УДК 004.415.056.5 **С.В.Толюпа, І.І Пархоменко**

ПОБУДОВА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ СКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ СТРУКТУРНОГО ПІДХОДУ

В статті запропонований системний підхід до побудови комплексних систем захисту інформації, що дозволяє істотно скоротити терміни розробки СЗІ й при цьому запропонувати замовнику дійсно оптимальне та обгрунтоване рішення. Показано, що поняття системності інтерпретувалося насамперед у тому сенсі, що захист інформації полягає не тільки у створенні відповідних механізмів, а являє собою регулярний процес, який здійснюється на всіх етапах життєвого циклу інформаційної системи при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи й заходи, які використовуються для захисту інформації, неодмінно та найбільш раціонально об'єднуються в єдиний цілісний механізм - систему захисту.Системний підхід до захисту інформації передбачає необхідність врахування всіх взаємопов'язаних, взаємодіючих і змінюються в часі елементів, умов і факторів, істотних для забезпечення безпеки інформаційної.

Ключові слова: інформаційна система, захист, модель, системний підхід, показник, синтез.

Вступ

Ми зараз живемо в складному інформаційному та кібернетичному просторах, складність яких постійно зростає. Передбачити архітектуру інформаційних систем майбутнього й навіть загальні принципи побудови досить складно, але аналіз тематики деяких сучасних теоретичних досліджень в області складних систем і різноманітних мережевих структур дозволяє зробити деякі припущення про можливу зовнішність і навіть деякі особливості таких систем. Є підстава вважати, що це будуть багатовимірні та багаторівневі інформаційні системи і забезпечити надійний їх захист буде досить складно.

Процеси, пов’язані з передачею інформації в такій інтегрованій системі, звичайно, багато складніше, ніж в існуючих системах. Крім того, уявити собі детально майбутні способи вдосконалення такого роду мережі за рахунок сумісного використання її ресурсів поки скрутно навіть на основі винаходів з даної тематики. Уже зараз є поняття того, що для використання потенціальних можливостей багатовимірної та багаторівневої інтегрованої системи необхідні адекватні методи дослідження і пошуку найкращих рішень, які не стали ще традиційними.

З іншого боку, не можна ігнорувати те, що підхід, пов’язаний з розглядом інформаційних систем, як відповідним чином структурованих систем, відкриваючи певні принадні перспективи їх вдосконалення, одночасно пов’язаний з необхідністю подолання істотних труднощів. До їх числа відноситься, наприклад, та обставина, що фундаментальна математична основа теорії гіпермереж, і тим більше пов’язані з нею обчислювальні методи, алгоритми й програмне забезпечення помітно складніше за ті, які вважаються традиційними, як, наприклад, методи, що базуються на математичному апараті звичайних матриць і теорії графів. Відповідно розробка технічних засобів таких систем і їх програмного забезпечення навряд чи стане менш трудомісткою й витратною не говорячи вже про системи захисту. Не виключено, що в процесі конструювання багатовимірних та багаторівневих інформаційних систем та їх захисту, для вирішення найбільш складних завдань буде потрібно об’єднання спільних зусиль фахівців галузевої і академічної науки[1].

Якщо розглядати проблеми й завдання синтезу структури інфокомунікаційних систем, то вони тісно взаємозалежні й утворять у сукупності складну проблему, що в повному обсязі не вирішена й у цей час інтенсивно розробляється багатьма дослідниками. Відомі різні підходи до синтезу структури складних систем, до них ставляться методи декомпозиції, координації й агрегації. Характер взаємодії між керуючими підсистемами й розподіл функцій між ними багато в чому визначаються прийнятими принципами й алгоритмами керування, ступенем централізації при виробленні керуючих впливів і при їхньому здійсненні, погодженістю цілей підсистем різного рівня.

Основна частина

Побудова ієрархічних систем із гнучким керуванням ставить зв'язані між собою питання: раціонального вибору схем керування, визначення необхідної кількості рівнів та вимірів ієрархії встановлення між рівнями ефективних взаємозв'язків, розподілення відповідальності, організації інформаційних потоків і створення контурів прийняття рішень. Зокрема, число необхідних рівнів ієрархії безпосередньо пов'язане з можливістю переробки інформації на кожному рівні.

