний загрозам НСД функціональний профіль захищеності інформації за моделлю політики побудови архітектури ЗКС з нормуванням рівнів рейтингу профілю, гарантій безпеки, обмежень видів інформаційної діяльності, вартості;

2. Дістала подальшого розвитку теорія технічного захисту інформації щодо необхідності обов'язкового використання державними експертами при оцінюванні не тільки функціональних послуг безпеки послуг, але і їх рівня гарантій за новими методичними вказівками [12, 13], що є вагомим внеском в теорію ТЗІ, але і за методичними вказівками щодо оцінювання функціональних послуг безпеки, адаптивних загрозам.

3. Запропонована Концепція може бути використана для формування та обґрунтування положень політики безпеки архітектури захищених комп'ютерних систем за критерієм ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість.

Література ***1.*** *Шорошев В. В., Давиденко А. М., Попенко О. С., Близнюк І. Л., Ковадло М. В., Вербенський М. Г., Терещенко Ю. В., Дмитренко О. П., Гіранова А. К. НДР «Синергетична система підтримки прийняття рішень щодо генерації і вибору профілів протидії загрозам забезпечення підвищених вимог до конфіденційності, цілісності, доступності і спостереженості інформації, оброблюваної в автоматизованих системах ОВС України ПРОФІЛЬ». Методичні рекомендації. МВС України, ДДЗР МВС України, ДНДІ МВС України, ІПМЕ ім. Г.Е.Пухова НАН України. Київ, 2011;* ***2.*** *Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Кн. 1.- М.: Энергоатомиздат, 1994.- 400 с.: ил.;* ***3.*** *Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем. Монографія. Вид. ДУІКТ, с. 257. К. 2011;* ***4.*** *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБУ, 199;* ***5.*** *НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні профілі захищеності інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 1999;* ***6.*** *НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. ДСТСЗІ СБУ, 1990 (зі зміною № 1, затвердженою наказом ДСТСЗІ СБУ від 18.06.02 № 37);* ***7.*** *НД ТЗІ 1.1-*

001-2000. Типове положення про службу захисту інформації в автоматизованій системі. ДСТСЗІ СБУ, 2000; ***8.*** *НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 2000;* ***9.*** *НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації від несанкціонованого доступу. ДСТСЗІ СБУ, 2001;* ***10.*** *НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. ДСТСЗІ СБУ, 2002;* ***11.*** *НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. ДСТСЗІ СБУ, 2003;* ***12.*** *НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.* ***13.*** *НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу;* ***14.*** *ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;* ***15.*** *ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;* ***16.*** *ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.*

УДК 004.056: 004.942

СИСТЕМНИЙ ПІДХІД У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Віталій Носов

Харківський національний університет внутрішніх справ, м. Харків

Анотація: **Запропоновано використання системного підходу в забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем. Представлена формальна модель і ключові характеристики мережі взаємин комплексної системи захисту інформації в складі узагальненої інформаційно-телекомунікаційної системи.**

Summary: **Approach Systems to information security of corporate information and telecommunication systems is proposed. The formal model and key characteristics of network relationships Information Security Complex System consisting in a Common Information and Telecommunication System is represented.**

Ключові слова: **Системний підхід, інформаційна безпека, формальна модель.**

I Вступ

Для забезпечення інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем створюються і експлуатуються системи захисту інформації, які, як і інші створені людиною організаційно-технічні системи, в своїй більшості мають суттєві недоліки, а саме:

- створені, як правило, без належного обґрунтування затрат;
- експлуатуються без оцінювання ефективності роботи;
- технічно реалізовані, але не використовуються;
- розроблені на стадії технічного проекту, але не впроваджені в діючу інформаційно-телекомунікаційну систему;
- і таке інше.

Одним із шляхів концептуального подолання більшості відомих вад систем захисту інформації є створення *життєздатної* системи захисту інформації, що потребує, на думку автора, системного мислення та системного підходу.

Метою статті є:

- представлення математичної моделі системи захисту інформації у складі корпоративної інформаційно-телекомунікаційної системи;
- формулювання ключових характеристик системного мислення та системного підходу у забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем.

II Основна частина

Системне мислення та системний підхід

Що таке система? За визначенням основоположника загальної теорії систем Ludwig von Bertalanffy [1] система – це сукупність елементів, що знаходяться в певних стосунках один з одним і з середовищем. Або за