Головним напрямком пошуку шляхів захисту інформації, в таких складних інформаційних системах, є неухильне підвищення системності підходу до самої проблеми захисту інформації. Поняття системності інтерпретувалося насамперед у тому сенсі, що захист інформації полягає не тільки у створенні відповідних механізмів, а являє собою регулярний процес, який здійснюється на всіх етапах життєвого циклу інформаційної системи при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи й заходи, які використовуються для захисту інформації, неодмінно та найбільш раціонально об'єднуються в єдиний цілісний механізм - систему захисту [2-3].

Системний підхід до захисту інформації передбачає необхідність врахування всіх взаємопов'язаних, взаємодіючих і змінюються в часі елементів, умов і факторів, істотних для забезпечення безпеки інформаційної системи (ІС).

Принципи побудови систем захисту інформації повинні забезпечувати багаторівневий захист, причому не тільки від зловмисників, але й від некомпетентних або недостатньо підготовлених користувачів і персоналу. У системі захисту має бути, принаймні, чотири контури безпеки: зовнішній, що охоплює всю територію, на якій розташовані споруди; контур споруд, приміщень або пристроїв системи; контур компонентів системи (технічних засобів, програмного забезпечення, елементів баз даних) і контур технологічних процесів обробки даних. Основні труднощі реалізації систем захисту полягають у тому, що вони повинні задовольняти двом групам суперечливих вимог. З одного боку, необхідно забезпечити надійний захист системної інформації, що в конкретному випадку формулюється у вигляді двох узагальнених задач: виключення випадкової і навмисної видачі інформації стороннім особам та розмежування доступу до пристроїв та ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу. З іншого боку, системи захисту не повинні створювати помітних незручностей в процесі роботи з використанням ресурсів інформаційної системи. Зокрема мають бути гарантовані: повна свобода доступу кожного користувача та незалежність його роботи в межах наданих йому прав і повноважень. На жаль, необхідність системного підходу до питань забезпечення безпеки інформаційних технологій поки ще не знаходить належного розуміння у користувачів сучасних ІС [4].

Сьогодні фахівці з найрізноманітніших галузей знань, так чи інакше, змушені займатися питаннями забезпечення інформаційної безпеки. Це обумовлено тим, що ми живемо в суспільстві (середовищі) інформаційних технологій, куди перекочують всі соціальні проблеми людства, в тому числі й питання безпеки.

Якщо зібрати всіх фахівців разом, то за наявності у кожного з них величезного досвіду й знань, створити систему інформаційної безпеки часто так і не вдається. Розмовляючи про одні й тіж речі, фахівці часто не розуміють один одного оскільки у кожного з них свій підхід, своя модель представлення системи захисту інформації. Такий стан справ обумовлено відсутністю системного підходу, який визначив би взаємні зв'язки (відносини) між існуючими поняттями, визначеннями, принципами, способами і механізмами захисту.

На сучасному етапі розвитку інформаційних технологій забезпечення ІБ в масштабах всієї СЗІ поки що проблематично в силу відсутності на ринку реальних рішень, що дозволяють будувати саме інтегровані СЗІ. Мабуть це пояснюється недостатньою зрілістю міжнародних стандартів у галузі захисту інформації, хоча рух з цьому напрямку простежується вже досить явно. З іншого боку побудова багатокомпонентних, а тим більше однокомпонентних СЗІ в більшості випадків вже не є сучасним рішенням проблеми ІБ,

особливо для великих компаній. Можна сміливо констатувати, що жоден окремо вибраний засіб захисту інформації не може захистити від різноманіття існуючих загроз безпеці, а проста комбінація різноманітних засобів захисту призводить до зниження рівня захисту в цілому із-за можливої конфліктності розрізнених засобів захисту. Тому останнім часом намітилася тенденція до побудови складних комплексних систем інформаційної безпеки(КСЗІ).

Як показує практика, проектування комплексної (в широкому сенсі цього слова) СЗІ є досить складним системно-аналітичним завданням, яке вимагає спеціальної і досить суворої методики.

Відомо, що в області ІТ давно й досить успішно застосовується стековая модель опису складних ІС, в якій система розглядається у вигляді ієрархії декількох функціонально-однакових рівнів (вимірів). Оскільки будь-яка СЗІ в кінцевому підсумку повинна «накладатися» на реальну ІС, для її опису також доцільно було б використовувати багаторівневу ієрархічну модель. Це дозволило б, з одного боку, чітко визначити основні завдання, які вирішуються в рамках СЗІ, а також систему зв'язків між цими завданнями і, з іншого боку, коректно описати порядок взаємодії двох різних СЗІ. На наш погляд типову СЗІ можна розглянути у вигляді наступних п'яти функціональних рівнів:

- фізичний рівень: фізична охорона приміщень, в яких обробляється або зберігається конфіденційна інформація; організація контролю доступу співробітників в дані приміщення; відповідальне зберігання резервних (архівних) копій конфіденційних інформаційних ресурсів; забезпечення енерго- і пожежобезпеки всій ІС в цілому та т.ін.
- технологічний рівень: усунення загроз безпеці інформації, пов'язаних з використанням неякісних апаратно-технічних засобів обробки та зберігання інформації і систем передачі даних; контроль якості програмного забезпечення; організація резервних сховищ даних, кластерів; періодичне архівування даних; контроль ліцензійної політики; організація захисту від шкідливих і руйнуючих програм і т.д.
- користувальницький рівень: усунення загроз, пов'язаних з некоректними (випадковими, помилковими і т.ін.) діями персоналу або навмисними діями нелояльних співробітників компанії або третіх осіб (розмежування доступу до інформаційних ресурсів, захист від НСД, аутентифікація користувачів, включаючи віддалених і мобільних співробітників компанії і т.ін.).
- мережевий рівень: система захисту на цьому рівні повинна усунути загрози, які виходять від зловмисників, що знаходяться як всередині, так і поза межами ІС на рівні базової мережевої інфраструктури (сегментація системи за рівнями конфіденційності оброблюваної інформації, захист інформації при її передачі за зовнішніми та внутрішніх каналах зв'язку, захист від зовнішніх вторгнень і т.ін.)
- рівень управління: організація зв'язку з системою управління ІС (якщо така є); управління, координація та контроль організаційних і технічних заходів на всіх низлежащих рівнях СЗІ; контроль повноти реалізації функцій захисту на кожному з рівнів і нерозривності функціонування СЗІ при переході від рівня до рівня; остаточний (а далі періодичний) контроль стійкості та комплексності всій СЗІ в цілому.

Слід сказати, що в конкретній автоматизованій системі наявність всіх п'яти рівнів СЗІ в явному вигляді не завжди обов'язково, хоча стійкість системи захисту безпосередньо залежить від наявності кожного рівня та його функціональної наповненості. Очевидно також, що вартість і складність реалізації СЗІ істотним чином зростає від рівня до рівня, причому знизу-вгору. Так, наприклад, значну частину необхідних функцій СЗІ на фізичному рівні можна реалізувати простими й звичними організаційними заходами, тобто практично «безкоштовно». А, наприклад, на мережевому рівні для захисту складних систем необхідно застосування вже досить дорогих технологій, таких як межмережне екранування, VPN, засоби виявлення вторгнень і т.ін.

Одним з головних переваг подання СЗІ у вигляді ієрархії функціонально-незалежних рівнів є істотне спрощення процесу проектування системи, оскільки тепер проектування однієї багатофункціональної і складної системи можна розкласти на кілька закінчених етапів проектування набагато менш складних систем для кожного рівня окремо й завершального етапу контролю цілісності системи захисту при переході від рівня до рівня. У тому випадку, коли цілісність системи захисту зберігається, СЗІ в цілому може вважатися комплексною.

Слід зазначити, що пропонований п'ятирівневий «стековий» підхід крім спрощення самого процесу проектування, дозволяє чітко формалізувати три досить складні завдання, які неминуче виникають при створенні систем захисту ІБ:

• забезпечення цілісності (комплексності) системи захисту;

• розмежування вимог і функцій СЗІ при захисті інформації, що володіє різним ступенем конфіденційності;

• забезпечення цілісності СЗІ при захисті територіально-розподілених ІС.

При цьому при вирішенні зазначених завдань в абсолютній більшості випадків вдаєтьсяз абезпечити оптимальне співвідношення функціональність/вартість СЗІ для власника ІБ і належним чином це обґрунтувати.

Проблема забезпечення цілісності системи захисту в рамках запропонованої моделі СЗІ приймає досить зрозумілу й наочну форму - це, як уже було сказано, забезпечення повноти реалізації функцій захисту на кожному рівні моделі СЗІ й забезпечення цілісності функцій захисту при переході від рівня до рівня. Очевидно, що максимальний ступінь комплексності СЗІ досягається в тому випадку, коли застосовуються технічні засоби, рішення й методи забезпечують захист кожного рівня відповідно до найжорсткіших вимог і при цьому всі СЗІ технічні засоби проявляють свою функціональність на кожному рівні моделі. Очевидно, що побудувати настільки «комплексну» СЗІ в принципі можливо тільки при необмежених ресурсах проекту. Тому на практиці необхідно знайти розумний і, головне, обгрунтований компроміс між «комплексністю» системи, тобто її функціональної наповненістю, й сукупною вартістю її побудови та експлуатації. Під вартістю експлуатації мається на увазі рівень адаптованості СЗІ (тобто збереження необхідного рівня захисту) до неминучих змін складу та конфігурації ІС.

Практика показує, що в даний час оптимальним підходом для забезпечення необхідної комплексності СЗІ є побудова системи на базі таких продуктів, які проявляють свої захисні функції на двох-трьох, при цьому необов'язково сусідніх, рівнях СЗІ. І, очевидно, «притаманні» на кожному рівні захисні функції повинні повністю перекривати вимоги, які накладаються на захист даного рівня. Зробити це можливо вже сьогодні на основі наявних на нашому ринку продуктів із захисту інформації. Так. наприклад, існуючі сьогодні розвинені продукти по реалізації функцій міжмережевого екранування дозволяють вирішувати не тільки традиційні для міжмережевих екранів завдання по фільтрації трафіку на мережевому рівні, а й частину завдань користувацького рівня (аутентифікація віддалених користувачів і завдання політик безпеки для кожного користувача при роботі у відкритій мережі), технологічного рівня (контроль вхідного трафіку на предмет наявності руйнують і шкідливих програм) і рівня управління (цілісне управління всім комплексом з єдиної консолі). Очевидно, що чим більше таких «багаторівневих» засобів захисту застосовується в СЗІ, тим легше її проектування й повніше та надійніше вона виконує свої функції [5].

Проблема розмежування системи захисту інформації різного ступеня конфіденційності полягає в тому, що часто на практиці в рамках однієї ІС доводиться «працювати» з інформацією, вимоги щодо захисту якої істотно відрізняються одина від одної. Так інформація, яка обробляється й зберігається в рамках єдиної ІС, як правило, поділяються на три групи: відкриті інформаційні ресурси, конфіденційні інформаційні ресурси, інформаційні ресурси обмеженого доступу,

Очевидно, що захист всіх трьох різновидів інформаційних ресурсів в рамках однієї і тієї ж СЗІ будуть захищатися за вимогами, що пред'являються до захисту секретної

інформації. Очевидно, це призведе до необґрунтовано високої вартості СЗІ й великих незручностей роботи для персоналу компанії. Так само неефективно буде побудова трьох різних СЗІ для кожного з ресурсів, оскільки, по-перше, чітко розділити ці ресурси в рамках однієї ІС практично ніколи не вдається, а по-друге, це знову призведе до підвищення вартості самої системи.

В рамках запропонованої моделі зазначена проблема може бути вирішена шляхом розмежування вимог і, відповідно, функціональності для кожного з рівнів захисту СЗІ стосовно кожної групи інформаційних ресурсів. Зробити це тим більше можливо, оскільки в межах одного рівня вимоги до захисту інформації знаходяться, можна сказати, «в одній системі координат». При цьому, якщо інформаційні ресурси в будь-якому сегменті ІС (приміщення, сервер БД, канал зв'язку, сегмент ІС і т.ін.) чітко фізично не розділені, в рамках СЗІ необхідно оцінити можливість поділу зазначених ресурсів на кожному з рівнів системи. Якщо в межах одного рівня сегментувати інформацію не вдається, система вимог для даного рівня, очевидно, повинна будуватися виходячи з вимог по захисту інформації максимальної ступеня конфіденційності. Якщо сегментація інформації можлива, до рівня може пред'являтися подвійна (потрійна і т.ін.) система вимог. У подібних випадках необхідно застосування нескладних економічних розрахунків з оцінки ефективності того чи іншого рішення [6].

Запропонований підхід до проектування СЗІ на базі ієрархії пятирівневої моделі носить досить загальний (методичний) характер і залишає велике поле для творчості компаніям - проектувальникам. Запропонований системний підхід дозволяє істотно скоротити терміни розробки СЗІ і при цьому запропонувати замовнику дійсно оптимальне і обгрунтоване рішення.

Наскільки ефективна система захисту інформаційних систем побудована на основі системного підходу можна оцінити різними методами та підходами. Ефективність КСЗІ можна характеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози. Існують якісні і кількісні методи аналізу ефективності КСЗІ. У багатьох випадках якісних оцінок не досить, щоб відповісти на питання, наскільки надійний захист інформації. Найбільш точніші кількісні методи. Проте для того, щоб “зміряти” ефективність, необхідно мати обґрунтований критерій (показник оцінки ефективності КСЗІ). На практиці зустрічаються наступні типи критеріїв:

1. Критерії типу “эффект-затрати”, що дозволяють оцінювати досягнення цілей захисту інформації при заданих витратах.

2. Критерії, що дозволяють оцінити рівень захисту інформації за заданими показниками й виключити ті варіанти, які не задовольняють заданим обмеженням. При цьому використовуються методи багатокритерійної оптимізації, відновлення функцій і функціоналів, методи дискретного програмування.

3. Штучно сконструйовані критерії, що дозволяють оцінювати інтегральний ефект (наприклад, “лінійна згортка” часткових показників, методи теорії нечітких множин).

Ефективність функціонування КСЗІ залежить від безлічі взаємопов’язаних між собою елементів, що діють, і, як правило, оцінюється сукупністю критеріїв, що знаходяться в складних конфліктних взаєминах.Відсутність на сьогоднішній день загального підходу до вирішення завдань даного класу закономірно спричиняє за собою різноманіття різних не взаємопов’язаних методів оцінки рівня захисту інформації.

Процес визначення ефективності систем захисту починають з вибору і обґрунтування показників (критеріїв) оцінки ефективності системи захисту, а потім переходять до підбору або розробки методик розрахунку цих показників. У таблиці 1 приведені умовні назви підходів, що використовуються для вибору критеріїв і оцінки параметрів, показники ефективності систем захисту і методики їх розрахунку.

Таблиця 1

Показники оцінки ефективності комплексних систем захисту і методики їх розрахунку

№ п/п	Підхід до оцінки КСЗІ	Показники оцінки ефективності	Спосіб розрахунку показників
1.	Статистичний	Загроза і-го типу виникає в середньому за період часу Ті.	Статистична обробка потенційних загроз і їх наслідків.
2.	Імовірнісний	Сумарні середні втрати $R = \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} P(\vec{\gamma} / \vec{x},) P(\vec{s}) \Pi(\vec{\gamma} / \vec{s}) + m$ $P(\vec{\gamma} / m\, \vec{s})$ - вірогідність усунення; $P(\vec{s})$ - апріорна вірогідність стану об'єкту контролю; $\Pi(\vec{\gamma} / \vec{s})$ - втрати прийняття рішення s при стані об'єкту s; m - кількість розпізнаваних погроз.	Визначається імовірність відмови системи від обробки даних в результаті реалізації загроз.
3.	Частотний	Очікуваний збиток від і-ї загрози: $R_i = F(S,V)$, де S - показник частоти виникнення загрози; V - умовний показник збитку.	На підставі аналізу статистичного матеріалу задається значення S, величина V вибирається рівною від 1 до max можливої суми збитку, розраховується значення показника R_i як функції параметрів V і S.
4.	Експертне оцінювання	Ступінь забезпечення безпеки *SR* системи *S* $SR_{(s,r)} = \frac{1}{n_{i=1}^{n}} W_i G_i.$	Визначається кількість (n) і перелік параметрів (i), які характерезують КСЗІ. Задаються значення суб'єктивних коефіцієнтів важливості (W_i) кожній з характеристик G_i, призначених експертним шляхом. Розраховуються значення параметра *SR*.
5.	Інформационно-ентропійний	Величина інформаційної ентропії Шенона: $\psi(t) = (\int_0^t s_n(t-\tau)...(\int^t s_3(\int_0^t s_1(\tau) s_2(t-\tau) d\tau ...) d\tau$ $s_1 .... s_n$ - значення інформаційної ентропії різних підсистем.	Проводиться аналітичне обчислення інформаційної ентропії системи, використовуючи поняття згортки функції. При лінійній залежності ефективність інтеграції підсистем в інформаційному плані вважають задовільною. Інакше – неефективною.

6.	Нейромережевий підхід	Нечіткі показники захисту інформаційної системи у вигляді лінгвістичних змінних, таких як: “абсолютно незахищена”, “недостатньо захищена”, “захищена”, “достатньо захищена”, “абсолютно захищена” $A = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$.	Приналежність певного рівня безпеки визначається на проміжку [0, 1], показники надійності являються функцією приналежності $\mu^A(x_i)$, де – є елемент множини X – вимог безпеки, A – безліч значень, що визначають виконання вимог безпеки. Оцінка ефективності проводиться по чітко визначених критеріях.
7.	Метод мінімізації ризиків	Показник економічного ефекту від управління ризиками розраховується по формулі, що враховує Мо – сумарні вірогідні втрати без обробки ідентифікованих ризиків; сумарні вірогідні втрати після обробки ризиків М; сумарні фактичні втрати від прояву ризиків Іф; сумарні фактичні витрати на обробку ідентифікованих ризиків ($H = H_ф$); сумарні фактичні втрати від прояву ризиків $I_{фн}$; сумарні фактичні витрати на обробку ризиків $H_{фн}$: $E = (\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i) - ((\sum_{i=1}^{N} I_{фi} + \sum_{i=1}^{N} H_{фi}) + (\sum$	1. Провести фіксацію ризиків. 2. Визначити індекс ризику (може бути виражений відносним або абсолютним рівнем витрат і вимірюється вірогідністю виникнення ризику і ступенем впливу ризику при його виникненні). 3. Класифікація ризиків за ступенем дії і по рівню впливу. 4. Визначення способів обробки ризику. 5. Розрахунок показників, що характеризують ризики. 6. Розрахунок показника економічного ефекту від управління ризиками.
8.	Матричний	Стан системи захисту описується трійкою параметрів, наприклад: (*S, O, M*) – множини *S* – суб'єктів, *O* – об'єктів, *M* – прав доступу; Або (*O, H, M*) - *O* - основи і складові частини системи (нормативно-правова, організаційна, інформаційна і так далі), *H* – напрями захисту, *M* – етапи створення КСЗІ.	1. Визначення параметрів. 2. Складання тривимірної матриці відносин. 3. Перетворення матриці відносин в двовимірну таблицю. 4. Визначення якісних і кількісних значень показників.
9.	Багаторі в-невий	Стан системи захисту описується сукупністю рівнів конфіденційності і набору категорій конфіденційності.	Модель кінцевих станів Бела Ла-Падули. Гратчаста модель Д. Деннінга.
10.	Оптимізаційний	Вирішується завдання дискретного програмування вигляду: максимізувати $\sum_{j=1}^{n} c_j x_j$ за умов $\sum_{j=1}^{n} a_{ij} x_j \le b_i, i = \overline{1,m};\ x_j \in \{0,1\},\ j = \overline{1,n}.$	Методи Балаша для цілочисельних змінних, гілок і меж, виключення групи невідомих, елементи теорії подвійності, інструментарій лінійного, опуклого і параметричного програмування.

Найбільш поширеними методами оцінки ефективності КСЗІ, які використовуються при так званому оптимізаційному або комбінаторному підході, є: адитивний метод Балаша та метод гілок і меж, що відноситься до класу завдань дискретного програмування з булевими змінними. Вказані методи використовуються як для побудови нової КСЗІ, так і для оцінки якісних характеристик існуючої КСЗІ [7].

Аналіз викладених підходів до оцінки рівня захищеності інформації показав, що вони мають низку проблемних питань, до основних з яких слід віднести:

- відсутність чіткої ієрархічної структури рівня захищеності інформації КСЗІ з визначенням інтегральних (загальних) і часткових показників різного рівня, принципів згортання часткових показників (у тому числі, різного типу) в інтегральні;
- складність комплексної оцінки рівня захищеності інформації КСЗІ на основі наведених в методиках часткових показників та способів їх згортки у інтегральний показник;
- відсутність можливості вирішення оптимізаційних завдань, важливих при формулюванні та прийнятті рішення на впровадження комплексу заходів з забезпечення захисту інформації на ОІД;
- неврахування у методиках оцінки ефективності КСЗІ зв'язків між показниками, що використовувалися як основними так і імовірними показниками;
- неврахування нестохастичних, у тому числі нечітких, факторів впливу на рівень захищеності інформації КСЗІ в ІС;
- фактична відсутність інтегральної оцінки рівня захищеності інформації за умов впливу загроз на інформацію що циркулює в ІС.

Аналіз підходів до оцінки ефективності КСЗІ, дозволяє зробити висновок, що в основі практично всіх відомих методик оцінки ефективності КСЗІ лежать такі математичні моделі (ММ)[8]: оціночні – за цільовою спрямованістю; однорівневі – за ієрархічною структурою; аналітичні – за способом опису функціональних зв'язків; комбіновані – за способом урахування випадкових факторів; імовірностні – з точки зору врахування стохастичної невизначеності.

Але при такому підході практично не враховується той факт, що будь-яка ІС діє за умов істотної невизначеності внутрішнього і зовнішнього середовищ та описується на основі інформації, що має неповний, неточний або не повністю визначений характер.

Існуючі підходи або зовсім виключають невизначеність зі своїх ММ, або нездібні формально описати й врахувати всю можливу її різноманітність. Отже, необхідні нові, додаткові, аналітичні підходи й інструменти для вирішення завдань щодо оцінки рівня захищеності інформації КСЗІ в ІС.

Аналіз існуючих методик показав, що цілком вірно пропонується оцінювати ефективність КСЗІ, як складну систему і характеризувати декількома частковими показниками, на підставі яких формується загальний критерій.

Усі зазначені підходи правомірні. Проте, їх реалізація не відображає у повній мірі суті захисту інформації і не дозволяє однозначно визначити запропоновані дослідниками показники ефективності КСЗІ, як адекватний процесу інтегральний показник, з точки зору реалізації можливостей КСЗІ щодо вирішення покладених на неї завдань.

Неврахування зазначених недоліків не дозволяє з достатньою достовірністю і точністю оцінити рівень захищеності інформації для подальшого обґрунтування рекомендацій щодо удосконалення КСЗІв зазначених умовах.

Таким чином, існуючі підходи щодо оцінки ефективності КСЗІ можуть бути покладені в основу розробки методики оцінки рівня захищеності інформації КСЗІ в ІС, що надає актуальності даному дослідженню.

Висновки

Показано, що проблем у проектуванні систем технічного захисту інформації предостатньо.

Однією з проблем природно є недосконаліть нормативно-правової бази, на підставі якої і виробляється весь процес проектування будь-якої системи - а тим більше системи технічного захисту інформації. І в цьому насамперед повинна бути зацікавлена держава - як носій і власник державної інформації. А відповідно, одним з найважливіших завдань для держави є визначення державної політики на збереження державних інтересов в галузі новітніх досліджень, інноваціонних технологій, наукових розробок, що носять державний рівень і т.ін.

Литература:

1. Кривуца В.Г., Беркман Л.Н., Толюпа С.В. Інфокомунікаційні мережі нового покоління. // Монографія. К. – ДУІКТ. – 2012. – с. 286.
2. Гайворонський М.В. Безпека інформаційно-комунікаційних систем / Гайворонський М.В., Новиков О.М. – К.: Вид. група BHV, 2009. – 608 с.
3. Павлов И.Н. Проектирование систем защиты информации. Формальный подход [Текст] / И.Н. Павлов. – “Правове, нормативне та метрологічнезабезпечення систем захистуінформації в Україні”. – Київ.: 2005. – Вып. 11. – С. 54 − 59.
4. В.И. Андреев, Ю.Ю. Гончаренко, М.М. Дивизинюк, И.Н. Павлов, В.А. Хорошко.Проектирование систем технической защиты информации / – Севастополь.: Изд. Центр СНУЯЭиП, 2011. – 235 с.
5. Толюпа С.В. Проектирование систем поддержки принятия решений в процессе восстановления и обеспечения комплексной защити информационных системах. // Науково-технічний журнал “Сучасний захист інформації”.– 2012. - №4. – С. 69-74.
6. Павлов І.М. Формалізація проектних показників якості захисту інформації комплексної системи захисту інформації / Павлов І.М., Бірюков В.О. – Захист інформації. – Київ: 2011. – № 2(51). – С. 15 – 21.
7. Власов О.М., Толюпа С.В. Комплексний підхід оцінки ефективності систем захисту інформації в інфокомунікаційних мережах нового покоління // Наукові записки Наукові записки Українського науково-дослідного інституту зв’язку. Науково-виробничий збірник – 2011 - №3(19). – С. 38-45.
8. D.E. BellSecureComputerSystems: Mathematicalfoundationsandmodel /D.E. Bell, L.J. LaPadula. – ReportESD – TR – 73 – 278, Mitre Corp., Bedford, Mass, Nov. 1973.

Надійшла 17.11.2015 р. Рецензент: д.т.н., проф. Хорошко В.О.